DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 170 and 171

RIN 0955–AA01

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Final rule.

SUMMARY: This final rule implements certain provisions of the 21st Century Cures Act, including Conditions and Maintenance of Certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program), the voluntary certification of health IT for use by pediatric health care providers, and reasonable and necessary activities that do not constitute information blocking. The implementation of these provisions will advance interoperability and support the access, exchange, and use of electronic health information. The rule also finalizes certain modifications to the 2015 Edition health IT certification criteria and Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

DATES:

Effective date: This final rule is effective on June 30, 2020.

Incorporation by reference: The incorporation by reference of certain publications listed in the rule was approved by the Director of the Federal Register as of June 30, 2020.

Compliance date: Compliance with 45 CFR 170.401, 170.402(a)(1), and 45 CFR part 171 is required by November 2, 2020.

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Executive Summary

A. Purpose of Regulatory Action

ONC is responsible for the implementation of key provisions in Title IV of the 21st Century Cures Act (Cures Act) that are designed to advance interoperability; support the access, exchange, and use of electronic health information (EHI); and address occurrences of information blocking. This final rule implements certain provisions of the Cures Act, including Conditions and Maintenance of Certification requirements for health information technology (health IT)

developers, the voluntary certification of health IT for use by pediatric health providers, and reasonable and necessary activities that do not constitute information blocking. The final rule also implements parts of section 4006(a) of the Cures Act to support patients' access to their EHI in a form convenient for patients, such as making a patient's EHI more electronically accessible through the adoption of standards and certification criteria and the implementation of information blocking policies that support patient electronic access to their health information at no cost. Additionally, the final rule modifies the 2015 Edition health IT certification criteria and ONC Health IT Certification Program (Program) in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

In addition to fulfilling the Cures Act's requirements, the final rule contributes to fulfilling Executive Order (E.O.) 13813. The President issued E.O. 13813 on October 12, 2017, to promote health care choice and competition across the United States. Section 1(c) of the E.O., in relevant part, states that government rules affecting the United States health care system should re-inject competition into health care markets by lowering barriers to entry and preventing abuses of market power. Section 1(c) also states that government rules should improve access to and the quality of information that Americans need to make informed health care decisions. For example, as mentioned above, the final rule establishes application programming interface (API) requirements, including for patients' access to their health information without special effort. The API approach also supports health care providers' independence to choose the ''provider-facing'' third-party services they want to use to interact with the certified API technology they have acquired. In addition, the final rule provides the Secretary of Health and Human Services' (Secretary) interpretation of the information blocking definition as established in the Cures Act and the application of the information blocking provision by identifying reasonable and necessary activities that would not constitute information blocking. Many of these activities focus on improving patient and health care provider access to EHI and promoting competition.

B. Summary of Major Provisions and Clarifications

1. Deregulatory Actions for Previous Rulemakings

Since the inception of the Program, we have aimed to implement and administer the Program in the least burdensome manner that supports our policy goals. Throughout the years, we have worked to improve the Program with a focus on ways to reduce burden, offer flexibility to both developers and providers, and support innovation. This approach has been consistent with the principles of E.O. 13563 on Improving Regulation and Regulatory Review (February 2, 2011), which instructs agencies to ''periodically review its existing significant regulations and determine whether any such regulations should be modified, streamlined, expanded, or repealed so as to make the agency's regulatory program more effective or less burdensome in achieving the regulatory objectives.'' To that end, we have historically, where feasible and appropriate, taken measures to reduce burden within the Program and make the Program more effective, flexible, and streamlined.

We reviewed and evaluated existing regulations and identified ways to administratively reduce burden and implement deregulatory actions through guidance. In this final rule, we have finalized new deregulatory actions that will reduce burden for health IT developers, providers, and other stakeholders. We have finalized five deregulatory actions in section III.B: (1) Removal of a requirement to conduct randomized surveillance on a set percentage of certified products, allowing ONC-Authorized Certification Bodies (ONC–ACBs) more flexibility to identify the right approach for surveillance actions; (2) removal of the 2014 Edition from the Code of Federal Regulations (CFR); (3) removal of the ONC-Approved Accreditor (ONC–AA) from the Program; (4) removal of certain 2015 Edition certification criteria; and (5) removal of certain Program requirements. We have not finalized a sixth deregulatory action we proposed, related to recognition of the Food and Drug Administration (FDA) Software Precertification Program, as comments and the early stage of development of the FDA program indicate finalization would be premature at this time.

2. Updates to the 2015 Edition Certification Criteria

This final rule updates the 2015 Edition to remove several certification criteria. It also updates some certification criteria to reflect standard and implementation specification updates. In consideration of public comments, the final rule adds only two new technical certification criteria and two new attestation-structured privacy and security certification criteria.

a. Adoption of the United States Core Data for Interoperability (USCDI) as a Standard

We noted in the Proposed Rule that, as part of continued efforts to ensure the availability of a minimum baseline of data classes that could be commonly available for interoperable exchange, ONC adopted the 2015 Edition ''Common Clinical Data Set'' (CCDS) definition and used the CCDS shorthand in several certification criteria. However, the CCDS definition also began to be used colloquially for many different purposes. As the CCDS definition's relevance grew outside of its regulatory context, it was often viewed as a ceiling to the industry's collective data set for access, exchange, and use. In addition, we noted in the NPRM that as we continue to move toward value-based care, the inclusion of additional data classes beyond the CCDS would be necessary. In order to advance interoperability, we proposed to remove the CCDS definition and its references from the 2015 Edition and replace it with the ''United States Core Data for Interoperability [1]'' (USCDI). We proposed to adopt the USCDI as a standard, naming USCDI Version 1 (USCDI v1) in § 170.213 and incorporating it by reference in § 170.299. The USCDI standard would establish a set of data classes and constituent data elements required to support interoperability nationwide. To achieve the goals set forth in the Cures Act, we indicated that we intended to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. We also noted that once the USCDI is adopted by the Secretary in regulation, health IT developers would be allowed to take advantage of a new proposed flexibility we called the ''Standards Version Advancement Process'' (SVAP) (see 84 FR 7497 through 7500, see also section VII.B.5 of this final rule). In order to advance interoperability, we have finalized the adoption of the USCDI standard. Because the USCDI is adopted as a standard and the SVAP is finalized, the SVAP will allow a developer to voluntarily have their products certified to newer, National Coordinator approved versions of the

[1] *https://www.healthit.gov/uscdi.*

USCDI in the future without waiting for rulemaking to update the version of the USCDI listed in the regulations.

b. Electronic Prescribing

We have finalized an update to the electronic prescribing National Council for Prescription Drug Programs (NCPDP) SCRIPT standard in 45 CFR 170.205(b) from NCPDP SCRIPT standard version 10.6 to NCPDP SCRIPT standard version 2017071 for the electronic prescribing certification criterion (§ 170.315(b)(3)). ONC and the Centers for Medicare & Medicaid Services (CMS) have historically maintained aligned e-Rx and medication history (MH) standards to ensure that the current standard for certification to the electronic prescribing criterion supports use of the current Part D e-Rx and MH standards. This helps advance alignment with CMS' program standards.

In a final rule published April 16, 2018, CMS finalized its update of its Part D standards to NCPDP SCRIPT standard version 2017071 for e-Rx and MH, effective January 1, 2020 (83 FR 16440). In addition to continuing to reference the transactions previously included in § 170.315(b)(3), and in keeping with CMS' final rule, we have adopted all of the additional NCPDP SCRIPT standard version 2017071 transactions that CMS adopted in 42 CFR 423.160(b)(2)(iv). Furthermore, we have adopted the same electronic Prior Authorization (ePA) request and response transactions supported by NCPDP SCRIPT standard 2017071 proposed by CMS in the Medicare Program; Secure Electronic Prior Authorization for Medicare Part D proposed rule (84 FR 28450). Some adopted transactions are required to demonstrate conformance to the updated § 170.315(b)(3) criterion, while other transactions are optional.

c. Clinical Quality Measures—Report

In this final rule, we have removed the Health Level 7 (HL7®) Quality Reporting Document Architecture (QRDA) standard requirements in the 2015 Edition ''Clinical Quality Measures—report'' criterion in § 170.315(c)(3) and, in their place, required Health IT Modules to support the CMS QRDA Implementation Guide (IGs).[2] This will help reduce the burden for health IT developers and remove certification requirements that do not support quality reporting for CMS programs.

[2] *https://ecqi.healthit.gov/qrda-quality-reporting-document-architecture.*

d. Electronic Health Information (EHI) Export

We proposed to adopt a new 2015 Edition certification criterion, referred to as ''EHI export'' in § 170.315(b)(10) in the Proposed Rule. The criterion's proposed conformance requirements were intended to provide a means to export the entire EHI a certified health IT product produced and electronically managed to support two contexts: (1) Single patient EHI export and (2) for patient EHI export when a health care provider is switching health IT systems. The proposals did not require the exported data to be in a specific standardized format. Rather, we proposed to require that such an export be in a computable, electronic format made available via a publicly accessible hyperlink. We noted that this transparency would facilitate the subsequent interpretation and use of the exported information.

We have finalized the criterion with modifications in response to public comment. We have refined the scope of data a Health IT Module certified to § 170.315(b)(10) must export, and aligned the criterion to the definition of EHI we finalized in § 170.102 and § 171.102. The finalized criterion requires a certified Health IT Module to electronically export all of the EHI, as defined in § 171.102, that can be stored at the time of certification by the product, of which the Health IT Module is a part. We finalized the 2015 Edition Cures Update ''EHI export'' criterion in § 170.315(b)(10) but did not finalize its inclusion in the 2015 Edition Base Electronic Health Record (EHR) definition, as proposed. Our intention with this criterion, in combination with other criteria set forth in this final rule, is to advance the interoperability of health IT as defined in section 4003 the Cures Act, including the ''complete access, exchange, and use of all electronically accessible health information.''

e. Application Programming Interfaces (APIs)

We have adopted a new API certification criterion in § 170.315(g)(10) to replace the ''application access—data category request'' certification criterion (§ 170.315(g)(8)), and added it to the updated 2015 Edition Base EHR definition. This new ''standardized API for patient and population services'' certification criterion focuses on supporting two types of API-enabled services: (1) Services for which a single patient's data is the focus and (2) services for which multiple patients' data are the focus. The API certification criterion requires the use of the Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standard Release 4 and references several standards and implementation specifications adopted in § 170.213 and § 170.215 to support standardization and interoperability. This certification criterion will align industry efforts around FHIR Release 4 and advance interoperability of API-enabled ''read'' services for single and multiple patients.

f. Privacy and Security Transparency Attestations

We have adopted two new privacy and security certification criteria requiring transparency attestations from developers of certified health IT as part of the updated 2015 Edition privacy and security certification framework. The attestations will serve to identify whether or not certified health IT supports encrypting authentication credentials and/or multi-factor authentication (MFA). While these criteria provide increased transparency, they do not require new development or implementation to take place. As part of ONC's ongoing commitment to advance transparency about certified health IT products, ONC will list the developers' attestation responses on the Certified Health IT Product List (CHPL).

g. Security Tags and Consent Management

In the 2015 Edition final rule (80 FR 62646, Oct. 16, 2015), we adopted two ''data segmentation for privacy'' (DS4P) certification criteria, one for creating a summary record according to the DS4P standard (§ 170.315(b)(7)) and one for receiving a summary record according to the DS4P standard (§ 170.315(b)(8)). Certification to these 2015 Edition DS4P criteria only required security tagging of Consolidated-Clinical Document Architecture (C–CDA) documents at the document level. As noted in the 2015 Edition final rule (80 FR 62646), certification to these criteria is not linked to meeting the Certified EHR Technology definition (CEHRT) used in CMS programs.

Since the 2015 Edition final rule, the health care industry has engaged in additional field testing and implementation of the DS4P standard. Stakeholders also shared with ONC—through public forums, listening sessions, and correspondence—that only tagging C–CDA documents at the document level did not permit providers the flexibility to address more complex use cases for representing patient privacy preferences. Based on public comment, in this final rule, we

have changed the names of the two current 2015 Edition DS4P criteria to Security tags—Summary of Care (send) and Security tags—Summary of Care (receive). We also updated the requirements for these criteria to support security tagging at the document, section, and entry levels. This change better reflects the purpose of these criteria and enables adopters to support a more granular approach to security tagging clinical documents for exchange.

In finalizing this more granular approach for security tagging Consolidated Clinical Document Architecture (C–CDA) documents, we note that we do not specify rules or requirements for the disposition of tagged data or any requirements on health care providers related to data segmentation for privacy. The use cases for which health IT certified to these criteria might be implemented would be driven by other applicable Federal, State, local, or tribal law and are outside the scope of the certification criteria. We recognize that the tagging of documents is not a fully automated segmentation of the record but rather a first, technological step or tool to support health IT developers implementing technology solutions for health care providers to replace burdensome manual processes for tagging sensitive information.

We also proposed to adopt a new 2015 Edition certification criterion, ''consent management for APIs'' in § 170.315(g)(11), to support data segmentation and consent management through an API in accordance with the Consent Implementation Guide (IG). However, in response to comments, we have chosen not to finalize our proposal for this criterion at this time.

3. Modifications to the ONC Health IT Certification Program

In this final rule, we have finalized corrections to the 2015 Edition privacy and security certification framework (80 FR 62705) and relevant regulatory provisions. We also have finalized corrections to the relevant current Certification Companion Guides (CCGs). We have adopted new and revised Principles of Proper Conduct (PoPC) for ONC–ACBs. We have finalized clarification that the records retention provision includes the ''life of the edition'' as well as three years after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules. We also have finalized revisions to the PoPC in § 170.523(h) to clarify the basis for certification, including to permit a certification decision to be based on an evaluation conducted by the ONC–ACB for Health IT Modules' compliance with certification criteria by use of conformity methods approved by the National Coordinator for Health Information Technology (National Coordinator). We also have finalized the addition of § 170.523(r) to require ONC–ACBs to accept test results from any ONC-Authorized Testing Laboratory (ONC–ATL) in good standing under the Program and compliant with the ISO/IEC 17025 accreditation requirements consistent with the requirements set forth in §§ 170.520(b)(3) and 170.524(a). We believe these new and revised PoPC provide necessary clarifications for ONC–ACBs and promote stability among the ONC–ACBs. We also have finalized the update of § 170.523(k) to broaden the requirements beyond just the Medicare and Medicaid EHR Incentive Programs (now renamed the Promoting Interoperability (PI) Programs and referenced as such hereafter) and provided other necessary clarifications.

We have finalized a revised PoPC for ONC–ATLs. The finalized revision clarifies that the records retention provision includes the ''life of the edition'' as well as three years after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules.

4. Health IT for the Care Continuum

Section 4001(b) of the Cures Act includes two provisions related to supporting health IT across the care continuum. The first instructs the National Coordinator to encourage, keep, or recognize through existing authorities the voluntary certification of health IT for use in medical specialties and sites of service where more technological advancement or integration is needed. The second outlines a provision related to the voluntary certification of health IT for use by pediatric health providers to support the health care of children. These provisions align closely with our core purpose to promote interoperability and to support care coordination, patient engagement, and health care quality improvement initiatives. Advancing health IT that promotes and supports patient care when and where it is needed continues to be a primary goal of the Program. This means health IT should support patient populations, specialized care, transitions of care, and practice settings across the care continuum.

We have explored how we might work with the health IT industry and with specialty organizations to collaboratively develop and promote health IT that supports medical specialties and sites of service. Over time, we have taken steps to make the Program modular, more open and accessible to different types of health IT, and better able to advance functionality that is generally applicable to a variety of care and practice settings. We considered a wide range of factors specific to the provisions in the Cures Act to support providers of health care for children. These include: The evolution of health IT across the care continuum, the costs and benefits associated with health IT, the potential regulatory burden and compliance timelines, and the need to help advance health IT that benefits multiple medical specialties and sites of service involved in the care of children. In consideration of these factors, and to advance implementation of section 4001(b) of the Cures Act specific to pediatric care, we held a listening session where stakeholders could share their clinical knowledge and technical expertise in pediatric care and pediatric sites of service. Through the information learned at this listening session and our analysis of the health IT landscape for pediatric settings, we identified existing 2015 Edition criteria, as well as new or revised 2015 Edition criteria proposed in the Proposed Rule, that could benefit providers of pediatric care and pediatric settings. In this final rule, we have identified the already existing 2015 Edition certification criteria and the new or revised 2015 Edition criteria adopted in this final rule that support the voluntary certification of health IT for pediatric care and pediatric settings. We also elaborate on our next steps to support pediatric care and pediatric settings through the development, adoption, certification, and use of health IT, including the continued support of a pediatrics health IT web page on *www.healthit.gov/pediatrics* and the future development of informational resources.

We also recognize the significance of the opioid epidemic confronting our nation and the importance of helping to support the health IT needs of health care providers committed to preventing inappropriate access to prescription opioids and to providing safe, appropriate treatment. Therefore, we requested public comment on how our existing Program requirements and the proposals in the Proposed Rule may support use cases related to Opioid Use Disorder (OUD) prevention and treatment and if there were additional areas that we should consider for effective implementation of health IT to help address OUD prevention and treatment. We received over 100

comments in responses to this RFI, which we are actively reviewing.

5. Conditions and Maintenance of Certification Requirements

We have established in this final rule, certain Conditions and Maintenance of Certification requirements for health IT developers based on the Conditions and Maintenance of Certification requirements outlined in section 4002 of the Cures Act. The Program's Conditions and Maintenance of Certification requirements express initial requirements for health IT developers and their certified Health IT Module(s) as well as ongoing requirements that must be met by both health IT developers and their certified Health IT Module(s) under the Program. In this regard, we have implemented the Cures Act Conditions of Certification requirements with further specificity as it applies to the Program and implemented any accompanying Maintenance of Certification requirements as standalone requirements to ensure that the Conditions of Certification requirements are not only met but continually being met through the Maintenance of Certification requirements. In this rule, we capitalize ''Conditions of Certification'' and ''Maintenance of Certification'' when referring to Conditions and Maintenance of Certification requirements established for the Program under section 4002 of the Cures Act for ease of reference and to distinguish from other conditions.

Information Blocking

Section 4002 of the Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification requirement under the Program, not take any action that constitutes information blocking as defined in section 3022(a) of the Public Health Service Act (PHSA). We have adopted the information blocking Condition of Certification requirement in § 170.401 as proposed. As finalized, the Condition of Certification requirement prohibits any health IT developer under the Program from taking any action that constitutes information blocking as defined by section 3022(a) of the PHSA. We have also finalized that definition in § 171.103.

Assurances

Section 4002 of the Cures Act also requires that a health IT developer, as a Condition of Certification requirement under the Program, provide assurances to the Secretary that, unless for legitimate purpose(s) as specified by the Secretary, the developer will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA or any other action that may inhibit the appropriate exchange, access, and use of EHI. We have finalized our proposed implementation of this provision through several Conditions of Certification and accompanying Maintenance of Certification requirements, which are set forth in § 170.402. We have also adopted more specific Conditions and Maintenance of Certification requirements, which are also set forth in § 170.402, for certified health IT developers to provide assurances to the Secretary that it does not take any other action that may inhibit the appropriate exchange, access, and use of EHI. These requirements serve to provide further clarity under the Program as to how health IT developers must meet our requirements as promulgated under the Cures Act.

Communications

The Cures Act also requires as a Condition and Maintenance of Certification requirement under the Program that health IT developers do not prohibit or restrict communications about certain aspects of the performance of health IT and the developers' related business practices. We have finalized (in § 170.403) provisions that permit developers to impose certain types of limited prohibitions and restrictions that strike a balance between the need to promote open communication about health IT, and related developer business practices, with the need to protect the legitimate business interests of health IT developers and others. The provisions identify certain narrowly-defined types of communications, such as communications required by law, made to a government agency, or made to a defined category of safety organization, which will receive ''unqualified protection'' under our Program. Under this policy, developers will be prohibited from imposing any prohibitions or restrictions on such protected communications. Based on public comment received, we have also finalized provisions that allow health IT developers certified under the Program to place limitations on certain types of communications, including screenshots and video.

We have adopted Maintenance of Certification requirements proposed in § 170.403(b) with modifications. A health IT developer must not impose or enforce any contractual requirement that contravenes the requirements of this Condition of Certification. Furthermore, if a health IT developer has contracts/agreements in existence that contravene the requirements of this Condition of Certification, the developer must notify all affected customers, other persons, or entities that the prohibition or restriction within the contract/agreement will not be enforced by the health IT developer. In response to comments, we have finalized in § 170.403(b)(2)(ii) that health IT developers are required to amend their contracts/agreements to remove or make void such provisions only when the contracts/agreements are next modified for other purposes and not within the proposed period of time from the effective date of this final rule.

Application Programming Interfaces (APIs)

As a Condition of Certification requirement in section 4002 of the Cures Act requires health IT developers to publish APIs that allow ''health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.'' The Cures Act's API Condition of Certification requirement also states that a developer must, through an API, ''provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.'' The Cures Act's API Condition of Certification requirement in section 4002 includes several key phrases and requirements for health IT developers that go beyond the technical functionality of the Health IT Modules they present for certification. This final rule captures both the technical functionality and behaviors necessary to implement the Cures Act API Condition of Certification requirement. Specifically, we have adopted new standards, new implementation specifications, a new certification criterion, and have modified the Base EHR definition. In addition, we have finalized detailed Condition and Maintenance of Certification requirements for health IT developers.

Real World Testing

The Cures Act also added a new Condition and Maintenance of Certification requirement that health IT developers must successfully test the real world use of health IT for interoperability in the type(s) of setting(s) in which such technology would be marketed. This provision is critical to advancing transparency regarding Health IT Modules' performance and to users having information that could be crucial to

their decisions to acquire certified health IT.

As discussed in section VII.B.5 of this final rule, we have established in § 170.405 real world testing Condition and Maintenance of Certification requirements that include Maintenance of Certification requirements to update Health IT Modules certified to certain certification criteria (see § 170.405(b)(3) through (7) and section IV.B of this final rule preamble) to ensure this certified technology meets its users' needs for widespread and continued interoperability.

As finalized, real world testing Condition and Maintenance of Certification requirements apply to health IT developers with one or more Health IT Module(s) certified to specific certification criteria focused on interoperability and data exchange that are listed in § 170.405(a), as discussed in section VII.B.5 of this final rule. Under these Condition and Maintenance of Certification requirements, health IT developers must submit publicly available annual real world testing plans as well as annual real world testing results for health IT certified to the criteria identified in § 170.405(a). We have also finalized a flexibility that we have named the Standards Version Advancement Process (SVAP). Under this flexibility, health IT developers will have the option to update their health IT that is certified to the criteria identified in § 170.405(a) to use more advanced version(s) of the adopted standard(s) or implementation specification(s) included in the criteria, provided such versions are approved by the National Coordinator for use in health IT certified under the Program. Similarly, we have finalized our proposal (84 FR 7497 through 7500) that health IT developers presenting health IT for initial certification to one of the criteria listed in § 170.405(a) would have the option to certify to National Coordinator-approved newer version(s) of one or more of the Secretary-adopted standards or implementation specifications applicable to the criterion. All health IT developers voluntarily opting to avail themselves of the SVAP flexibility must ensure that their annual real world testing plans and real world testing results submissions address all the versions of all the standards and implementation specifications to which each Health IT Module is certified. In addition, we have finalized in § 170.405(b)(8)(i) the requirement that health IT developers with existing certifications to criteria listed in § 170.405(a) who wish to avail themselves of the SVAP flexibility must notify both their ONC–ACB and their affected customers of their plans to update their certified health IT, and the update's anticipated impact on their existing certified health IT and customers, specifically including but not limited to whether, and if so for how long, the health IT developer intends to continue supporting the prior version(s) [3] of the standard(s) to which the Health IT Module has already been certified, in addition to the National Coordinator-approved newer version(s) included in a planned update.

We have finalized our proposal (84 FR 7501) to establish in § 170.523(p) a new PoPC for ONC–ACBs that requires ONC–ACBs to review and confirm that each health IT developer with one or more Health IT Module(s) certified to any one or more of the criteria listed in § 170.405(a) submits real world testing plans and real world results on a timeframe that allows for the ONC–ACB to confirm completeness of all plans and results by applicable annual due dates. The specific annual due dates finalized in § 170.523(p) differ from those proposed as, and for the reasons, discussed in section VII.B.5 of this final rule preamble. Once completeness is confirmed, ONC–ACBs must make the plans available to ONC and the public via the Certified Health IT Product List (CHPL).[4] We have also finalized, with clarifying revisions, the PoPC proposed in § 170.523(m) to require ONC–ACBs to aggregate and report to ONC no less than quarterly all updates successfully made to support National Coordinator-approved newer versions of Secretary-adopted standards in certified health IT pursuant to the developers having voluntarily opted to avail themselves of the SVAP flexibility. We also finalize in § 170.523(t) the new PoPC for ONC–ACBs that requires them to ensure that developers seeking to take advantage of the SVAP flexibility provide the advance notice required in § 170.405(b)(8) to all affected customers and its ONC–ACB, and comply with all other applicable requirements.

Attestations

Section 4002(a) of the Cures Act requires that a health IT developer, as Condition and Maintenance of Certification requirements under the Program, provide to the Secretary an attestation to all of the other Conditions of Certification required in section 3001(c)(5)(D) of the PHSA, except for the ''EHR reporting criteria submission'' Condition of Certification requirement in § 3001(c)(5)(D)(vii). We have finalized regulation text implementing the Cures Act's ''attestations'' Condition of Certification requirement in § 170.406. Under § 170.406 as finalized by this rule, health IT developers will attest twice a year to compliance with the Conditions and Maintenance of Certification requirements (except for the EHR reporting criteria submission requirement, which would be metrics reporting requirements separately implemented through a future rulemaking). We believe requiring attestations every six months under § 170.406(b) will properly balance the need to support appropriate enforcement with our desire to limit the burden on health IT developers. In this regard, we have also identified methods to make the process as simple and efficient for health IT developers as possible (*e.g.,* 30-day attestation window, web-based form submissions, and attestation alert reminders).

We have also finalized that attestations will be submitted to ONC–ACBs. We have finalized a new PoPC in § 170.523(q) that an ONC–ACB must review these submissions for completion and share the health IT developers' attestations with us. We would then make the attestations publicly available through the CHPL.

EHR Reporting Criteria Submission

The Cures Act specifies that health IT developers be required, as Condition and Maintenance of Certification requirements under the Program, to submit reporting criteria on certified health IT in accordance with the EHR Reporting Program established under section 3009A of the PHSA, as added by the Cures Act. We have not yet established an EHR Reporting Program. Once we establish such program, we will undertake rulemaking to propose and implement the associated Condition and Maintenance of Certification requirements for health IT developers.

Enforcement

Section 4002(a) of the Cures Act adds (in section 3001(c)(5)(D) of the PHSA) Program requirements aimed at addressing health IT developers' actions and business practices through the Conditions and Maintenance of Certification requirements, which expands the current focus of the

[3] In the near term, many of these prior versions are likely to be the same versions adopted by the Secretary and incorporated by reference in subpart B of 45 CFR part 170. Over time, however, we anticipate increasing frequency of prior versions certified including National Coordinator-approved newer versions of these Secretary-adopted standards.

[4] Although real world testing plans and results will not be immediately available upon publication of this final rule, an overview of the CHPL is available at *https://chpl.healthit.gov/#/resources/overview* (last accessed 07/12/2019). For additional information on how to navigate the CHPL, please refer to the *CHPL Public User Guide*.

Program requirements beyond the certified health IT itself. Equally important, Cures Act section 4002(a) also provides that the Secretary may encourage compliance with the Conditions and Maintenance of Certification requirements and take action to discourage noncompliance. We, therefore, have finalized our proposed enforcement framework for the Conditions and Maintenance of Certification requirements in §§ 170.580 and 170.581 to encourage consistent compliance with the requirements. More specifically, we have finalized our proposed corrective action process in § 170.580 for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement under the Program has not been met or is not being met by a health IT developer. We have also finalized in §§ 170.580 and 170.581 our proposal to utilize, with minor modifications, the processes previously established for ONC direct review of certified health IT in the enforcement of the Conditions and Maintenance of Certification requirements. Where we identify noncompliance, our first priority will be to work with the health IT developer to remedy the matter through a corrective action process. However, under certain circumstances, ONC may ban a health IT developer from the Program and/or terminate the certification of one or more of its Health IT Modules.

6. Information Blocking

Section 4004 of the Cures Act added section 3022 of the PHSA (42 U.S.C. 300jj–52, ''the information blocking provision''). Section 3022(a)(1) of the PHSA defines practices that constitute information blocking when engaged in by a health care provider, or a health information technology developer, exchange, or network. Section 3022(a)(3) authorizes the Secretary to identify, through notice and comment rulemaking, reasonable and necessary activities that do not constitute information blocking for purposes of the definition set forth in section 3022(a)(1).

We identify eight reasonable and necessary activities as exceptions to the information blocking definition, each of which does not constitute information blocking for purposes of section 3022(a)(1) of the PHSA. The exceptions apply to certain activities that are likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, but that would be reasonable and necessary if certain conditions are met.

In developing and finalizing the final exceptions, we were guided by three overarching policy considerations. First, the exceptions are limited to certain activities that we believe are important to the successful functioning of the U.S. health care system, including promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI, and protecting patient safety and promoting competition and innovation in health IT and its use to provide health care services to consumers. Second, each exception is intended to address a significant risk that regulated individuals and entities (*i.e.,* health care providers, health IT developers of certified health IT, health information networks, and health information exchanges) will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking. Third, and last, each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt.

The eight exceptions are set forth in section VIII.D of this final rule. The five exceptions finalized in §§ 171.201–205, and discussed in section VIII.D.1.a–e of this final rule, involve not fulfilling requests to access, exchange, or use EHI. These exceptions are intended to prevent harm and protect patient safety, promote the privacy and security of EHI, excuse an actor from responding to requests that are infeasible, and address activities that are reasonable and necessary to promote the performance of health IT. The three exceptions finalized in §§ 171.301–303, and discussed in section VIII.D.2.a–c of this final rule, involve procedures for fulfilling requests to access, exchange, or use EHI. These exceptions describe when an actor's practice of limiting the content of its response to or the manner in which it responds to a request to access, exchange, or use EHI will not be considered information blocking; when an actor's practice of charging fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI will not be considered information blocking; and when an actor's practice to license interoperability elements for EHI to be accessed, exchanged, or used will not be considered information blocking.

An actor will not be subject to enforcement actions under the information blocking provision for civil monetary penalties (CMP) or appropriate disincentives if the actor's practice satisfies at least one exception. In order to satisfy an exception, each relevant practice by an actor at all relevant times must meet all of the applicable conditions of the exception. However, failure to meet the conditions of an exception does not automatically mean a practice constitutes information blocking. A practice failing to meet all conditions of an exception only means that the practice would not have guaranteed protection from CMPs or appropriate disincentives. The practice would instead be evaluated on a case-by-case basis to assess the specific facts and circumstances (*e.g.,* whether the practice would be considered to rise to the level of an interference, and whether the actor acted with the requisite intent) to determine whether information blocking has occurred.

In addition to establishing the exceptions, we have defined and interpreted terms that are present in section 3022 of the PHSA (such as the types of individuals and entities covered by the information blocking provision). We have also finalized new terms and definitions that are necessary to implement the information blocking provision. We have codified the information blocking section in a new part of title 45 of the Code of Federal Regulations, part 171.

C. Costs and Benefits

Executive Orders 12866 on Regulatory Planning and Review (September 30, 1993), and 13563 on Improving Regulation and Regulatory Review (February 2, 2011), direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). OMB has determined that this final rule is an economically significant rule as the costs associated with this final rule could be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this final rule.

We have estimated the potential monetary costs and benefits of this final rule for health IT developers, health care providers, patients, ONC–ACBs, ONC–ATLs, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out into the following categories: (1) Deregulatory actions (no associated costs); (2) updates to the 2015 Edition health IT certification criteria; (3) Conditions and Maintenance of Certification requirements for a health

IT developer; (4) oversight for the Conditions and Maintenance of Certification requirements; and (5) information blocking.

We note that we have rounded all estimates to the nearest dollar and all estimates are expressed in 2017 dollars as it is the most recent data available to address all cost and benefit estimates consistently. We also note that we did not have adequate data to quantify some of the costs and benefits within this RIA. In those situations, we have described the non-quantified costs and benefits of our provisions; however, such costs and benefits have not been accounted for in the monetary cost and benefit totals below.

We estimated that the total cost for this final rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would, on average, range from $953 million to $2.6 billion with an average annual cost of $1.8 billion. We estimate that the total perpetual cost for this final rule (starting in year two), based on the cost estimates outlined above, would, on average, range from $366 million to $1.3 billion with an average annual cost of $840 million.

We estimated the total annual benefit for this final rule, based on the benefit estimates outlined above, would range from $1.2 billion to $5.0 billion with primary estimated annual benefit of $3.1 billion.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the Recovery Act) (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created ''Title XXX—Health Information Technology and Quality'' (Title XXX) to improve health care quality, safety, and efficiency through the promotion of health IT and electronic health information (EHI) exchange.

The 21st Century Cures Act (hereinafter the ''Cures Act'') was enacted on December 13, 2016, to accelerate the discovery, development, and delivery of 21st century cures, and for other purposes. The Cures Act, Pub. L. 114–255, included Title IV—Delivery, which amended portions of the HITECH Act (Title XIII of Division A of Pub. L. 111–5) by modifying or adding certain provisions to the PHSA relating to health IT.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two new Federal advisory committees, the HIT Policy Committee (HITPC) and the HIT Standards Committee (HITSC). Each was responsible for advising the National Coordinator for Health Information Technology (National Coordinator) on different aspects of standards, implementation specifications, and certification criteria.

Section 3002 of the PHSA, as amended by section 4003(e) of the Cures Act, replaced the HITPC and HITSC with one committee, the Health Information Technology Advisory Committee (HIT Advisory Committee or HITAC). After that change, section 3002(a) of the PHSA established that the HITAC would advise and recommend to the National Coordinator on different aspects of standards, implementation specifications, and certification criteria, relating to the implementation of a health IT infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information. Further described in section 3002(b)(1)(A) of the PHSA, this included providing the National Coordinator with recommendations on a policy framework to advance interoperable health IT infrastructure, updating recommendations to the policy framework, and making new recommendations, as appropriate. Section 3002(b)(2)(A) identified that in general, the HITAC would recommend to the National Coordinator, for purposes of adoption under section 3004 of the PHSA, standards, implementation specifications, and certification criteria and an order of priority for the development, harmonization, and recognition of such standards, specifications, and certification criteria. Similar to the process previously required of the former HITPC and HITSC, the HITAC will develop a schedule for the assessment of policy recommendations for the Secretary to publish in the **Federal Register**.

Section 3004 of the PHSA identifies a process for the adoption of health IT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria. As specified in section 3004(a)(1), the Secretary is required, in consultation with representatives of other relevant Federal agencies, to jointly review standards, implementation specifications, and certification criteria endorsed by the National Coordinator under section 3001(c), and subsequently determine whether to propose the adoption of any grouping of such standards, implementation specifications, or certification criteria. The Secretary is required to publish all determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA, which is titled Subsequent Standards Activity, provides that the Secretary shall adopt additional standards, implementation specifications, and certification criteria as necessary and consistent with the schedule published by the HITAC. We consider this provision in the broader context of the HITECH Act and Cures Act to continue to grant the Secretary the authority and discretion to adopt standards, implementation specifications, and certification criteria that have been recommended by the HITAC and endorsed by the National Coordinator, as well as other appropriate and necessary health IT standards, implementation specifications, and certification criteria.

2. Health IT Certification Program(s)

Under the HITECH Act, section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a program or programs for the voluntary certification of health IT. Specifically, section 3001(c)(5)(A) specifies that the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), shall keep or recognize a program or programs for the voluntary certification of health IT that is in compliance with applicable certification criteria adopted under this subtitle (*i.e.,* certification criteria adopted by the Secretary under section 3004 of the PHSA). The certification program(s) must also include, as appropriate, testing of the technology in accordance with section 13201(b) of the HITECH Act. Overall, section 13201(b) of the HITECH Act requires that with respect to the development of standards and implementation specifications, the Director of National Institute of Standards and Technology (NIST) shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. The same HITECH Act provision (section 13201(b)) also indicates that the development of this conformance testing infrastructure may include a program to accredit independent, non-Federal laboratories to perform testing.

Section 4001 of the Cures Act amended section 3001(c)(5) of the PHSA to instruct the National Coordinator to encourage, keep, or recognize, through

existing authorities, the voluntary certification of health IT under the program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. Section 3001(c)(5)(C)(iii) in particular identifies that the Secretary, in consultation with relevant stakeholders, shall make recommendations for the voluntary certification of health IT for use by pediatric health providers to support the care of children, as well as adopt certification criteria under section 3004 to support the voluntary certification of health IT for use by pediatric health providers. The Cures Act further amended section 3001(c)(5) of the PHSA by adding section 3001(c)(5)(D), which provides the Secretary with the authority to require, through notice and comment rulemaking, Conditions and Maintenance of Certification requirements for the Program.

B. Regulatory History

The Secretary issued an interim final rule with request for comments on January 13, 2010, (75 FR 2014), which adopted an initial set of standards, implementation specifications, and certification criteria. On March 10, 2010, we published a proposed rule (75 FR 11328) that proposed both a temporary and permanent certification program for the purposes of testing and certifying health IT. A final rule establishing the temporary certification program was published on June 24, 2010, (75 FR 36158), and a final rule establishing the permanent certification program was published on January 7, 2011, (76 FR 1262). We have issued multiple rulemakings since these initial rulemakings to update standards, implementation specifications, certification criteria, and the certification program, a history of which can be found in the October 16, 2015 final rule titled, ''2015 Edition Health Information (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications'' (80 FR 62602) (''2015 Edition final rule''). A final rule corrections and clarifications notice was published for the 2015 Edition final rule on December 11, 2015, (80 FR 76868), to correct preamble and regulatory text errors and clarify requirements of the Common Clinical Data Set (CCDS), the 2015 Edition privacy and security certification framework, and the mandatory disclosures for health IT developers.

The 2015 Edition final rule established a new edition of certification criteria (''2015 Edition health IT certification criteria'' or ''2015 Edition'') and a new 2015 Edition Base EHR definition. The 2015 Edition established the capabilities and specified the related standards and implementation specifications that CEHRT would need to include to, at a minimum, support the achievement of ''meaningful use'' by eligible clinicians, eligible hospitals, and critical access hospitals under the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) (now referred to as the Promoting Interoperability (PI) Programs)[5] when the 2015 Edition is required for use under these and other programs referencing the CEHRT definition. The 2015 Edition final rule also made changes to the ONC HIT Certification Program. The final rule adopted a proposal to change the Program's name to the ''ONC Health IT Certification Program'' from the ONC HIT Certification Program, modified the Program to make it more accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond the ambulatory and inpatient settings, and adopted new and revised PoPC for ONC–ACBs.

After issuing a proposed rule on March 2, 2016, (81 FR 11056), we published a final rule titled, ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' (81 FR 72404) (''EOA final rule'') on October 19, 2016. The EOA final rule finalized modifications and new requirements under the Program, including provisions related to our role in the Program. The final rule created a regulatory framework for our direct review of health IT certified under the Program, including, when necessary, requiring the correction of non-conformities found in health IT certified under the Program and suspending and terminating certifications issued to Complete EHRs and Health IT Modules. The final rule also sets forth processes for us to authorize and oversee accredited testing laboratories under the Program. In addition, it includes provisions for expanded public availability of certified health IT surveillance results.

On March 4, 2019, the Secretary published a proposed rule titled, ''21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program'' (84 FR 7424) (''Proposed Rule''). The Proposed Rule proposed to implement certain provisions of the Cures Act that would advance interoperability and support the access, exchange, and use of electronic health information and is the subject of this final rule.

C. General Comments on the Proposed Rule

Comments. Numerous commenters expressed support for the overall direction of the Proposed Rule. Numerous commenters also expressed support for the policy goals expressed in the Proposed Rule, including: Reduced health care costs; improved public health surveillance; improved care coordination, continuity of care, and shared access of data between patient and provider; improved quality and patient safety; increased cost and quality transparency; greater efficiencies; and better health outcomes for patients. A few commenters also commended our interest in ways to use health IT to address opioid use disorders. Many commenters also appreciated detailed context for the provisions in the Proposed Rule. Many commenters stated that the proposed provisions and standards will provide opportunities for innovation as well as increase the ability of health care providers to connect new tools and services to their systems.

A number of commenters commended our responsiveness to the health care community, including patients, in drafting the rule. A few commenters suggested that the existing language in the rule should remain mostly unchanged as ONC drafts the final rule. Many commenters commended us for collaborating with public- and private-sector partners in developing the Proposed Rule. Specifically, some commenters expressed appreciation for our work with CMS and their companion Interoperability and Patient Access Proposed Rule. A number of commenters shared that they look forward to working with us and CMS as the health care industry progresses toward an interoperable system, making it easier for small independent practices and providers to move to value-based care.

Response. We appreciate the support expressed by many commenters. This final rule maintains the direction of the Proposed Rule, and we too look forward to ongoing collaboration with public and private sector partners as we implement the provisions of this final rule.

Comments. A few commenters recommended that the final rule include additional resources to assist with readability and ease of understanding.

Response. We thank commenters for their feedback. As we did with the

[5] *https://www.federalregister.gov/d/2018-16766/p-4.*

Proposed Rule, we are providing resources such as infographics, fact sheets, webinars, and other forms of educational materials and outreach. Many of the education materials can be found on *www.HealthIT.gov/curesrule.*

Comments. Several commenters expressed the opinion that the use of EHRs—and health IT, more generally—has negatively affected the quality of health care delivery and that the Proposed Rule will exacerbate this issue. Some of these commenters stated that the need to input information into EHRs during office visits has resulted in clinicians spending less time communicating with patients, and some noted the impact of data entry on clinician burnout. A few commenters made a similar point that use of EHRs has reduced productivity and, as a result, increased health care spending.

Response. We thank commenters for their feedback. We are aware of the challenges stakeholders have experienced in using EHRs and health IT more broadly. In the Cures Act, Congress identified the importance of easing regulatory and administrative burdens associated with the use of EHRs and health IT. Specifically, through section 4001(a) of the Cures Act, Congress directed the Department of Health and Human Services to establish a goal, develop a strategy, and provide recommendations to reduce EHR-related burdens that affect care delivery.

To that end, on November 28, 2018, we, in partnership with CMS, released a draft *Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs* [6] for public comment. This draft strategy reflects input HHS received through several wide-reaching listening sessions, written input, and stakeholder outreach. We released the final report on February 21, 2020. Reflective of public comment, the final *Strategy on Reducing Regulatory and Administrative Burdens Relating to the Use of Health IT and EHRs* [7] targets burdens tied to regulatory and administrative requirements that HHS can directly impact through the rulemaking process. The report's strategies, recommendations, and policy shifts aim to give clinicians more time to focus on what matters—caring for their patients. Based on stakeholder input, the final strategy outlines three overarching goals designed to reduce clinician burden: (1) Reduce the effort and time required to record health information in EHRs for clinicians; (2) reduce the effort and time required to meet regulatory reporting requirements for clinicians, hospitals, and health care organizations; and (3) improve the functionality and intuitiveness (ease of use) of EHRs.

In addition to the final strategy mentioned above, we refer readers to section III of this final rule, Deregulatory Actions for Previous Rulemakings, for more information on how we have worked to improve the Program with a focus on ways to reduce burden, offer flexibility to both health IT developers and providers, and support innovation.

Comments. We received several comments from a variety of stakeholders to extend the 60-day comment period for the Proposed Rule, stating that due to the depth and complexity of the policies proposed, it would be critical for the public to have extended time to provide sufficient and thoughtful comments to advance shared goals and shape the interoperability landscape.

Response. In response to stakeholder inquiries to extend the 60-day public comment period and based on the stated goals of the Proposed Rule to improve interoperability and patient access to health information for the purposes of promoting competition and better care, we extended the comment period for the Proposed Rule for an additional 30 days which ended on June 3, 2019.

Comments. A number of commenters recommended delaying the final rule by issuing an Interim Final Rule (IFR) with comment. Commenters noted that many organizations are providing comments that include new information blocking exceptions and that we will not be able to incorporate such suggestions into the final rule without an opportunity for comment. Several commenters stated that an IFR was appropriate due to the significance and breadth of the Proposed Rule, as well the magnitude of changes proposed and that an IFR would allow for additional opportunity for stakeholder comment.

Several commenters recommended that ONC consider issuing a Supplemental Notice of Proposed Rulemaking (SNPRM) to seek additional comments on the information blocking provisions. Some of these commenters stated that new definitions and terms introduced in the Proposed Rule need additional clarification and an SNPRM would enable ONC to propose such clarifications and seek feedback on modified proposals.

Response. We recognize the importance of allowing enough time for comment given the breadth of the Proposed Rule and acknowledge the comments requesting the issuance of an IFR or a SNPRM. We believe that the advance posting of the Proposed Rule on the ONC website, the initial 60-day comment period, and the 30-day extension, provided adequate time for comment, especially given the large volume of comments received.

As discussed in the information blocking section of the Proposed Rule (84 FR 7508), after hearing from stakeholders and based on our findings from our 2015 Report to Congress,[8] we concluded that information blocking is a serious problem and recommended that Congress prohibit information blocking and provide penalties and enforcement mechanisms to deter these harmful practices. Congress responded by enacting the Cures Act on December 13, 2016, with many provisions specifying a need for swift implementation. It has been three years since the Cures Act was enacted and information blocking remains a serious concern. This final rule includes provisions that will address information blocking and cannot be further delayed.

We have taken multiple actions to address some expressed concerns regarding the timing of the Conditions and Maintenance of Certification requirements as well as the comprehensiveness of the information blocking proposals. These actions include some burden reduction by removing certain certification criteria, narrowing the scope of certain certification criteria, and increasing the compliance timeline with criteria. For purposes of information blocking, we have established compliance date for 45 CFR part 171 that is six months, rather than sixty days, after the date this final rule publishes in the **Federal Register**. We have also focused the scope of EHI, and provided new and revised exceptions that are actionable and reduce burden. One of these new exceptions (see § 171.301(a) and section VIII.D.2.a of this final rule) includes a provision by which, until 24 months after this rule is published in the **Federal Register**, an actor's conduct can satisfy the conditions of the Content and Manner Exception (§ 171.301) if they provide at least the content that is within the USCDI in response to a request for access, exchange, or use of EHI. Because of these reasons and those noted above, we decline to issue an IFR or SNPRM. Rather, we have issued this final rule to support interoperability, empower patient control of their health care, and instill competition in health care markets.

[6] *https://www.healthit.gov/sites/default/files/page/2018–11/Draft%20Strategy%20on%20Reducing%20Regulatory%20and%20Administrative%20Burden%20Relating.pdf.*

[7] *https://www.healthit.gov/sites/default/files/page/2020-02/BurdenReport_0.pdf.*

[8] *https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.*

III. Deregulatory Actions for Previous Rulemakings

A. Background

1. History of Burden Reduction and Regulatory Flexibility

Since the inception of the ONC Health IT Certification Program (Program), we have aimed to implement and administer the Program in the least burdensome manner that supports our policy goals. Through the years, we have worked to improve the Program with a focus on ways to reduce burden, offer flexibility, and support innovation. This approach has been consistent with the principles of Executive Order (E.O.) 13563 on Improving Regulation and Regulatory Review (February 2, 2011), which instructs agencies to periodically review its existing significant regulations and ''determine whether any such regulations should be modified, streamlined, expanded, or repealed so as to make the agency's regulatory program more effective or less burdensome in achieving the regulatory objectives.'' To that end, we have historically taken measures where feasible and appropriate to reduce burden within the Program and make the Program more effective, flexible, and streamlined.

For example, in the 2014 Edition final rule (77 FR 54164, Sept. 4, 2012), we revised the certified electronic health record technology (CEHRT) definition to provide flexibility and create regulatory efficiencies by narrowing required functionality to a core set of capabilities (*i.e.,* the Base EHR definition) plus the additional capabilities each eligible clinician, eligible hospital, and critical access hospital needed to successfully achieve the applicable objective and measures under the EHR Incentive Programs (now referred to as the Promoting Interoperability (PI) Programs). ONC has also supported more efficient testing and certification methods and reduced regulatory burden through the adoption of a gap certification policy. As explained in the 2014 Edition final rule (77 FR 54254) and the 2015 Edition final rule (80 FR 62681), as modified by the 2015 final rule with corrections and clarifications at 80 FR 76868, where applicable, gap certification allows for the use of a previously certified health IT product's test results for certification criteria identified as unchanged. Developers have been able to use gap certification for more efficient certification of their health IT when updating from the 2011 Edition to the 2014 Edition and from the 2014 Edition to the 2015 Edition.

ONC introduced further means to reduce regulatory burden, increase regulatory flexibility, and promote innovation in the 2014 Edition Release 2 final rule (79 FR 54430) published on September 11, 2014. The 2014 Edition Release 2 final rule established a set of optional 2014 Edition certification criteria that provided flexibility and alternative certification pathways for health IT developers and providers based on their specific circumstances. The 2014 Edition Release 2 final rule also simplified the Program by discontinuing the use of the ''Complete EHR'' certification concept beginning with the 2015 Edition (79 FR 54443).

In the 2015 Edition final rule, we did not ''carry forward'' certain 2014 Edition certification criteria into the 2015 Edition, such as the ''image results,'' ''patient list creation,'' and ''electronic medication administration record'' criteria. We determined that these criteria did not advance functionality or support interoperability (80 FR 62682 through 62684). We also did not require all health IT to be certified to the ''meaningful use measurement'' certification criteria for ''automated numerator recording'' and ''automated measure calculation'' (80 FR 62604 and 62605), which the 2014 Edition had previously required. Based on stakeholder feedback and Program administration observations, we also permitted testing efficiencies for the 2015 Edition ''automated numerator recording'' and ''automated measure calculation'' criteria by removing the live demonstration requirement of recording data and generating reports (80 FR 62703). Health IT developers may now self-test their Health IT Modules' capabilities and submit the resulting reports to the ONC-Authorized Testing Laboratory (ONC–ATL) to verify compliance with the ''meaningful use measurement'' criterion.[9] In order to further reduce burden for health IT developers, in our 2015 Edition final rule, we adopted a more straightforward approach to privacy and security certification requirements and clarified which requirements apply to each criterion within the regulatory functional areas (80 FR 62605).

2. Executive Orders 13771 and 13777

On January 30, 2017, the President issued E.O. 13771 on Reducing Regulation and Controlling Regulatory Costs, which requires agencies to identify deregulatory actions. This order was followed by E.O. 13777, titled ''Enforcing the Regulatory Reform Agenda'' (February 24, 2017). E.O. 13777 provides further direction on implementing regulatory reform by identifying a process by which agencies must review and evaluate existing regulations and make recommendations for repeal or simplification.

In order to implement these regulatory reform initiatives and policies, ONC reviewed and evaluated existing regulations in the year leading to the issuance of the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule (Proposed Rule) (84 FR 7424 through 7610). During our review, we sought to identify ways to further reduce administrative burden, to implement deregulatory actions through guidance, and to put forth deregulatory actions in this final rule that will reduce burden for health IT developer, providers, and other stakeholders.

Prior to publishing the Proposed Rule, on August 21, 2017, ONC issued *Relied Upon Software Program Guidance.*[10] Health IT developers are permitted to use ''relied upon software'' [11] to demonstrate compliance with certification criteria adopted at 45 CFR part 170, subpart C. Historically, in cases where a Health IT Module is paired with multiple ''relied upon software'' products for the same capability, health IT developers were required to demonstrate compliance for the same certification criterion with each of those ''relied upon software'' products in order for the products to be listed on the Certified Health IT Product List (CHPL). With the guidance issued on August 21, 2017, health IT developers could demonstrate compliance with only one ''relied upon software'' product for a criterion/capability. Once the health IT developer demonstrates compliance with a minimum of one ''relied upon software'' product, the developer can have multiple, additional ''relied upon software'' products for the same criterion/capability listed on the CHPL (*https://chpl.healthit.gov/*). This approach reduces burden for health IT developers, ONC–ATLs, and ONC-Authorized Certification Bodies (ONC–ACBs).

On September 21, 2017, ONC announced a deregulatory action to reduce the overall burden for testing

[9] *https://www.healthit.gov/test-method/automated-numerator-recording* and *https://www.healthit.gov/test-method/automated-measure-calculation.*

[10] *https://www.healthit.gov/sites/default/files/relieduponsoftwareguidance.pdf.*

[11] ''Relied upon'' software is defined in the 2011 final rule establishing the permanent certification program (76 FR 1276).

health IT to the 2015 Edition certification criteria.[12] ONC reviewed the 2015 Edition test procedures and changed 30 of the 2015 Edition test procedures from requiring ONC–ATL evaluation to requiring only attestation by health IT developers that their product has capabilities conformant with those specified in the associated certification criterion/criteria.[13] This deregulatory action reduced burden and costs program-wide, while still maintaining the Program's high level of integrity and assurances. The total testing cost savings for health IT developers have been estimated between $8.34 and $9.26 million. ONC–ATLs also benefitted by having more time and resources to focus on tool-based testing (for interoperability-oriented criteria) and being responsive to any retesting requirements that may arise from ONC–ACB surveillance activities. Health care providers and other users of certified health IT did not lose confidence in the Program because health IT developers were still required to meet certification criteria requirements and maintain their products' conformance to the full scope of the associated criteria, including when implemented in the field and in production use. ONC and ONC–ACBs continue to conduct surveillance activities and respond to end-user complaints.

B. Deregulatory Actions

In the Proposed Rule, we proposed (84 FR 7434 through 7439) and sought comment on six specific deregulatory actions. Having considered the comments received on the proposals, which are summarized below, we have decided to finalize five of the six proposed deregulatory actions and not to finalize the proposal to recognize the FDA Software Precertification Pilot Program. We refer readers to section XIII (Regulatory Impact Analysis) of this final rule for a discussion of the estimated cost savings from these finalized deregulatory actions.

1. Removal of Randomized Surveillance Requirements

ONC–ACBs are required under § 170.556 to conduct surveillance of certified health IT to ensure that health IT continues to conform with and function as required by the full scope of the certification requirements. Surveillance is categorized as either reactive surveillance (for example, complaint-based surveillance) or randomized surveillance. Previously finalized regulations in § 170.556(c)(2) required ONC–ACBs to proactively surveil two percent of the certificates they issue annually. As discussed in the Proposed Rule, in the time since the two percent randomized surveillance requirement was finalized, stakeholders had expressed concern that the benefits of in-the-field, randomized surveillance may not outweigh the time commitment required by providers, particularly if no non-conformities are found (84 FR 7434). We noted in the Proposed Rule that, in general, health care providers had expressed that reactive surveillance (*e.g.,* surveillance based on user complaints) is a more logical and economical approach to surveillance. Consistent with our September 21, 2017, exercise of enforcement discretion on implementation of randomized surveillance by ONC–ACBs,[14] we proposed in the Proposed Rule to eliminate certain regulatory randomized surveillance requirements (84 FR 7434).

In the Proposed Rule, we specifically proposed to revise § 170.556(c) by changing the requirement that ONC–ACBs *must* conduct in-the-field, randomized surveillance to specify that ONC–ACBs *may* conduct in-the-field, randomized surveillance (84 FR 7434). We further proposed to remove § 170.556(c)(2), which specified that ONC–ACBs must conduct randomized surveillance for a minimum of two percent of certified health IT products per year. We also proposed to remove the requirements in § 170.556(c)(5) regarding the exclusion and exhaustion of selected locations for randomized surveillance. Additionally, we proposed to remove the requirements in § 170.556(c)(6) regarding the consecutive selection of certified health IT for randomized surveillance. As noted in the Proposed Rule, without these regulatory requirements, ONC–ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, using the methodology identified by ONC with respect to scope (§ 170.556(c)(1)), selection method (§ 170.556(c)(3)), and the number and types of locations for in-the-field surveillance (§ 170.556(c)(4)).

Comments. A substantial number of commenters supported removing the requirements for randomized surveillance. Many commenters supported the proposal to revise § 170.556(c) by changing the requirement that ONC–ACBs must conduct in-the-field, randomized surveillance to specify that ONC–ACBs may conduct in-the-field, randomized surveillance, including the removal of § 170.556(c)(2). Commenters noted that since ONC–ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, the regulatory requirement to conduct randomized surveillance on a specified portion of certified health IT would be unnecessary. Commenters supporting this proposal praised the deregulatory action as allowing more flexibility for ONC–ACBs. A number of commenters were generally supportive of the proposal and applied the caveat that if an ONC–ACB did voluntarily conduct randomized surveillance, they should not do so repeatedly on the same Health IT Module. These commenters indicated a preference that the requirements in § 170.556(c)(6) regarding the consecutive selection of certified health IT for randomized surveillance remain. Several commenters were supportive of removing randomized surveillance requirements and indicated they found this appropriate in view of the Conditions and Maintenance of Certification enhancements to the Program as directed by the Cures Act, while others noted that reactive surveillance may be more effective in surfacing and correcting non-conformities. A number of commenters did not support the proposal, with many expressing concerns that this could be or be perceived to be a reduction in oversight of developers or could reduce providers' confidence that certified Health IT Modules would meet their needs. While a majority of commenters speaking to surveillance burdens on health care providers indicated the removal of mandatory randomized surveillance would, on the whole, reduce burden on health care providers, several expressed concerns about whether providers can discern when a product does not meet certification requirements or know where and how to report their concerns about their certified health IT's conformance to Program requirements. A few commenters suggested that the increased emphasis on reactive surveillance (particularly in some commenters' view because ONC is removing randomized surveillance requirements in advance of the full implementation of the EHR Reporting Program called for by section 4002 of

[12] *https://www.healthit.gov/buzz-blog/healthit-certification/certification-program-updates-support-efficiency-reduce-burden/.*

[13] *https://www.healthit.gov/sites/default/files/policy/selfdeclarationapproachprogramguidance17-04.pdf.*

[14] *https://www.healthit.gov/sites/default/files/ONC_Enforcement_Discretion_Randomized_Surveillance_8-30-17.pdf.*

the Cures Act) indicates a need for additional guidance to help providers and particularly clinicians understand how to recognize and report potential non-conformities in the certified health IT they use.

Response. We thank commenters for their input and reiterate our continued commitment to sustaining the integrity of our Program, including ensuring robust oversight of certified health IT products while avoiding unnecessary burdens on all program stakeholders. Having considered all comments received, in context of the totality of updates we proposed to the Program, we have concluded that the removal of the regulatory requirements for ONC–ACBs to conduct randomized surveillance is consistent with enhancing Program efficiency while maintaining its efficacy. We leave ONC–ACBs the option to conduct randomized surveillance as they determine necessary or appropriate to support continued conformance to Program requirements by Health IT Modules they have certified. We also note that ONC–ACBs that choose to conduct randomized surveillance will still be required to use the methodology identified by ONC with respect to scope (§ 170.556(c)(1)), selection method (§ 170.556(c)(3)), and the number and types of locations for in-the-field surveillance (§ 170.556(c)(4)). While we appreciate concerns that removal of requirements in § 170.556(c)(6) regarding the consecutive selection of certified health IT creates a potential that the same Health IT Module(s) could be selected for randomized surveillance in consecutive years, we are unaware of evidence suggesting that ONC–ACBs choosing to implement randomized surveillance would do so in a manner that would tend to erode its efficacy by over-sampling some products at the expense of under-sampling others. Rather than retain a regulatory provision intended to counterbalance a regulatory requirement for randomized surveillance of a required minimum percent of certified products each year, we believe it is more appropriate at this time to remove the restriction on consecutive selection of the same Health IT Module(s) or location(s) for randomized surveillance and monitor the results of this and other Program enhancements finalized in this rule for any indication that we may need to further adjust regulatory requirements in the future.

We thank commenters for bringing to our attention that health care providers may be uncertain about how or where they can engage the ONC Health IT Certification Program for assistance when the certified health IT they rely on is not performing its certified functions as they expect and their health IT developer is unresponsive or fails to resolve non-conformities with Program requirements. Reactive surveillance by ONC–ACBs, informed and focused by end-user complaints, has always been an essential component of the Program's oversight and assurance of continued conformity of certified Health IT Modules when deployed in the field. While we encourage users to begin seeking troubleshooting and issue resolution support from the developer of their health IT—because the developer is often in the best position to act most promptly to resolve problems with their products' performance—we also encourage the user to share their concerns with the ONC–ACB that certified the health IT in question when the developer has not addressed users' concerns that their certified health IT is not performing as it is certified to perform. As we recognize that users may in some circumstances need, or for purposes potentially including but not limited to their own preferences may wish, to share their concerns about their certified health IT's performance or other health IT matters directly with ONC, we invite health IT users and all other interested parties to share their health IT-related feedback or concerns with ONC through the *Health IT Feedback Form* on our *HealthIT.gov* website.[15] Depending on the nature of a specific feedback message, we may contact the submitter for additional information and, in some instances, may share the information provided with other appropriate entities—such as but not limited to the ONC–ACBs who certify the products about which we receive feedback, as they are often in the best position to assess and respond to feedback expressing concerns about conformance of specific certified criteria used by Health IT Modules in production environments. All information submitted through the *Health IT Feedback Form* is carefully reviewed and helps us to improve our awareness and ability to address health IT-related issues and challenges. Also, we note for clarity that persons sharing health IT-related concerns with ONC via the *Health IT Feedback Form* have the option to remain anonymous and this option has been chosen by some submitters. However, we wish to note that anonymous submissions will prevent us from acquiring additional information to fully follow up on a matter if the submission does not include sufficient detail on which to act. In general, submitters should provide as much detail as possible about the developer, product name, and version of the certified health IT as well as their specific concerns about the certified health IT's performance.

[15] *https://www.healthit.gov/form/healthit-feedback-form.*

2. Removal of the 2014 Edition From the Code of Federal Regulations

In the March 4, 2019 Proposed Rule, we also proposed to remove the 2014 Edition from the Code of Federal Regulations (CFR), which includes standards and functionality now significantly outmoded (84 FR 7434). We noted that removal of the 2014 Edition would make the 2015 Edition the new baseline for health IT certification. The 2015 Edition, including the additional certification criteria, standards, and requirements adopted in this final rule, will better enable interoperability and the access, exchange, and use of electronic health information, as discussed in the Proposed Rule (84 FR 7434), and its adoption and implementation by providers is expected to yield the estimated costs savings described (84 FR 7563 and 7564) within the Regulatory Impact Analysis (section XIV) of the Proposed Rule and in the Regulatory Impact Analysis section (section XIII) of this final rule.

To implement the removal of the 2014 Edition from the CFR, we proposed (84 FR 7434 and 7435) to remove the 2014 Edition certification criteria (§ 170.314) and related standards, terms, and requirements from the CFR. In regard to terms, we proposed to retire the 2014 Edition-related definitions found in § 170.102, including the ''2014 Edition Base EHR,'' ''2014 Edition EHR certification criteria,'' and ''Complete EHR, 2014 Edition.'' As explained in the 2015 Edition final rule (80 FR 62719), the ability to maintain Complete EHR certification is only permitted with health IT certified to the 2014 Edition certification criteria. Because this concept was discontinued for the 2015 Edition, we proposed (84 FR 7435) to remove § 170.545 and any references to Complete EHR from the regulation text in conjunction with the removal of the 2014 Edition. We also proposed (84 FR 7435) to remove references to the 2014 Edition from the Common Clinical Data Set (CCDS) definition and effectively replace it with a new government-unique standard, the United States Core Data for Interoperability (USCDI). We proposed (84 FR 7435) to remove the standards and implementation specifications found in §§ 170.200, 170.202, 170.204, 170.205, 170.207, 170.210, and 170.299 that are only

referenced in the 2014 Edition certification criteria. Adopted standards that are also referenced in the 2015 Edition would remain. Finally, we proposed (84 FR 7435) to remove requirements in § 170.550(f) and any other requirements in subpart E, §§ 170.500 through 170.599, which are specific to the 2014 Edition and do not apply to the 2015 Edition.

As discussed in the Proposed Rule (84 FR 7435), in order to avoid regulatory conflicts, we took into consideration the final rule released by CMS on November 16, 2017, titled ''Medicare Program; CY 2018 Updates to the Quality Payment Program; and Quality Payment Program: Extreme and Uncontrollable Circumstance Policy for the Transition Year'' (82 FR 53568). This Quality Payment Program (QPP) final rule permits eligible clinicians to use EHR technology certified to either the 2014 or 2015 Edition certification criteria, or a combination of the two for the CY 2018 performance period. This QPP final rule also states that the 2015 Edition certified EHR technology (CEHRT) will be required starting with the CY 2019 QPP program year (82 FR 53671). Therefore, we proposed (84 FR 7435) the effective date of removal of the 2014 Edition certification criteria and related standards, terms, and requirements from the CFR would be the effective date of this final rule.

Comments. The majority of the comments received supported removing the 2014 Edition certification criteria from the Code of Federal Regulations. Commenters supporting the removal noted that it will reduce confusion and acknowledges that standards and functionality in the 2014 Edition are now significantly outmoded. Some commenters requested the removal be delayed until the end of CY 2019.

Response. We thank commenters for their support. We have finalized the removal of the 2014 Edition from the CFR as proposed, including making the removal effective as of the effective date of this final rule (60 days after the rule is published in the **Federal Register**). The 2015 Edition was the sole edition permitted to meet the CEHRT definition beginning in the CY 2019 program year. This final rule is published in CY 2020. Therefore, the removal is not in conflict with CMS' regulatory requirements for QPP.

To finalize removal of the 2014 Edition from the CFR, we have removed, effective as of the effective date of this final rule, the 2014 Edition certification criteria in § 170.314. We also finalized removal of terms and definitions specific to the 2014 Edition from § 170.102, including the ''2014 Edition Base EHR,'' ''2014 Edition EHR certification criteria,'' and ''Complete EHR, 2014 Edition'' definitions. As explained in the 2015 Edition final rule (80 FR 62719), the ''Complete EHR'' concept was discontinued for the 2015 Edition. Therefore, in conjunction with the removal of the 2014 Edition, we also remove in this final rule § 170.545 and all other references to ''Complete EHR'' from the regulation text. Moreover, in finalizing the removal of the 2014 Edition from the CFR, we also finalize removal of the standards and implementation specifications found in §§ 170.200, 170.202, 170.204, 170.205, 170.207, 170.210, and 170.299 that are referenced only in the 2014 Edition certification criteria. Adopted standards that are also referenced in the 2015 Edition, as modified by this final rule, remain in the CFR. We also retained the CCDS definition in § 170.102 but removed the standards and implementation specifications that reference the 2014 Edition. Additionally, we finalized the removal of requirements in § 170.550(f) and any other requirements in subpart E, §§ 170.500 through 170.599, that are specific to the 2014 Edition and do not apply to the 2015 Edition.

3. Removal of the ONC-Approved Accreditor From the Program

We proposed to remove the ONC–AA from the Program (84 FR 7435). The ONC–AA's role is to accredit certification bodies for the Program and to oversee the ONC–ACBs. However, years of experience and changes with the Program have led ONC to conclude that, in many respects, the role of the ONC–AA to oversee ONC–ACBs is now duplicative of ONC's oversight. More specifically, ONC's experience with administering the Principles of Proper Conduct (PoPC) for ONC–ACBs as well as issuing necessary regulatory changes (*e.g.,* ONC–ACB surveillance and reporting requirements in the 2015 Edition final rule) has demonstrated that ONC on its own has the capacity to provide the appropriate oversight of ONC–ACBs. Therefore, we believe removal of the ONC–AA will reduce the Program's administrative complexity and burden.

Comments. All but one commenter specifically addressing this proposal were in support of removing the ONC–AA. The one commenter opposed to the proposal stated concerns related to de-coupling accreditation to ISO/IEC 17065 standards (an internationally recognized standard for bodies certifying products, processes, and services to provide assurance of compliance with specified requirements such as initial testing, inspection, and quality management systems) from specific assessment of a certification body's ability to apply their accredited ISO/IEC 17065 capabilities to the Program's certification scheme requirements. The commenter noted that this might place a greater burden on ONC staff than did the Program structure that included an ONC–AA. Finally, one of the commenters in support of removing the ONC–AA from the Program requested additional clarification about criteria and processes that will be used for accreditation of certification bodies following removal of the ONC–AA from the Program.

Response. We thank all commenters for their thoughtful feedback. Upon consideration of all comments received on this proposal, we have finalized it as proposed. As noted in the preamble to the Proposed Rule (84 FR 7435), ONC's experience with administering the PoPC for ONC–ACBs as well as issuing necessary regulatory changes (*e.g.,* ONC–ACB surveillance and reporting requirements in the 2015 Edition final rule) has demonstrated that ONC on its own has the capacity to provide the appropriate oversight of ONC–ACBs. Therefore, we believe removal of the ONC–AA will reduce the Program's administrative complexity and burden while maintaining its effectiveness. We anticipate providing updated information about ONC's updated processes for approval and oversight of certification bodies through familiar mechanisms including but not necessarily limited to the *HealthIT.gov* website prior to the effective date of this final rule, and on an ongoing basis as needed or otherwise appropriate to ensure effective transparency about this aspect of the Program.

To finalize this deregulatory action, we have removed the definition for ''ONC-Approved Accreditor or ONC–AA'' from § 170.502. We also removed §§ 170.501(c), 170.503, and 170.504 regarding requests for ONC–AA status, ONC–AA ongoing responsibilities, and reconsideration for requests for ONC–AA status. Regarding correspondence and communication with ONC, we have revised § 170.505 to remove specific references to the ''ONC–AA'' and ''accreditation organizations requesting ONC–AA status.'' We also have finalized our proposal to sunset the policies reflected in the final rule titled ''Permanent Certification Program for Health Information Technology; Revisions to ONC-Approved Accreditor Processes'' (76 FR 72636), and to remove § 170.575, which established a process for addressing instances where the ONC–AA engages in improper conduct or does not perform its

responsibilities under the Program. Because the regulations promulgated in this prior final rule relate solely to the role of the ONC–AA, we have finalized the removal of those requirements. Accordingly, we also revised the application process for ONC–ACB status in § 170.520(a)(3) to require documentation, with an appropriate scope, that confirms that the applicant has been accredited to ISO/IEC 17065 by any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF), in place of the ONC–AA accreditation documentation requirements. Similarly, instead of requiring the ONC–AA to evaluate the conformance of ONC–ACBs to ISO/IEC 17065, we revise § 170.523(a) to simply require ONC–ACBs to maintain accreditation in good standing to ISO/IEC 17065. This means that ONC–ACBs would need to continue to comply with ISO/IEC 17065 and requirements specific to the ONC Health IT Certification Program scheme.

4. Removal of Certain 2015 Edition Certification Criteria and Standards

Having reviewed and analyzed the 2015 Edition, we proposed to remove certain certification criteria and standards as discussed in the Proposed Rule (84 FR 7435 through 7437) and below. We stated (84 FR 7435) that we believe the removal of these criteria and standards will reduce burden and costs for health IT developers and health care providers by eliminating the need to: Design and meet specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting and disclosure requirements; maintain and update certifications for certified functionalities, and participate in routine surveillance (84 FR 7435). Although we did not expressly state it in the Proposed Rule preamble, the burdens and costs reduced by removal of certain criteria from the 2015 Edition would be those associated with the needs we discussed in the preamble (84 FR 7435) specifically in connection to the criteria we proposed to remove, which are those that had been set forth in § 170.315(a)(6), (7) and (8), (10) and (11), and (13), (b)(4) and (5), and (e)(2) (as the text of 45 CFR part 170 stood prior to this final rule).

a. 2015 Edition Base EHR Definition Certification Criteria

We proposed to remove certain certification criteria from the 2015 Edition that had been included in the 2015 Edition Base EHR definition. As discussed in the preamble to the Proposed Rule (84 FR 7435), the removal of these criteria supports burden and cost reductions for health IT developers and health care providers by eliminating the need to: Design and meet these specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting and disclosure requirements; maintain and update certifications for these specific certified functionalities; and participate in surveillance of health IT certified to these criteria and standards.

i. Problem List

We proposed to remove the 2015 Edition ''problem list'' certification criterion (§ 170.315(a)(6)) from the 2015 Edition (84 FR 7436). As we noted in the Proposed Rule, the functionality in this criterion was first adopted as a 2011 Edition certification criterion to support the associated meaningful use Stage 1 objective and measure for recording problem list information. This 2015 Edition ''problem list'' criterion functionally remains relatively the same as the 2011 Edition and has exactly the same functionality as the 2014 Edition ''problem list'' criterion. We proposed to remove this criterion because the criterion no longer supports the ''recording'' objective and measure of the CMS PI Programs as such objective and measure no longer exist.[16] Additionally, we stated the functionality is sufficiently widespread among health care providers since it has been part of certification and the Certified EHR Technology definition since the 2011 Edition and has not substantively changed with the 2015 Edition. Furthermore, we stated in the Proposed Rule that the functionality is essential to clinical care and would be in EHR systems absent certification, particularly considering the limited certification requirements.

Comments. A number of commenters expressed support for removing the ''problem list'' certification criterion from the 2015 Edition and ''Base EHR'' definition. Several of those expressing support for the removal of this criterion specifically noted that the inclusion of the same data elements in the USCDI should suffice to ensure continued ability of certified health IT to record and facilitate access and exchange of these data. However, a few commenters expressed concern that removing this and other requirements would be a disincentive to maintain the functionality in the future, and some commenters expressed concern about ONC's ability to continue to provide effective oversight and require correction if developers do not ensure the functionalities perform safely and effectively. Commenters stated that while many developers will still continue to support the functionalities proposed for removal, eliminating the certification requirement may allow for developers to provide a ''stripped-down'' product at a lower price point and, in absence of CEHRT definition to guide the providers, mislead independent and small providers into unwittingly acquiring certified health IT that does not fully meet their needs.

Response. As discussed in the preamble to the Proposed Rule, a criterion specific to the ''problem list'' functionality was first adopted in the 2011 Edition, specifically to ensure support for the associated meaningful use Stage 1 objective and the measure for recording problem list information under the CMS PI Programs. The ''recording'' objective and measure is no longer a part of the CMS PI Programs. However, the functionality remains widespread among EHR systems used by health care providers. While this prevalence may be due in part to its inclusion in the Certified EHR Technology definition, without substantive changes, since the 2011 Edition, we believe the more significant reason that this functionality is widely available is because it is essential to clinical care, and therefore, that the market will and should drive its continued presence in EHR systems regardless of certification requirements. While we also appreciate the concerns of commenters about the need for health IT to support the accurate recording of patients' problems and the standards-based exchange of that information, we reiterate that the interoperability-focused criteria that will remain in the Base EHR definition and reference the USCDI will ensure that any system of certified health IT meeting the Base EHR definition is capable of using and exchanging data on a patient's problems using content, format, and other standards applicable to each mode of exchange (*e.g.,* standardized API and C–CDA). Moreover, these interoperability-focused criteria will be subject not only to the Program's familiar initial certification testing and in-the-field reactive surveillance requirements but also to the new Condition and

[16] By stating in the NPRM that the objective and measure no longer exist, we meant in the CMS PI (formerly EHR Incentive) Programs. The authority citation for this statement is the December 15, 2015 CMS Final Rule ''Medicare and Medicaid Programs; Electronic Health Record Incentive Program-Stage 3 and Modifications to Meaningful Use in 2015 Through 2017'' (80 FR 62761 and 62785).

Maintenance of Certification requirements for developers to test annually their certified Health IT Modules' interoperability performance in the types of real world settings for which they are sold.

After consideration of all comments received, and for the reasons noted in the preamble to the Proposed Rule and above, we have finalized the removal of the ''problem list'' certification criterion (§ 170.315(a)(6)). We further note that upon the effective date of this final rule, the ''problem list'' certification criterion is removed from the 2015 Edition and the criterion will no longer be included in the 2015 Edition ''safety-enhanced design'' criterion. This criterion, in § 170.315(g)(3), specifies the user-centered design testing that must be applied to particular EHR functionality submitted for certification. However, in response to specific commenters' concerns about the impact of removing the functionally-based problem list criterion on our ability to take action where developers may retain the functionality, but fail to ensure it does not pose a danger to patient safety or public health, we note that our responsibility, pursuant to section 3001(b) of the PHSA, includes ensuring certified health IT does not pose a risk to patient safety or public health, and is not limited to measuring the conformity of the health IT to specific certification criteria. As discussed in the ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' (EOA) rule which was proposed in 81 FR 11056, and finalized in 81 FR 72404 in 2016, ONC has the authority to address suspected or confirmed non-conformities to the requirements under the ONC Health IT Certification Program if the certified health IT is causing or contributing to serious risks to public health or safety (81 FR 72406). The EOA final rule established in § 170.580 a regulatory framework for ONC's direct review of health IT certified under the Program, which expressly addresses the potential for ONC to initiate direct review if we have a reasonable belief that certified health IT may not conform to the requirements of the Program because the certified health IT may be causing or contributing to conditions that present a serious risk to public health or safety.

With respect to health care providers' selection of certified health IT products, we would encourage all providers to consider the Base EHR or Certified EHR Technology (CEHRT) definition as a useful starting point. Certain health care payment programs, including the CMS PI Programs, require the use of certified health IT. CMS refers to the minimum set of required certification functionalities that the health IT used by eligible clinicians must have in order to qualify for the CMS incentive programs as CEHRT.

Using certified health IT improves care coordination through the electronic exchange of clinical-care documents. It provides a baseline assurance that the technology will perform clinical-care and data-exchange functions in accordance with interoperability standards and user-centered design.

ii. Medication List

We proposed to remove the 2015 Edition ''medication list'' certification criterion (§ 170.315(a)(7)) (84 FR 7436). As we noted in the Proposed Rule, the 2015 Edition ''medication list'' criterion remains functionally the same as the 2011 Edition and 2014 Edition ''medication list'' criteria. As also discussed in the Proposed Rule, a functionally-based ''medication list'' criterion was first adopted as a 2011 Edition certification criterion to support the associated meaningful use Stage 1 objective and measure for recording medication list information. The ''medication list'' criterion that we proposed to remove does not require use of a specific vocabulary standard to record medications.

Comments. Comments on the proposal to remove the ''medication list'' criterion were somewhat mixed. While a number of comments expressed support for the removal of the ''medication list'' criterion from the 2015 Edition as duplicative of medication data included in the USCDI a number of commenters expressed concerns with, and a few commenters indicated opposition to, the removal of the ''medication list'' criterion. A few commenters raised concerns specific to elimination of the ''medication list'' criterion in view of the need to respond to the opioids crisis. One commenter expressed concern in the context of both the medication list and the drug-formulary and preferred drug lists criteria as to whether the removal of these criteria could potentially impact patients' drug costs. Several comments also expressed the same concerns for eliminating the ''medication list'' that were expressed in regard to removal of the ''problem list'' criterion, which are summarized above, regarding whether developers will continue to include the functionality and maintain its safe performance.

Response. We thank commenters for their input. Upon consideration of all comments received on this proposal, we have finalized the removal of the ''medication list'' criterion (§ 170.315(a)(7)). The ''recording'' objective and measure of the CMS PI Programs that the ''medication list'' criterion was originally adopted to support has since been retired from the CMS Programs. However, the functionality remains widespread among EHR systems used by health care providers. While this prevalence may be due in part to its inclusion in the Certified EHR Technology definition since the 2011 Edition, we believe this functionality is widely available and used in more significant part because it is essential to clinical care and, therefore, the market will and should drive its continued presence in EHR systems regardless of certification requirements. While we also appreciate the concerns of commenters about the need for health IT to support clinicians' ability to access, maintain, use, and exchange accurate and up-to-date information on their patients' current medication lists and medication history, we repeat for clarity and emphasis that the interoperability-focused criteria that will remain in the Base EHR definition, and their inclusion of the USCDI, will ensure that any system of certified health IT meeting the Base EHR definition is capable of using and exchanging data on a patient's medications using content, format, and other standards applicable to each mode of exchange (*e.g.,* standardized API consistent with § 171.315(g)(10), or exchange of C–CDA documents using the transport standards and other protocols in § 171.202). We recognize the critical importance of providers' and patients' ability to have, use, and exchange medications information to avoid harms that can arise from interactions and duplications of therapeutic effects amongst newly prescribed drugs and those the patient may already be taking. While the clinical importance of maintaining and referencing current, reconciled medication lists is not limited to those medications with significant risks of misuse or dependency, we agree that it is highlighted by the urgent need to ensure opioids are prescribed and used only with due care when clinically necessary. We believe this clinical importance supports the expectation that the market will ensure this functionality is maintained and will drive innovations that improve its usability for the clinicians who use it in the course of caring for their patients. Moreover, the inclusion of medication information in interoperability-focused criteria in § 170.405(a) will ensure certified health IT can access, use, and exchange medications data according to

applicable content and formatting standards, which the ''medication list'' functionality did not ensure. This interoperability of the data is critical to reducing clinician burden related to manually entering updated drug lists and necessary to enable use of medication information by clinical decision support functionalities. The interoperability-focused criteria will also be subject not only to the Program's familiar initial certification testing and in-the-field reactive surveillance requirements but also to the new Condition and Maintenance of Certification requirements for developers to test annually their certified Health IT Modules' interoperability performance in the types of real world settings for which they are marketed.

We note that once removed from the 2015 Edition, the criterion will no longer be included in the 2015 Edition ''safety-enhanced design'' criterion in § 170.315(g)(3). However, as noted above in context of the ''problem list'' criterion, ONC's responsibility, pursuant to section 3001(b) of the PHSA, includes ensuring certified health IT does not pose a risk to patient safety or public health. Our responsibility for certified health IT and patient safety or public health is not limited to measuring the conformity of the health IT to specific certification criteria. As discussed in the EOA rule, ONC has the authority to address suspected or confirmed non-conformities to the requirements under the Health IT Certification Program if the certified health IT is causing or contributing to serious risks to public health or safety (81 FR 72406). The EOA final rule established in § 170.580 a regulatory framework for ONC's direct review of health IT certified under the Program, which expressly addresses the potential for ONC to initiate direct review if we have a reasonable belief that certified health IT may not conform to the requirements of the Program because the certified health IT may be causing or contributing to conditions that present a serious risk to public health or safety.

iii. Medication Allergy List

We proposed to remove the 2015 Edition ''medication allergy list'' certification criterion (§ 170.315(a)(8)). The functionality in this criterion was first adopted as a 2011 Edition certification criterion to support the associated meaningful use Stage 1 objective and measure for recording medication allergies information. The criterion does not require use of a vocabulary standard to record medication allergies, and does not directly support interoperability as the criterion does not require representation of medication allergies in standardized nomenclature. The criterion no longer supports a ''recording'' objective and measure of the CMS PI Programs as such objective and measure no longer exist. This 2015 Edition ''medication allergy list'' criterion remains functionally the same as the 2011 Edition and 2014 Edition ''medication allergy list'' criteria. The functionality is essential to clinical care and would be in EHR systems absent certification.

Comments. Comments on the proposed removal of the ''medication allergy list'' criterion were mixed, with several commenters supportive of the removal noting that the criterion would be redundant now that medication allergy data will be included in the USCDI. Commenters expressed concern with the removal of the criterion and questioned the ubiquity of the medication allergy list functionality and whether health IT developers would continue to support the functionality if not required by ONC regulations.

Response. We thank commenters for their input. Upon consideration of all comments received on this proposal, we have finalized the removal of the ''medication allergy list'' certification criterion (§ 170.315(a)(8)). The ''recording'' objective and measure of the CMS PI Programs that this criterion was originally adopted to support has since been retired from the CMS Programs. However, the functionality remains widespread among EHR systems. While this prevalence may be due in part to its inclusion in the Certified EHR Technology definition since the 2011 Edition, its importance to clinical care suggests the market will drive ongoing availability and enhancement of this functionality over time. Furthermore, because medication allergies are included in the USCDI, all systems of certified health IT meeting the Base EHR definition will be required to be able to exchange and use medication allergy information according to applicable content and formatting standards, which the ''medication allergies'' criterion did not ensure. This interoperability is critical to reducing clinician burden related to manually entering updated drug lists and necessary to enable use of medication information by clinical decision support functionalities. We believe that requiring the interoperability of medication allergy information will facilitate innovation and improvement in health IT's ability to meet clinicians' and patients' needs more than would the continuation of the ''medication allergies'' functionally-based criterion.

We note that once removed from the 2015 Edition, the ''medication allergy list'' criterion will also no longer be included in the 2015 Edition ''safety-enhanced design'' criterion. However, as noted in context of removed criteria above, ONC's responsibility, pursuant to section 3001(b) of the PHSA includes ensuring certified health IT does not pose a risk to patient safety or public health. Our responsibility for certified health IT and patient safety or public health is not limited to measuring the conformity of the health IT to specific certification criteria. As discussed in the EOA rule, ONC has the authority to address suspected or confirmed non-conformities to the requirements under the Health IT Certification Program if the certified health IT is causing or contributing to serious risks to public health or safety (81 FR 72406). The EOA final rule established in § 170.580 a regulatory framework for ONC's direct review of health IT certified under the Program, which expressly addresses the potential for ONC to initiate direct review if we have a reasonable belief that certified health IT may not conform to the requirements of the Program because the certified health IT may be causing or contributing to conditions that present a serious risk to public health or safety.

iv. Smoking Status

We proposed to remove the 2015 Edition ''smoking status'' criterion (§ 170.315(a)(11)), which would include removing it from the 2015 Edition Base EHR definition (84 FR 7436). We had previously adopted a 2015 Edition ''smoking status'' certification criterion that does not reference a standard. However, the CCDS definition, which we proposed to remove from regulation in favor of adopting the new USCDI standard, required smoking status to be coded in accordance with a standard value set of eight SNOMED CT® codes defined in § 170.207(h). As with other functionality that was included in 2014 Edition, we believe this functionality is now widespread. Further, smoking status data will continue to be required to be available for access and exchange via the USCDI.

Comments. Comments on this proposal were mixed, with a number of commenters expressing support for the removal of ''smoking status'' criterion in the Program and several noting that it is not needed or duplicative in the context of Program requirements to support the USCDI. A few commenters stated concerns that eliminating the requirement would provide a

disincentive for developers to maintain the function in the future. Several commenters expressing concerns about removal of this criterion noted its importance to patient care and to public health, raising points such as the use of smoking status as a key determinant to classify cases of some reportable conditions, such as carbon monoxide poisoning. Concerns raised by commenters opposed to removing smoking status data from providers' EHR systems included potential for additional provider burden, such as that related to providing complete case reporting data and responding to public health requests for additional information on patient smoking status during case investigation processes.

Response. We thank commenters for their input. Upon consideration of the comments, we have finalized the removal of the ''smoking status'' criterion (§ 170.315(a)(11)). While we continue to believe that accurate, up-to-date information on a patient's smoking status and history has significant clinical value, we believe that its importance to clinical care provides adequate motivation for the market to drive ongoing availability and enhancement of this functionality over time. Because smoking status information is included in the USCDI, all systems of certified health IT meeting the Base EHR definition will now be required to be able to exchange and use smoking status information according to applicable content and formatting standards. The ''smoking status'' recording functionality criterion we have removed did not ensure smoking status information was captured in a structured, interoperable manner and interoperability of this data is critical to reducing clinician burden related to maintaining complete, current smoking status information. It is also necessary to enable use of smoking status information by clinical decision support and public health reporting functionalities. We believe that interoperability and exchange of smoking status information through the interoperability-focused certification criteria that reference the USCDI standard will better facilitate innovation and improvement in health IT's ability to meet clinicians' and patients' needs than would continuation of the ''smoking status'' functionally-based recording criterion.

Removal of Specific USCDI Smoking Status Code Set

Along with the ''smoking status'' criterion, we proposed to remove the requirement to code smoking status according to the eight smoking status SNOMED CT® codes referenced in the value set adopted in § 170.207(h). These eight codes reflected an attempt to capture smoking status in a consistent manner. Stakeholder feedback indicated that these eight codes do not appropriately and accurately capture all clinically relevant patient smoking statuses. Accordingly, we proposed to no longer require use of only the specific eight SNOMED CT® codes for representing smoking status and remove the value set standard by deleting and reserving § 170.207(h).

Comments. Comments specifically addressing this proposal were generally supportive of removing the specific value set of eight SNOMED CT® codes, though many also noted the importance of continuing to require health IT certified under the Program to retain the ability to include or access, exchange, and use appropriately standardized smoking status information. Several comments made specific suggestions related to broadening or revising the vocabulary standard requirements for smoking status information going forward. Other commenters suggested adding other forms of tobacco use, including smokeless and second hand, as well as e-cigarette (vaping) use.

Response. We appreciate all commenters' input and note that no comments received raised concerns that are not addressed by inclusion of smoking status information in the USCDI, which all interoperability-focused criteria within the 2015 Edition Base EHR definition, as revised through this final rule, reference. As is the case with patient problems, medications, and medication allergies, we believe having smoking status information available for standards-based exchange is an important facilitator of better care and more effective public health reporting with less data-related burden on clinicians and less need for follow-up by public health professionals to compensate for case reporting data that is incomplete or is not fully interoperable. As is the case with the other removed criteria that were focused on internal recording capabilities, we believe the market can, will, and should be the primary driver for the ongoing maintenance and enhancement of functionalities for end users to record or modify these data. Furthermore, the Program's focus is more appropriately spent on ensuring that certified health IT supports interoperable access, use, and exchange of these data as the key facilitator for more coordinated patient care and for ongoing innovation and improvement in both provider- and patient-facing functionalities. Because comments on revisions or enhancements to smoking status data standardization moving forward are outside the scope of this section, we will not address them in specific detail here. However, we note that the USCDI v1 references as the standard for smoking status information SNOMED CT®, U.S. Edition.[17]

Having considered all comments received on this proposal, we have finalized the removal of the eight-code value set standard and removed and reserved § 170.207(h).

b. Drug-Formulary and Preferred Drug List Checks

We proposed to remove the 2015 Edition ''drug-formulary and preferred drug list checks'' criterion in § 170.315(a)(10).

Comments. Some commenters expressed concern that this criterion's removal could negatively impact prescribers' ability to help their patients manage their prescription drug expenses. Although several commenters supported the removal of this criterion in principle, a number of comments expressed concerns about the effect of removal of the ''drug-formulary and preferred drug list checks'' and other criteria from the Program on health care providers' ability to comply with CMS and State-specific regulatory requirements for successful participation in the Medicare Quality Payment Program (QPP), or the Medicare or Medicaid PI Programs. One commenter, noting that the Drug-Formulary and Preferred Drug List Checks criterion is associated with the CMS e-prescribing objective measures that CMS has finalized for 2019 and subsequent performance years specifically, recommended coordination with CMS to ensure alignment across the policies maintained by these two components of HHS.

Response. We thank commenters for their input. As discussed in the Proposed Rule (84 FR 7437), the 2015 Edition ''drug-formulary and preferred drug list checks'' criterion does call for functionality to check drug formulary and preferred drug lists, but does not require use of any specific interoperability standards. The 2015 Edition ''drug-formulary and preferred drug list checks'' criterion does not include functionality or advance interoperability beyond what was required by the 2014 Edition ''drug-formulary checks'' criterion. While we

[17] For more information on finalized policy regarding adoption of the USCDI standard, see section IV.B.1 of this final rule. USCDI v1 can be accessed freely and directly in its entirety at *https://www.healthit.gov/isa/sites/isa/files/inline-files/USCDIv12019revised2.pdf.*

believe this functionality is fairly ubiquitous now due in part to the widespread adoption of health IT certified to the 2014 Edition, we do not believe it is necessary to continue to require certification to it under the Program in order to ensure it remains widely available. Instead, we believe, prescribers' and patients' interest in assuring patients can get the medications they need at the best available value will provide adequate motivation for the market to drive ongoing availability and enhancement of this functionality over time, including through increasing use of relevant interoperability standards essential to making this functionality more affordable and seamlessly reliable at scale than is feasible in the absence of interoperability driven by ubiquitous use of open standards. Because the ''drug-formulary and preferred drug list checks'' criterion we proposed to remove does not require use of standards or directly drive interoperability, we do not believe its continued inclusion in the Program would provide sufficient value to providers or patients to justify the burden on developers and providers of meeting Program compliance requirements specific to this criterion. We also recognize the importance of ensuring alignment between ONC Health IT Certification Program regulations and the CMS regulations that reference them. We have been and will continue to work in close partnership with our CMS colleagues to ensure that our regulations remain aligned, and that we provide affected stakeholders with the information they need to understand how the rules work together and how to succeed under CMS' PI Programs using health IT certified under ONC's Program. We, therefore, permit ONC–ACBs to issue certificates for this criterion up until January 1, 2022 to align with the requirements of the CMS Medicaid PI Program, as this criterion is associated with measures under the Medicaid program that will continue through 2021; after 2021 there will be no further incentives under the Medicaid Promoting Interoperability Program (84 FR 42592). We have not finalized our proposal to remove the criterion from the CFR but included a provision in § 170.550(m)(1) to only allow ONC–ACBs to issue certificates for this criterion until January 1, 2022.

c. Patient-Specific Education Resources

We proposed to remove the 2015 Edition ''patient-specific education resources'' certification criterion in § 170.315(a)(13) (84 FR 7437). We stated that, based on the number of health IT products that have been certified for this functionality as part of 2014 Edition certification and already for 2015 Edition, we believe that health IT's ability to identify appropriate patient education materials is widespread now among health IT developers and their customers (*e.g.,* health care providers). We also noted that we have recently seen innovative advancements in this field, including the use of automation and algorithms to provide appropriate education materials to patients in a timely manner. These advancements help limit clinical workflow interruptions and demonstrate the use and promise of health IT to create efficiencies and improve patient care. As such, we stated that removal of this criterion would prevent certification from creating an unnecessary burden for developers and providers and an impediment to innovation.

Comments. Some commenters expressed concern related to this functionality not yet being consistently used by all providers and to whether removal of this criterion may create a barrier to successful participation for providers in the Medicaid PI Program. One commenter noted that providers' workflow changes to use this functionality are substantial and expressed concern related to providers potentially not undertaking such changes if the criteria were not required to be included in health IT and used by providers.

Response. While we continue to recognize the importance of patient and provider interaction to promote positive health outcomes, we also believe that this criterion, narrowly focused on a specific functionality not connected to interoperability, is no longer the best way to encourage innovation and advancement in health IT's ability to support clinician-patient interactions and relationships.

Having reviewed all comments received on this proposal, we have decided not to remove the ''patient-specific education resources'' criterion from the Program at this time. We recognize the importance of ensuring alignment between ONC Health IT Certification Program regulations and the CMS regulations that reference them. We will continue to work in close partnership with our CMS colleagues to ensure that our regulations remain aligned and that we provide affected stakeholders with the information they need to understand how the rules work together and how to succeed under CMS incentive programs using health IT certified under ONC's Program. CMS has identified this criterion as supporting the patient electronic access to health information objective and measure, which is expected to remain operational for Medicaid until January 1, 2022; after 2021, there will be no further incentives under the Medicaid Promoting Interoperability Program (84 FR 42592). We, therefore, will permit ONC–ACBs to issue certificates for this criterion up until January 1, 2022, to align with the requirements of the CMS Medicaid PI Program (84 FR 42592). We have included a provision in § 170.550(m)(1) to only allow ONC–ACBs to issue certificates for this criterion until January 1, 2022.

d. Common Clinical Data Set Summary Record—Create; and Common Clinical Data Set Summary Record—Receive

As stated in the proposed rule (84 FR 7437), we assessed the number of products certified to the 2015 Edition ''Common Clinical Data Set summary record—create'' (§ 170.315(b)(4)) and ''Common Clinical Data Set summary record—receive'' (§ 170.315(b)(5)) criteria that have not also been certified to the 2015 Edition ''transitions of care'' criterion (§ 170.315(b)(1)) that also requires health IT be capable of creating and receiving Common Clinical Data Set (CCDS) Summary Records using the same interoperability standards. We explained that, based on our findings of only two unique products certified only to these criteria and not to the ''transitions of care'' criterion at the time of the drafting of the Proposed Rule, there appears to be little market demand for certification to 2015 Edition ''Common Clinical Data Set summary record—create'' (§ 170.315(b)(4)) and ''Common Clinical Data Set summary record—receive'' (§ 170.315(b)(5)) criteria alone. Therefore, we proposed to remove these certification criteria from the 2015 Edition.

Comments. The comments we received on this proposal supported this removal.

Response. We thank commenters for their support and have finalized removal of the 2015 Edition ''Common Clinical Data Set summary record—create'' (§ 170.315(b)(4)) and ''Common Clinical Data Set summary record—receive'' (§ 170.315(b)(5)) criteria.

e. Secure Messaging

We proposed to remove the 2015 Edition ''secure messaging'' criterion (§ 170.315(e)(2)). As explained in the Proposed Rule (84 FR 7437), ONC strongly supports patient and provider communication, as well as protecting the privacy and security of patient information, but no longer believes that a separate certification criterion focused

on a health IT's ability to send and receive secure messages between health care providers and patients is necessary. This criterion would also no longer be associated with an objective or measure under the CMS PI Programs based on proposals and determinations in recent CMS rulemakings (83 FR 41664; 83 FR 35929).

Comments. Several comments specifically referencing this proposal were supportive of removing this criterion. A number of commenters expressed concern with the removal of the ''secure messaging'' criterion, including whether removal of this criterion may create a barrier to successful participation for providers in the CMS PI Programs. Other commenters expressed concerns about continued availability of secure digital endpoints for health care providers. Some commenters noted that some providers and patients might prefer to continue using ''secure messaging'' functionality in lieu of other options for a variety of purposes for which they currently use it, while others expressed concern that the separate ''secure messaging'' functionality will disappear from the market if no longer supported by ONC requirements. Commenters expressed that options for data access and exchange, such as portals and APIs, might satisfy providers' and patients' needs for interoperable communication. However, commenters expressed a concern that these options may not ensure continued availability to new market entrants' health IT without requiring the technology to interact with developer- or system-specific interfaces.

Response. We thank commenters for their input. Having reviewed all comments received on this proposal, we have decided not to remove the ''secure messaging'' criterion from the Program at this time. We recognize the importance of ensuring alignment between ONC Health IT Certification Program regulations and the CMS regulations that reference them. We will continue to work in close partnership with our CMS colleagues to ensure that our regulations remain aligned and that we provide affected stakeholders with the information they need to understand how the rules work together and how to succeed under CMS incentive programs using health IT certified under ONC's Program. CMS has identified this criterion as supporting the coordination of care through patient engagement objective and measure, which is expected to remain operational for Medicaid until January 1, 2022; after 2021 there will be no further incentives under the Medicaid Promoting Interoperability Program (84 FR 42592). We, therefore, will permit ONC–ACBs to issue certificates for this criterion up until January 1, 2022 to align with the requirements of the CMS Medicaid PI Program (84 FR 42592). We have included a provision in § 170.550(m)(1) to only allow ONC–ACBs to issue certificates for this criterion until January 1, 2022.

Limiting certificates to this criterion for this period will help spur further innovations in patient engagement while helping to reduce regulatory burdens and costs for health IT developers and health care providers. The other 2015 Edition certification criteria that support patient engagement, such as the 2015 Edition ''view, download, and transmit to 3rd party,'' ''API,'' and ''patient health information capture'' certification criteria better support interoperability and innovation in patient engagement. We have seen developers integrate secure messaging functionality as part of other patient engagement features, such as patient portals, and integrate messaging with access to and exchange of clinical and administrative data. These integrated technologies currently in use offer more comprehensive options for providers and patients to interact and share information via a secure platform and may render the separate ''secure messaging'' criterion and functionality redundant to robust integrated options. We also believe removing the standalone ''secure messaging'' criterion will encourage the market to pursue other innovative means of offering patient engagement and interaction functionalities that providers and patients want, with the convenience and efficiency they demand. Thus, we believe that the removal of this criterion will help reduce burden and costs without negative impact on current or future innovations in patient engagement and secure information exchange. In response to the concern about new market entrants being able to receive data needed to serve their customers, we note that the ''view, download, and transmit to 3rd party'' criterion remains available for patients who wish to send their health information to a third party of the patient's choice. Other remaining interoperability-focused criteria, such as ''transitions of care,'' ensure that systems of health IT certified to at least those criteria remaining in the ''Base EHR'' definition will remain capable of supporting providers' use of new entrant and other third party health IT of their choosing without requiring that health IT to integrate or interface with their certified health IT.

5. Removal of Certain ONC Health IT Certification Program Requirements

We proposed to remove certain mandatory disclosure requirements and a related attestation requirement under the Program. As discussed in the Proposed Rule (84 FR 7437), we believe removal of these requirements will reduce costs and burden for Program stakeholders, particularly for health IT developers and ONC–ACBs.

a. Limitations Disclosures

We proposed to remove § 170.523(k)(1)(iii)(B), which requires ONC–ACBs to ensure that certified health IT includes a detailed description of all known material information concerning limitations that a user may encounter in the course of implementing and using the certified health IT, whether to meet ''meaningful use'' objectives and measures or to achieve any other use within the scope of the health IT's certification. We proposed to remove § 170.523(k)(1)(iv)(B) and (C), which state that the types of information required to be disclosed include, but are not limited to: (B) Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified; (C) limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

Comments. Most of the comments specifically referencing this proposal were supportive. A few commenters raised concerns regarding the utility of mandatory disclosures to health care providers, their health information exchange partners, and ONC, with some commenters offering suggestions for how ONC could use disclosures information in the future. A few commenters' concerns specifically referenced the disclosure of costs information.

Response. We thank commenters for their input. We have finalized removal of § 170.523(k)(1)(iii)(B) and § 170.523(k)(1)(iv)(B) and (C), as proposed (84 FR 7437 and 7438). As

discussed in the Proposed Rule (84 FR 7438), these specific disclosure requirements are superseded by the Cures Act information blocking provision and Conditions of Certification requirements, which we proposed to implement in the same Proposed Rule (84 FR 7424). As also noted in the Proposed Rule (84 FR 7438), we proposed (84 FR 7465 and 7466) a complementary Condition of Certification requirement that developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification discussed further in section VII.2.

We also note here to ensure clarity that we did not propose, and have not finalized, a complete removal of the transparency requirements in § 170.523(k)(1). Requirements under § 170.523(k)(1) *other than* those specifically proposed for removal will remain in place. The transparency requirements remaining in place include: § 170.523(k)(1)(iii)(A), which describes the plain language detailed description of all known material information concerning additional types of costs that a user may be required to pay to implement or use the Complete EHR or Health IT Module's capabilities, whether to meet meaningful use objectives and measures, or to achieve any other use within the scope of the health IT's certification; and § 170.523(k)(1)(iv)(A) specification that the types of information required by § 170.523(k)(1)(iii) include, but are not limited to, additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

b. Transparency and Mandatory Disclosures Requirements

We proposed to remove the Principle of Proper Conduct (PoPC) in § 170.523(k)(2), which requires ONC–ACBs to ensure health IT developers' adherence to a requirement that the health IT developer submit an attestation that it will disclose all of the information in its mandatory disclosures per § 170.523(k)(1) to specified parties (*e.g.,* potential customers or anyone inquiring about a product quote or description of services). As discussed in the Proposed Rule (84 FR 7438), we believe this provision is no longer necessary and that its removal is appropriate to further reduce administrative burden for health IT developers and ONC–ACBs.

Comments. The majority of commenters specifically discussing this proposal expressed support for the removal of the PoPC in § 170.523(k)(2). A few commenters expressed concern that the high degree of transparency ONC noted in the Proposed Rule might not be maintained as they noted a possibility that the PoPC requiring the ONC–ACBs to ensure the developers submitted an attestation, and, in turn, the developers' obligation to make the attestation, may be driving the currently observed levels of transparency.

Response. We thank commenters for their input. We have decided to finalize the removal of the PoPC in § 170.523(k)(2). We appreciate the importance of holding health IT developers accountable for meeting all requirements of participation in the Program, including meeting or exceeding the minimum required transparency disclosures. We believe that the needed transparency and accountability will be maintained and enhanced by certain Condition and Maintenance of Certification requirements we have finalized in this rule, which include the assurances and attestations specifically discussed in section VII.2 in relation to this proposed removal of § 170.523(k)(2). We believe that the removal of the PoPC requirements in § 170.523(k)(2) will likely aid in the avoidance of unnecessary costs and burden for Program stakeholders, particularly health IT developers and ONC–ACBs.

6. Recognition of Food and Drug Administration Processes

Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA), Public Law 112–144, required that the Food and Drug Administration (FDA), in consultation with ONC and the Federal Communications Commission (FCC) (collectively referred to as ''the Agencies'' [18] for this final rule), develop a report containing a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health IT, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication. The FDASIA Health IT Report of April 2014,[19] contained a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health IT that promotes innovation, protects patient safety, and avoids regulatory duplication. Public comments, received prior to the report's publication and after,[20] recommended that health IT developers/manufacturers apply a single process that satisfies the requirements of all agencies, and existing safety and quality-related processes, systems, and standards should be leveraged for patient safety in health IT. On July 27, 2017, FDA announced a voluntary Software Precertification Pilot Program as part of a broader Digital Health Innovation Action Plan.[21] It was developed in order to create a tailored approach toward recognizing the unique characteristics of digital technology by looking first at the firm, rather than primarily at each product of the firm, as is currently done for traditional medical products. The FDA plans to explore whether and how pre-certified companies that have demonstrated a culture of quality, patient safety, and organizational excellence could bring certain types of digital health products to market either without FDA premarket review or with a more streamlined FDA premarket review.

a. FDA Software Precertification Pilot Program

We proposed (84 FR 7438 and 7439) to establish processes that would provide health IT developers that can document holding pre-certification under the FDA Software Precertification Pilot Program with exemptions to the ONC Health IT Certification Program's requirements for testing and certification of its health IT to the 2015 Edition ''quality management systems'' criterion (§ 170.315(g)(4)) and the 2015 Edition ''safety-enhanced design'' criterion (§ 170.315(g)(3)), as these criteria are applicable to the health IT developer's health IT presented for

[18] ONC is not an agency, but an office within the Department of Health and Human Services.

[19] *https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf.*

[20] *https://www.federalregister.gov/documents/2013/05/30/2013-12817/food-and-drug-administration-safety-and-innovation-act-fdasia-request-for-comments-on-the, https://blogs.fda.gov/fdavoice/index.php/2014/04/fda-seeks-comment-on-proposed-health-it-strategy-that-aims-to-promote-innovation/* and *https://www.regulations.gov/document?D=FDA-2014-N-0339-0001.*

[21] *https://www.fda.gov/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/Default.htm.*

certification. We also stated that such a ''recognition'' could, depending on the final framework of the FDA Software Precertification Pilot Program, be applicable to the functionally-based 2015 Edition ''clinical'' certification criteria (§ 170.315(a)). We noted in the Proposed Rule that the proposed ''recognition'' could also be appropriate to address any or all of the following functionally-based 2015 Edition criteria in the event their proposed removal were not finalized: ''problem list'' (§ 170.315(a)(6)), ''medication list'' (§ 170.315(a)(7)), ''medication allergy list'' (§ 170.315(a)(8)), ''drug-formulary and preferred drug list checks'' (§ 170.315(a)(10)),'' and ''smoking status'' (§ 170.315(a)(11)).

We noted (84 FR 7439) that despite proffered benefits including alignment with both EOs 13563 and 13771 regarding deregulatory, less burdensome, and more effective regulatory schemes and programs, and serving as a regulatory relief for those health IT developers qualifying as small businesses under the Regulatory Flexibility Act (84 FR 7587 and 7588), there may be reasons not to adopt such a ''recognition'' approach. We noted as examples of such reasons that stakeholders may not agree that the FDA Software Precertification Program sufficiently aligns with our Program, and that stakeholders may have operational concerns. Accordingly, we welcomed comments on these and other aspects of our proposed ''recognition'' approach, including the 2015 Edition certification criteria that should be eligible for ''recognition.''

Comments. The majority of commenters commended ONC's efforts to recognize the FDA Software Precertification Program. However, most commenters expressed concerns that FDA's program was not yet mature enough to assess the degree of alignment to the ONC Health IT Certification Program. Many commenters expressed concerns that the FDA Software Precertification Pilot Program focuses on development and business practices, with a potential for streamlining requirements for pre-market clearance of specific functionalities, while ONC's certification Program focuses less on development practices and more on certification of individual software products as meeting Program-specified requirements for functionality and interoperability, including conformance with specific interoperability standards. Many of these commenters indicated that until the FDA program is more fully mature they would prefer to reserve judgment on how recognition could or should be structured to satisfy the needs of ONC's Program at lower burden on those developers for whom dual participation is a need or an appealing option. Several commenters noted potential for recognition of developers who achieve precertification status under the FDA's program to streamline or offer them a low-burden option for satisfying certain requirements under ONC's Program. However, several commenters urged that obtaining FDA precertification status should not be the only way a developer could satisfy any requirement under ONC's Program, noting that a developer of one or more certified Health IT Modules that is newer to the market or simply smaller and not engaged in development of software subject to FDA regulation could find the FDA Software Precertification Program's requirements a higher hurdle to entering or remaining in the ONC-certified health IT market sector than the ONC requirements the recognition might replace.

Response. Considering commenters' concerns and the maturity of the FDA Software Precertification Program—which remains in a pilot phase at the time this final rule is being drafted—we have decided not to finalize recognition of the FDA Software Precertification Program at this time. However, we anticipate continuing to consult and coordinate with our colleagues at FDA and to monitor the details and experience of the FDA Software Precertification Program as it continues to mature. We continue to believe that there may be potential for recognition of the FDA Software Precertification Program to contribute in the future to our ongoing goals of reducing burden and promoting innovation while maintaining or enhancing the assurance that the ONC Health IT Certification Program provides, but we have not finalized our proposal at this time.

b. Development of Similar Independent Program Processes—Request for Information

In the Proposed Rule (84 FR 7439), we included a request for information (RFI) related to the development of similar independent processes to those of the FDA Software Precertification Program for purposes of our Program. We received 21 comments on this RFI and appreciate the input provided by commenters. We will continue to consider whether to develop similar independent processes and whether this should be included in future rulemaking.

IV. Updates to the 2015 Edition Certification Criteria

In order to capture and share patient data efficiently, health care providers need health IT that store data in structured formats. Structured data allows health care providers to easily retrieve and transfer patient information, and use health IT in ways that can aid patient care. We proposed to update the 2015 Edition by adopting a limited set of revised and new 2015 Edition certification criteria, including new standards, to support these objectives. Some of these criteria and standards are included in the Certified EHR Technology (CEHRT) definition used for participation in HHS Programs, such as the Promoting Interoperability (PI) Programs (formerly the EHR Incentive Programs), some are required to be met for participation in the ONC Health IT Certification Program, and some, though beneficial, are unassociated with the CEHRT definition and not required for participation in any HHS program, including the ONC Health IT Certification Program (Program).

Comments. We received a few comments in support of our approach to modify the 2015 Edition health IT certification criteria. One commenter commended ONC for proposing logical updates to the 2015 Edition certification criteria, rather than overhauling the Program or establishing a new edition of certification, stating iterative changes will provide stability and allow the industry to adapt to new market forces. Commenters stated that this incremental approach best serves the health care provider and health IT developer community. One commenter applauded ONC for proposing logical updates to the 2015 Edition health IT certification criteria and recommended that ONC continue to seek to maximize the impact of these certification changes and pursue all opportunities to simplify existing criteria.

However, a number of commenters requested that ONC put forth a new edition and suggested varied approaches to a new edition. Commenters suggested that ONC clearly delineate the difference between the editions by creating a new naming convention for the updated criteria, such as a version number. Others recommended a 2020 Edition or the corresponding year in which this rule is effective. Still other commenters recommended the proposed updated 2015 Edition be renamed to the 2021 Edition instead of renamed with a Release 2 at end of the existing name. Some commenters identified the scope of the proposed

changes as the reason ONC should establish the updates as a new edition of certification criteria rather than simply updating the 2015 Edition. However, the majority of commenters recommending a new edition based their concern on the potential confusion among providers who purchase and use certified health IT resulting from different products available under the same label.

Response. We thank commenters for their input on the tradeoffs associated with modifying the current 2015 Edition versus creating a new edition. We considered a variety of factors when we framed our proposals. First, we reviewed the scope of each proposed update and the cumulative scope of the proposals overall for health IT developers and sought to identify whether it would be more appropriate to require health IT developers participating in the Program to implement updates to Health IT Modules certified to the 2015 Edition or to test and certify health IT products to an entirely new edition of certification criteria. Second, we considered the impact that either approach would have on health care providers, including how such updated Health IT Modules or products certified to a new edition would be implemented by providers participating in CMS programs.

We have considered the impact on health IT developers related to the scope of the individual updates as well as the cumulative scope of all updates to the 2015 Edition adopted in this final rule (see also section XIII Regulatory Impact Analysis). In this final rule, we have only adopted two new technical certification criteria in § 170.315(b)(10) and § 170.315(g)(10) to which health IT developers seeking to upgrade their products will need to present Health IT Modules for certification. Unlike the new criteria introduced in prior certification edition rulemakings, both of these new criteria are an expansion or modification of existing criteria within the 2015 Edition which are currently in use in certified health IT. The new criteria in § 170.315(b)(10) relates to the 2015 Edition criteria in § 170.315(b)(6) with an expansion of the data and a removal of the specificity for the standard requirement. The new Standardized API criteria in § 170.315(g)(10) relates to the 2015 Edition API criteria with an expansion of security requirements and the addition of applicable standards. For the remainder of the updated criteria, a developer would not be required to present a Health IT Module for certification in order to update a certified product in accordance with this final rule. Instead, a health IT developer would update their certified Health IT Module, notify the ONC–ACB that they have done so, and make the update available their customers. Additionally, unlike prior certification edition rulemakings, the certification criteria updated to address compliance with the USCDI do not include new functionality nor do they require a complete redesign of Health IT Modules certified to such certification criteria. As noted in the Proposed Rule, the updates to the CCDS to create the USCDI were intentionally limited to a modest expansion that most health IT developers already supported, were already working toward, or should be capable of updating their health IT to support in a timely manner. Please see Table 1 for a list of all certification criteria changes.

In consideration of the impact our approach would have on health care providers, we note that impact and potential burden for providers is of particular importance given that CY2019 was the first performance year where eligible clinicians (ECs), eligible hospitals, dual-eligible hospitals, and critical access hospitals (CAHs) participating in CMS programs—including the CMS Promoting Interoperability Program and the Quality Payment Program/Merit-based Incentive Payment System—were required to use health information technology certified to the 2015 Edition to meet the requirements of the CMS CEHRT definition. If we were to adopt a new edition of certification criteria, CMS programs would have to consider establishing a new CEHRT definition and a subsequent requirement for program participants who have only recently completed a full edition update to their technology used for program participation. Historically, with a new edition of certification criteria, health IT developers have packaged Health IT Modules certified to new, modified, and unchanged criteria into a wholly new certified product. Historical data indicates that these complete updates to the edition are particularly challenging for both health IT developers seeking certification and for health care providers as they place deadlines for a significant number of health IT developers to support and implement new products for a significant number of health care providers simultaneously. As a result, the burden of updating the technology is compounded for both health IT developers and health care providers. While ONC does not itself place any such requirements on health care providers, we believe the risk of such significant burden must be considered in health IT policy decisions.

Further, we believe the scope of the updates and the impact on health IT developers and health care providers must be considered in tandem—meaning that an entirely new edition should only be established when the scope of the updates is significant enough to warrant the impacts of implementation. When the scope of updates does not warrant implementation of an entirely new edition of certification criteria, we believe it is appropriate to update the existing criteria. For example the 2015 Edition included new criteria that were neither built upon nor updated to existing criteria in the 2014 Edition, which was significantly different than the 2011 Edition. In contrast, health IT developers have been able to employ regular or cyclical updates without modifying all Health IT Modules certified to unchanged criteria in order to implement updates to existing certification criteria such as the annual updates to CMS eCQMs or for changes made to public health reporting standards. In such cases, the changes may be implemented by health IT developers in the manner most appropriate for their product and their customers, such as through routine service and maintenance rather than a completely new implementation.

In order to understand the impact these updates would have on participants in the CMS programs which reference them for use by program participants, we compare these updates to the current definition of CEHRT established by CMS at 42 CFR 495.4 for eligible hospitals, CAHs and Medicaid eligible professionals and at 42 CFR 414.1305 for eligible clinicians in MIPS. For 2019 and subsequent years, the CMS CEHRT definition specifies the use of EHR technology certified to 2015 Edition including technology that meets the 2015 Edition Base EHR definition in § 170.102, as well as other certified technology necessary to be a meaningful user. The updates finalized in this final rule impact both certification criteria included in the Base EHR definition as well as criteria required for applicable objectives and measures. Specifically, this final rule updates several criteria currently applicable for certified Health IT Modules used by CMS program participants for the CMS objectives and measures necessary to be a meaningful user, including:

- Revisions to the electronic prescribing criterion in § 170.315(b)(3) to reference an updated e-prescribing standard;

- Revisions relating to the drug-formulary and preferred drug list checks criterion in § 170.315(a)(10) to include at 170.550(m)(1) to only allow ONC–ACBs to issue certificates for this criterion until January 1, 2022;
- Replacement of the API criterion in § 170.315(g)(8) with a new API criterion in § 170.315(g)(10) referencing an API standard and related security standards;
- Revisions to several criteria to reference the USCDI and implement other standards updates (see Table 1 for specifics); and
- Revisions to § 170.315(c)(3), to update quality reporting standards.

In general, health IT developers have 24 months from the publication date of the final rule to make technology certified to these updated criteria available to their customers, and during this time developers may continue supporting technology certified to the prior version of certification criteria for use by their customers. For providers participating in CMS programs, this means they can continue to use the certified technology they have available to them to support program participation and can work with their developers to implement any updates in a manner that best meets their needs.

For the revisions to electronic prescribing criterion in § 170.315(b)(3) and to the quality reporting standards, in § 170.315(c)(3), the updates adopted for certified health IT align specifically with changes already required by CMS for use by health care providers. This means health IT developers are already implementing and supporting these updates. The implementation of these updates is driven by other requirements and so repackaging such updates in a new edition (or a new product) would create a redundancy and could have unintended cost burden on health care providers. For the updates to the criteria referencing the USCDI, as noted previously, we based the USCDI on the existing CCDS with modest expansion that most health IT developers already supported, were already working toward, or should be capable of updating their health IT to support in a timely manner. Finally, for the removal of the drug-formulary and preferred drug list checks in § 170.315(a)(10), we note that the removal from the Program has negligible impact on health care providers.

First, as discussed in past CMS regulations related to the use of these functionalities by participants in CMS programs, health care providers have noted that while formulary checks are a promising approach, the utility of the specific functionality that is certified is not necessarily consistently applicable for all prescriptions (80 FR 62833). Second, as it does not remove the product from the market, any providers who are using the current functionality may continue to use the technology for their purposes. For the replacement of the API criterion in § 170.315(g)(8) with a new Standardized API criterion in § 170.315(g)(10) referencing an API standard and related security standards, we reiterate that health IT developers have 24 months from the date of publication of this final rule to update their technology and make such available to their customers. The 2015 Edition final rule adopted an API criterion in § 170.315(g)(8) which was implemented by many health IT developers using the underlying standard adopted in this final rule for the Standardized API criterion in § 170.315(g)(10). This common use impacted our decision to adopt the standard in our update to the 2015 Edition (*see* also section VII.B.4.c Standardized API for Patient and Population Services). We, therefore, believe that both the scope of the updates and the potential impact on health IT developers and health care providers do not constitute sufficient justification for the potential burden associated with adopting an entirely new edition of certification criteria. Instead, we believe it is most reasonable and effective for these updates to be part of the existing 2015 Edition as modified in this final rule.

We acknowledge the concerns of commenters who expressed the potential risk of confusion about the updates among their customers and how to best communicate that a product meets the updated version of a given certification criterion. We strongly encourage health IT developers to work with their customers to promote understanding of these updates. In addition, we have taken several mitigating steps. First, we revisited our proposed regulatory structure and revised it so that the structure more clearly reflects if a change is updating the previously adopted standard, or a more significant change to the criterion such as adding a new standard. This maintains the prior 2015 Edition regulatory structure for the majority of the updates except for § 170.315(b)(10) and (g)(10) as discussed previously, and establishes a more clear sense of scope.

Second, in order to support effective communication of the updates, we are implementing a practical approach to facilitate transparency using the Certified Health IT Product List (CHPL),[22] which is the tool that health care providers and the general public may use to identify the specific certification status of a product at any given time, to explore any certification actions for a product, and to obtain a CMS Certification ID for a product used when participating in CMS programs. While we retain the overall 2015 Edition title, we will distinguish the 2015 Edition certification criteria from the new or revised criteria adopted in this final rule by referring to the new or revised criteria as the 2015 Edition Cures Update on the CHPL for products that are certified. The CHPL will also differentiate to what standards the health IT will be certified and will allow health care providers to identify if and when a specific Health IT Module has been updated. This will help to eliminate some of the confusion among providers who are seeking to understand the certification and update the status of the product they are currently using. It can also be a resource for providers who may be making a new purchase of certified health IT to make an informed decision about which products support the most up to date available standards and functionality.

We further note that, while in the past ONC has largely relied on creating a new edition to implement changes to certification criteria, in each case, those changes included some updates to existing criteria, but also criteria containing functionality and standards that were entirely new and did not build on the prior edition. In addition, the Cures Act set in motion a shift for the ONC Health IT Certification Program by including Conditions and Maintenance of Certification requirements which allowed for processes such as the Standards Version Advancement Process (SVAP) flexibility within real world testing, which allows better alignment to industry efforts for standards advancement while maintaining accountability. These new provisions help to remove barriers for standards development and version updates, which limit a health IT developer's ability to provide individually relevant, timely, and innovative solutions to their clients. This change is consistent with our approach to adopt incremental updates in this final rule rather than to adopt a complete new edition of certification criteria. This final rule is the first time we have executed on the concept of Maintenance of Certification requirements for existing certificates, and we foresee the potential for future

[22] ONC Certified Health IT Product List: *https://chpl.healthit.gov.*

rulemakings to include incremental updates to certification criteria when such updates are appropriate.

Please see Table 1 for a list of all certification criteria changes.

TABLE 1—2015 EDITION CURES UPDATE

Certification criteria	Reference	New/revised/ removed/time-limited certification	2015 Edition cures update—timing	Impact on CMS promoting interoperability (PI) programs
Problem list	§ 170.315(a)(6)	Removed	Effective date of final rule (60 days after publication).	Removed from 2015 Edition Base EHR definition.
Medication list	§ 170.315(a)(7)	Removed	Effective date of final rule (60 days after publication).	Removed from 2015 Edition Base EHR definition.
Medication allergy list	§ 170.315(a)(8)	Removed	Effective date of final rule (60 days after publication).	Removed from 2015 Edition Base EHR definition.
Drug Formulary and Preferred Drug List Checks.	§ 170.315(a)(10)	Time-limited Certification.	ONC–ACBs only permitted to issue certificates for this criterion until January 1, 2022.	PI Measures: —e-Rx —-Query of PDMP Operational for Medicaid until January 1, 2022.
Smoking status	§ 170.315(a)(11)	Removed	Effective date of final rule (60 days after publication).	Removed from 2015 Edition Base EHR definition.
Patient-specific Education Resource.	§ 170.315(a)(13)	Time-limited Certification.	ONC–ACBs only permitted to issue certificates for this criterion until January 1, 2022.	Operational for Medicaid until January 1, 2022 Supports Patient Electronic Access to Health Information Objective Measure.
Transitions of Care	§ 170.315(b)(1)	Revised	Update to USCDI/C–CDA companion guide within 24 months after the publication date of final rule.	PI Measures: —Support Electronic Referral Loops by Sending Health Information —Support Electronic Referral Loops by Receiving and Incorporating Health Information.
Clinical information reconciliation and incorporation.	§ 170.315(b)(2)	Revised	Update to USCDI/C–CDA companion guide within 24 months after the publication date of final rule.	PI Measures: —Support Electronic Referral Loops by Receiving and Incorporating Health Information.
Electronic prescribing	§ 170.315(b)(3)	Revised	Update standard within 24 months after the publication of final rule.	PI Measures: —e-Prescribing.
Common Clinical Data Set summary record—create.	§ 170.315(b)(4)	Removed	Effective date of final rule (60 days after publication).	
Common Clinical Data Set summary record—receive.	§ 170.315(b)(5)	Removed	Effective date of final rule (60 days after publication).	
Data Export	§ 170.315(b)(6)	Time-limited Certification.	ONC–ACBs may only issue certificates until 36 months after the publication date of the final rule.	Removed from 2015 Edition Base EHR definition effective date of the final rule (60 days after publication).
Security tags—summary of care—send.	§ 170.315(b)(7)	Revised	Document, section, and entry (data element) level; or Document level for the period until 24 months after publication date of final rule.	
Security tags—summary of care—receive.	§ 170.315(b)(8)	Revised	Document, section, and entry (data element) level; or Document level for the period until 24 months after publication date of final rule.	
Care plan	§ 170.315(b)(9)	Revised	Update to C–CDA companion guide within 24 months after publication date of final rule.	
EHI export	§ 170.315(b)(10)	New	Update within 36 months of publication date of final rule.	
Clinical quality measures (CQMs)—report.	§ 170.315(c)(3)	Revised	Effective date of final rule (60 days after publication).	PI Programs.
Auditable events and tamper-resistance.	§ 170.315(d)(2)	Revised	Update to new ASTM standard within 24 months after publication date of final rule.	
Audit report(s)	§ 170.315(d)(3)	Revised	Update to new ASTM standard within 24 months after publication date of final rule.	
Auditing actions on health information.	§ 170.315(d)(10)	Revised	Update to new ASTM standard within 24 months after publication date of final rule.	
Encrypt authentication credentials.	§ 170.315(d)(12)	New	Effective date of final rule (60 days after publication) (New and updated certifications only).	
Multi-factor authentication (MFA).	§ 170.315(d)(13)	New	Effective date of final rule (60 days after publication) (New and updated certifications only).	
View, Download, and Transmit to 3rd Party.	§ 170.315(e)(1)	Revised	Update to USCDI/C–CDA companion guide within 24 months after publication date of final rule.	PI Measure: —Provide Patients Electronic Access to Their Health Information.
Secure Messaging	§ 170.315(e)(2)	Time-limited Certification.	ONC–ACBs only permitted to issue certificates for this criterion until January 1, 2022.	Operational for Medicaid until January 1, 2022 Supports the Coordination of Care through Patient Engagement Objective.
Transmission to public health agencies—electronic case reporting.	§ 170.315(f)(5)	Revised	Update to USCDI/C–CDA companion guide within 24 months after publication date of final rule.	PI Measure: —Electronic Case Reporting.
Consolidated CDA creation performance.	§ 170.315(g)(6)	Revised	Update to USCDI/C–CDA companion guide within 24 months after publication date of final rule.	
Application Access—Data Category Request.	§ 170.315(g)(8)	Time-limited Certification.	24 months after publication date of final rule	PI Measure: —Provide Patients Electronic Access to Their Health Information.

TABLE 1—2015 EDITION CURES UPDATE—Continued

Certification criteria	Reference	New/revised/ removed/time-limited certification	2015 Edition cures update—timing	Impact on CMS promoting interoperability (PI) programs
Application Access—All Data Request.	§ 170.315(g)(9)	Revised	Update to USCDI/C–CDA companion guide within 24 months after publication date of final rule.	PI Measure: —Provide Patients Electronic Access to Their Health Information.
Standardized API for patient and population services.	§ 170.315(g)(10) ...	New	Update within 24 months of publication date of final rule.	Added to the 2015 Edition Base EHR definition.

Note: The CHPL will be updated to indicate the standards utilized for new or revised certification criteria, as well as denote criteria removed from the Program.

A. Standards and Implementation Specifications

1. National Technology Transfer and Advancement Act

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et. seq.*) and the Office of Management and Budget (OMB) Circular A–119 [23] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to electing only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. Agencies have the discretion to decline the use of existing voluntary consensus standards if determined that such standards are inconsistent with applicable law or otherwise impractical, and instead use a government-unique standard or other standard. In addition to the consideration of voluntary consensus standards, the OMB Circular A–119 recognizes the contributions of standardization activities that take place outside of the voluntary consensus standards process. Therefore, in instances where use of voluntary consensus standards would be inconsistent with applicable law or otherwise impracticable, other standards should be considered that meet the agency's regulatory, procurement or program needs, deliver favorable technical and economic outcomes, and are widely utilized in the marketplace.

Comments. A couple of commenters stated that they do not support Federal programs' use of the NTTAA voluntary consensus standards exceptions, and asked that the involved Federal programs continue to utilize consensus-based standards developed through work done by organizations such as HL7®. They noted that such work incorporates public health inputs, and stated that it is critical for there to be sufficient discussion and consideration of all stakeholder concerns in adopting such critical technologies such as FHIR®.

Response. We thank commenters for their feedback. We clarify that many of the standards we adopt in this final rule are developed and/or adopted by voluntary consensus standards bodies, except where we found that a government unique standard is more appropriate. We are aware of no voluntary consensus standards that could serve as an alternative for the following purposes in this final rule.

In this final rule, we use voluntary consensus standards except for:

- The standard adopted in § 170.213, the United States Core Data for Interoperability (USCDI), Version 1 (v1), is a hybrid of government unique policy (*i.e.,* determining which data to include in the USCDI) and voluntary consensus standards (*i.e.,* the vocabulary and code set standards attributed to USCDI data elements). We have placed time limitations on the predecessor to this standard, the Common Clinical Data Set (CCDS) definition, under this rule, and replaced it with the USCDI in all applicable criteria except for the data export criterion in § 170.315(b)(6), on which we have also placed a time limit. We refer readers to the ''Revised and New 2015 Edition Criteria'' in section IV.B of this preamble.
- The standards adopted in § 170.205(h)(3) and (k)(3). We replaced the current HL7® QRDA standards with government unique standards, the CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2019, and the CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2019, that will more effectively support the associated certification criterion's use case, which is reporting electronic clinical quality measure (eCQM) data to CMS.

2. Compliance With Adopted Standards and Implementation Specifications

In accordance with Office of the Federal Register regulations related to ''incorporation by reference,'' 1 CFR part 51, which we follow when we adopt proposed standards and/or implementation specifications in a final rule, the entire standard or implementation specification document is deemed published in the **Federal Register** when incorporated by reference therein with the approval of the Director of the Federal Register. Once published, compliance with the standard and/or implementation specification includes the entire incorporated document, unless we specify otherwise. For example, for the HL7® FHIR U.S. Core Implementation Guide (IG) STU 3.1.0 adopted in this final rule (*see* section VII.B.4), health IT certified to certification criteria referencing this IG would need to demonstrate compliance with all mandatory elements and requirements of the IG. If an element of the IG is optional or permissive in any way, it would remain that way for testing and certification *unless* we specified otherwise in regulation. In such cases, the regulatory text would preempt the permissiveness of the IG.

3. ''Reasonably Available'' to Interested Parties

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies propose to incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5(b)). To comply with these requirements, in section XI (''Incorporation by Reference'') of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we have adopted and subsequently incorporate by reference in the Code of Federal Regulations. To note, we also provide relevant information about these standards and implementation specifications

[23] *https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A119/revised_circular_a-119_as_of_1_22.pdf.*

throughout the relevant preamble policy discussions and regulation text sections of the final rule.

B. Revised and New 2015 Edition Criteria

1. The United States Core Data for Interoperability Standard (USCDI)

As we noted in the Proposed Rule, the initial focus of the Program was to support the Medicare and Medicaid EHR Incentive Programs (76 FR 1294) now referred to as the Promoting Interoperability (PI) Programs. As such, the 2014 Edition certification criteria mirrored those functions specified by the CMS PI Programs objectives and measures for providers demonstrating meaningful use (MU) of certified health IT. In order to improve efficiency and streamline the common data within our Program's certification criteria, we created a single definition for all the required data that could be referenced for all applicable certification criteria. We created the term ''Common MU Data Set'' to encompass the common set of MU data types/elements (and associated vocabulary standards) for which certification would be required across several certification criteria (77 FR 54170).

The 2015 Edition final rule modified the Program to make it open and accessible to more types of health IT, and health IT that supports various care and practice settings beyond those included in the CMS PI Programs (80 FR 62604). In comparison to the previous editions, the 2015 Edition focused on identifying health IT components necessary to establish an interoperable nationwide health information infrastructure, fostering innovation and opening new market opportunities, and allowing for more health care provider and patient choices in electronic health information access and exchange. In order to align with this approach, we made changes in the 2015 Edition final rule that resulted in updated vocabulary and content standards to improve and advance interoperability and health information exchange (80 FR 62604). The 2015 Edition final rule further expanded accessibility and availability of data exchanged by updating the definition of Base EHR in the 2015 Edition to include enhanced data export, transitions of care, and application programming interface (API) capabilities, all of which previously required that, at a minimum, the CCDS be available (80 FR 62602 through 62604).

We further noted in the Proposed Rule (84 FR 7440) that the regulatory approach to using and referencing a ''definition'' to identify electronic health information, for access, exchange and use, including associated vocabulary codes, has had its drawbacks. While ONC's ''CCDS'' definition served its designed purpose (to reduce repetitive text in each of the certification criteria in which it is referenced), the term CCDS, and the data set it represents, also began to be used by outside organizations such as the Argonaut Project [24] for additional use cases beyond the C–CDA and ONC's Health IT Certification Program. As these organizations identified the need to expand the content of the CCDS, the CCDS definition in regulation became a limitation to developing additional data access, exchange, and uses outside of ONC's programs. As we move towards value-based care and the inclusion of Data Classes that go beyond clinical data, and as part of ONC's continued efforts to evaluate the availability of a minimum baseline of Data Classes that must be commonly available for interoperable exchange, we acknowledge the need to change and improve our regulatory approach to the CCDS. Therefore, in order to advance interoperability by adopting new data and vocabulary codes sets that support data exchange, we proposed to remove the ''Common Clinical Data Set'' in § 170.315(b)(4) and § 170.315(b)(5), and its references throughout the 2015 Edition and replace it with the ''United States Core Data for Interoperability'' (USCDI) standard. This first version of USCDI will be designated ''version 1 (v1).'' The USCDI standard aims to achieve the goals set forth in the Cures Act by specifying a common set of data classes and elements that have been designed to improve data usage and interoperable data exchange.

We proposed to adopt the USCDI v1 as a standard defined in § 170.102. Here, ''Standard'' is defined as a ''technical, functional, or performance-based rule, condition, requirement, or specification that stipulates instructions, fields, codes, data, materials, characteristics, or actions.'' The USCDI standard would be composed of Data Classes, which may be further delineated into groupings of specific Data Element(s). For example, ''patient demographics'' is a Data Class, and within that Data Class there is ''patient name,'' which is a Data Element. As noted in section IV.B.1.b, for the overall structure and organization of the USCDI, please consult *www.healthIT.gov/USCDI.*

We noted in the Proposed Rule (84 FR 7441) that ONC intended to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. We indicated that once the Secretary adopts the first version of the USCDI through rulemaking, which we proposed in § 170.213 in the Proposed Rule, health IT developers would be allowed to take advantage of the ''Standards Version Advancement Process'' (SVAP) flexibility. The SVAP (which we proposed in § 170.405(b) and which is discussed in section VII.B.5, below) would permit health IT developers to voluntarily implement and use a newer version of a Secretary-adopted standard such as the USCDI, subject to certain conditions including a requirement that the newer version is approved for use by the National Coordinator, and does not conflict with requirements under other applicable law. We received a number of comments regarding these proposals, which are outlined in the subsections below.

Comments. We received broad support for the adoption of version 1 of the USCDI as a new standard defining critical health care data to promote interoperability. Some commenters from health plans, while supportive of patient and provider access to health care data, voiced concerns about health plans being required to make data available in the USCDI standard. Other commenters noted that USCDI v1 does not include data classes and elements that pertain to all health care settings, including public health, and would therefore not be broadly applicable to all health care settings.

Response. We thank commenters for their support of the adoption of USCDI v1 as a standard. We wish to clarify that the adoption of version 1 of the USCDI as a standard for our Program is not specific to a setting of care, a health care specialty, or a specific category of health IT user. Nor is the USCDI specific to a particular content exchange standard (*e.g.,* HL7 C–CDA, HL7 FHIR, HL7 V2, and NCPDP SCRIPT). Rather, it applies to the certification of health IT and certified health IT's ability to send and receive the Data Elements defined by USCDI without requirements regarding functionality, user interface, or the use of those Data Elements in exchange. While some users may find few opportunities to exchange these Data Elements, many will exchange these Data Elements frequently, and we believe that all health care providers should have certified health IT that can provide them with a means to appropriately share and access the USCDI data set when exchanging data with other providers. Accordingly, we

[24] *https://argonautwiki.hl7.org/Main_Page.*

seek to clarify a point with respect to our proposal regarding the USCDI and health IT certification. For the purposes of the ONC Health IT Certification Program, specific certification criteria are the way the USCDI comes into effect. For example, the USCDI is referenced as part of the data requirements in the updated ''transitions of care'' certification criterion (§ 170.315(b)(1)), which also specifies that for certification to that criterion, the C–CDA must be used as the syntax to hold all of the USCDI data.

As we explained, we believe that the adoption of USCDI v1 for all certified health IT will advance interoperability by ensuring utilization of common data and vocabulary code sets, and that standardization will support both electronic exchange and usability of the data. Furthermore, because ONC will establish and follow a predictable, transparent, and collaborative process to expand future versions of USCDI, including providing stakeholders with the opportunity to comment on draft USCDI's expansion, stakeholders will have ample opportunities to advance additional Data Classes and Data Elements relevant to a wide range of health care use cases. After consideration of these comments and the overall support of commenters, we have adopted the USCDI v1 as a standard in § 170.213.

We have also extended the compliance timelines with which a health IT developer needs to update to the USCDI, therefore, we have not removed the CCDS definition from § 170.102 as proposed but revised it to remove references to 2014 Edition standards and provided time limitations for when health IT developers need to update to the USCDI.

a. USCDI 2015 Edition Certification Criteria

We proposed (84 FR 7441) to adopt the USCDI Version 1 (USCDI v1) in § 170.213.[25] The USCDI is a standardized set of health Data Classes and constituent Data Elements that would be required to support nationwide electronic health information exchange. Once adopted in this final rule, health IT developers would be required to update their certified health IT to support the USCDI v1 for all certification criteria affected by this proposed change. We also proposed conforming changes in the sections below to update the following formerly CCDS-dependent 2015 Edition certification criteria to incorporate the USCDI standard:

- ''transitions of care'' (§ 170.315(b)(1));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''transmission to public health agencies—electronic case reporting'' (§ 170.315(f)(5));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6)); and
- ''application access—all data request'' (§ 170.315(g)(9)).

We did not include the ''data export'' criterion (§ 170.315(b)(6)) in the proposed list of criteria that would be revised to include the USCDI standard because we proposed to remove the ''data export'' criterion (§ 170.315(b)(6)) and instead proposed to adopt a criterion that we referenced as ''EHI export'' in the Proposed Rule (§ 170.315(b)(10)). For similar reasons, we did not include the ''application access—data category request'' criterion (§ 170.315(g)(8)) because we proposed to replace it with the API certification criterion (§ 170.315(g)(10)) that derives its data requirements from the USCDI.

We also proposed, as a Maintenance of Certification requirement (§ 170.405(b)(3)) for the real world testing Condition of Certification requirement (§ 170.405(a)), that health IT developers with health IT certified to the five above-identified certification criteria prior to the effective date of this final rule would have to update such certified health IT to the proposed revised standards (84 FR 7441 and 7596). We further proposed, as a Maintenance of Certification requirement (§ 170.405(b)(3)) for the real world testing Condition of Certification requirement (§ 170.405(a)), that health IT developers must provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the effective date of this final rule (84 FR 7441 and 84 FR 7596). For the purposes of meeting this compliance timeline, we noted that we expected health IT developers to update their certified health IT and notify their ONC–ACB on the date at which they have reached compliance. We noted that developers would also need to factor these updates into their next real world testing plan as discussed in section VII.B.5 of the Proposed Rule.[26]

Comments. The majority of commenters supported the proposed adoption of USCDI v1 and incorporation of the USCDI into the revised and new certification criteria. Some commenters expressed concern that incorporation of the USCDI into the ''transmission to public health agencies—electronic case reporting'' certification criteria could have a negative impact on data received by public health reporting programs. Some commenters stressed the need for reasonable adoption timelines. Some suggested a longer adoption and implementation timeline for incorporation of the USCDI as part of certified health IT.

Response. ONC acknowledges that some entities, such as public health agencies, may need to consider what the expanded set of data the USCDI v1 offers may mean to their reporting programs and requirements. To be clear, the USCDI's existence as a stand-alone standard will not impact or change public health reporting requirements. However, certain data now included in the USCDI, such as clinical notes, would now become more readily available for public health reporting and a State's public health program's policy may need to be revisited if a State seeks to make use of the ''new'' data the adoption of the USCDI stands to make more easily available, and more usable upon receipt. We also believe that the proposed 24-month timeline for updating certified health IT to comply with the new USCDI standard in § 170.213 is an adequate implementation timeline, based on other adoption timelines with similar technical complexities. We, therefore, have finalized revisions for the five above-identified formerly CCDS-dependent 2015 Edition certification criteria to incorporate the USCDI standard.

We have finalized a modification to the regulation text for these criteria based on public comment related to mitigating the risk of potential confusion caused by updates to existing criteria. As discussed earlier in this preamble (section IV), we received public comment requesting that all revised criteria be included in a new edition of certification criteria. At the start of section IV, we discuss in response to these comments that we do not believe the creation of a new edition is appropriate given that the scope of the updates to the 2015 Edition is tied

[25] We note that USCDI v1 is an updated version and distinguished from the *Draft United States Core Data for Interoperability (USCDI)* previously made available for public review and comment in the course of its development as a prospective standard. The data classes and elements in the USCDI v1 were proposed in § 170.213 and defined in the Proposed Rule, and an additional USCDI v1 document with technical standards information was posted electronically concurrent with the publication of the Proposed Rule in order to provide the public adequate time to fully review and comment on both the proposed regulation and the USCDI v1 technical information.

[26] The finalized real world testing Condition and Maintenance of Certification requirements are discussed in section VII.B.5 of this final rule.

to standards updates required to keep pace with current industry practices. However, we do plan to distinguish the 2015 Edition certification criteria from the updated criteria in this final rule by referring to them as the 2015 Edition Cures Update on the CHPL.

However, as Health IT Modules are updated to the new standards over time, there is a need to define what is required for certification and what is required for compliance to prior certification. Therefore, we have finalized that for criteria being updated from the CCDS to the USCDI, 24 months after publication date of the final rule shall be applicable for a transition from the CCDS to the USCDI. We have finalized that for the period until 24 months after the publication date of the final rule, the CCDS remains applicable for certified Health IT Modules until such Health IT Modules are updated to the USCDI. This means that upon the effective date of the rule, for the identified criteria the following apply for certification and compliance:

- The USCDI, or
- The CCDS for the period up to 24 months after the publication date of the final rule.

This allows for developers to plan the transition for their products more effectively and supports certification continuity. We have finalized a modification to the regulation text to require the USCDI, or the CCDS for the period lasting until 24 months after the publication date of the final rule.

We have finalized this modification to the regulation text for the following criteria:

- ''transitions of care'' (§ 170.315(b)(1));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''transmission to public health agencies—electronic case reporting'' (§ 170.315(f)(5));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6)); and
- ''application access—all data request'' (§ 170.315(g)(9)).

We have finalized in § 170.405(b)(3), as a Maintenance of Certification requirement under the real world testing Condition of Certification requirement, that health IT developers with health IT certified to the five above-identified certification criteria prior to the effective date of this final rule, would have to update such certified health IT to the revisions within 24 months of the publication date of this rule.

As of this final rule's effective date, the ''data export'' criterion in § 170.315(b)(6) is no longer required as a part of the 2015 Edition Base EHR definition. ONC–ACB's will not be permitted to issue certificates to this certification criteria after 36 months after the publication date of this final rule. As discussed in the ''EHI export'' section below, we have retained § 170.315(b)(6) ''as is,'' without updates to the USCDI. Thus, health IT developers with health IT certified to the prior certification criterion in § 170.315(b)(6) do not have to update such certified health IT to the revisions listed above, but are permitted to maintain or seek new Health IT Module certification to this criterion should they desire this functionality.

b. USCDI Standard—Data Classes Included

As we noted in the Proposed Rule (84 FR 7441), the USCDI Version 1 (USCDI v1) and its constituent Data Elements incorporated recommendations we had accepted from public comments we had previously received on our Draft USCDI and Proposed Expansion Process,[27] which we published January 5, 2018 as well as initial feedback on that draft from the Health IT Advisory Committee, both of which occurred prior to the publication of the Proposed Rule. The standard we proposed to adopt in § 170.213 also reflected and acknowledged the burden that rapidly expanding the USCDI v1 beyond the CCDS could cause. As a result, the USCDI v1 that we proposed was a modest expansion of the CCDS, which we indicated that most health IT developers already supported, were already working toward, or should be capable of updating their health IT to support in a timely manner. Therefore, in our Proposed Rule, we outlined only the delta between the CCDS and the USCDI v1. For the overall structure and organization of the USCDI standard, we urged stakeholders to consult *www.healthIT.gov/USCDI.*

Comments. We received numerous comments proposing new Data Classes, Data Elements, and other changes within the USCDI beyond those we included in the Proposed Rule. Comments recommended including new Data Elements and/or classes within the USCDI v1 related to encounter data, financial transaction and insurance data, and specialty-specific Data Elements related to cancer treatment, social determinants of health, and more. Another commenter identified an error in the Procedures Data Class citing the wrong code set for dental procedures in the USCDI v1.

Response. We thank the many commenters for their input on the USCDI. We recognize that the USCDI v1 as proposed represents a modest change over the current CCDS definition. As we indicated in the Proposed Rule (84 FR 7441), we view this initial version of the USCDI standard as a starting point to support improved interoperability. We are also sensitive to requirements related to the development and implementation of adopting the USCDI standard. In the interests of maintaining our proposed implementation timeline of 24 months from the publication of this final rule, and after consideration of these comments and the overall support of commenters, we have finalized the adoption of the Data Classes and elements of the USCDI standard as proposed, with changes outlined in the subsections below. Additionally, in order to address the error pointed out to us via comments in the Procedures Data Class, as was stated in the draft USCDI v1,[28] we clarified that the American Dental Association's Code on Dental Procedures and Nomenclature (CDT) should be used for Dental Procedures in the USCDI v1, not SNODENT as was erroneously stated in the draft USCDI v1.

With respect to the USCDI's expansion in future years, ONC will establish and follow a predictable, transparent, and collaborative process to expand the USCDI, which will provide stakeholders with the opportunity to comment on the USCDI's expansion and to advance additional Data Classes and Data Elements relevant to a wide range of use cases related to health care. Prior to this final rule, we published our initial thinking as well as examples of Data Classes and Data Elements that we believed could be appropriate to propose for adding to the USCDI.[29] We have also solicited feedback and recommendations from the HITAC. As we evaluated public comments and conducted our own research prior to the issuance of this final rule, we also wanted to identify for stakeholders another potential source that could be used to focus efforts around new USCDI Data Classes and Data Elements. As is noted throughout this rule, the HL7® FHIR® standard represents health information in what are called ''FHIR resources.'' When it comes to logically organizing FHIR resources that relate to one another and share common properties, FHIR uses a concept called a ''compartment.'' Through the standards development process a ''Patient Compartment'' has been

[27] *https://www.healthit.gov/sites/default/files/draft-uscdi.pdf (January 5, 2018).*

[28] *https://www.healthit.gov/sites/default/files/draft-uscdi.pdf.*

[29] *https://www.healthit.gov/sites/default/files/draft-uscdi.pdf.*

created, which lists all of the FHIR resources that are associated with a patient. The Patient Compartment ''includes any resources where the subject of the resource is the patient, and some other resources that are directly linked to resources in the patient compartment.'' This organizing framework provides a potentially rich set of a Data Classes and Data Elements to consider for inclusion in the USCDI, including clinical, encounter, specialty, and financial data. As ONC looks to make its own investments to advance the implementation experience associated with prospective USCDI Data Classes and Data Elements, we intend to leverage the Patient Compartment to guide our thinking. In addition, we will also look to and encourage industry to look at other organizing frameworks such as the Clinical Quality/Clinical Decision Support realms and the payer-to-provider community (*e.g.,* DaVinci Project [30]) to help identify data that would be best to focus on for USCDI expansion.

i. Updated Versions of Vocabulary Standard Code Sets

We proposed (84 FR 7441) that the USCDI v1 would include the newest versions of the ''minimum standard'' code sets included in the CCDS available at publication of this final rule. We requested comment on that proposal and on whether it could result in any interoperability concerns. We also noted that criteria such as the 2015 Edition ''family health history'' criterion (§ 170.315(a)(12)), the 2015 Edition ''transmission to immunization registries'' criterion (§ 170.315(f)(1)), and the 2015 Edition ''transmission to public health agencies—syndromic surveillance'' criterion (§ 170.315(f)(2)) reference ''minimum standard'' code sets; however, we indicated that we were considering updating the versions of these standards listed and incorporated by reference in part 170 subpart B that are referenced by these criteria from the versions adopted in the 2015 Edition final rule.

We also noted, for purposes of clarity, that consistent with § 170.555, unless the Secretary prohibits the use of a newer version of an identified minimum standard code set for certification, health IT could continue to be certified or upgraded by developers to a newer version of an identified minimum standard code set than that included in USCDI v1 or the most recent USCDI version that the National Coordinator has approved for use in the Program using the SVAP flexibility.

Comments. There was general support from commenters for updating ''minimum standard'' code sets requirements to the newest versions of these code sets as part of the update from CCDS to the USCDI. One commenter recommended adopting the Data Class requirement first, followed by a delayed requirement of updated versions of the ''minimum standards'' code sets, in order to allow implementers more time to make changes to their systems.

Response. We do not believe that adopting the corresponding ''minimum standards'' code sets that are updated in the USCDI v1 would impose a significant burden on implementers. In consideration of the overall support from commenters, we have finalized our proposal that the USCDI v1 include the newest versions of the ''minimum standard'' code sets available at the time of finalization of this final rule. We have not, however, finalized the proposal for the 2015 Edition ''family health history'' criterion (§ 170.315(a)(12)), the 2015 Edition ''transmission to immunization registries'' criterion (§ 170.315(f)(1)), and the 2015 Edition ''transmission to public health agencies—syndromic surveillance'' criterion (§ 170.315(f)(2)) to reference the newest versions of the ''minimum standard'' code sets for these criteria, because the flexibility already exists to use newer versions of code sets included in these criteria. We note that for these certification criteria, health IT developers may take advantage of the previously established [31] flexibility to seek certification to newer versions of the ''minimum standards'' code with § 170.555.

ii. Address and Phone Number

We proposed (84 FR 7442) new Data Elements in the USCDI v1 for ''address'' and ''phone number.'' We noted that the inclusion of ''address'' (to represent the postal location for the patient) and ''phone number'' (to represent the patient's telephone number) would improve the comprehensiveness of health information for patient care. We further noted that the inclusion of these Data Elements was consistent with the list of patient matching Data Elements already specified in the 2015 Edition ''transitions of care'' certification criterion (§ 170.315(b)(1)(iii)(G)), which supports the exchange of patient health information between providers of patient care.

Comments. Commenters unanimously supported the addition of address and phone numbers to the USCDI v1. The majority of commenters on this proposal recommended the use of the U.S. Postal Service address format to improve address data quality. Commenters also recommended additional elements of address and phone number indicating effective period (*e.g.,* current address, former address); use (*e.g.,* mobile phone number, landline, etc.), and email address.

Response. We thank the commenters for their recommendations and agree that these additional Data Elements can be useful to provide better care and assist with patient matching. In consideration of these comments, we have finalized the addition of the following Data Elements within the Patient Demographics Data Class:

- ''current address'';
- ''previous address'';
- ''phone number'';
- ''phone number type''; and
- ''email address.''

We further clarify that ''phone number'' and ''phone number type'' must be represented using the same standards, ITU–T E.123 (02/2001) and ITU–T E.164, as already adopted for this data in 45 CFR 170.207(q) and referenced in the 2015 Edition ''transitions of care'' certification criterion (§ 170.315(b)(1)(iii)(G)).

We appreciate commenters' recommendations to use the U.S. Postal Service Postal Addressing Standards, which include address formatting guidance and a variety of products to improve address quality, such as address element standardization and validation which are published and available for public use.[32] The U.S. Postal Service Postal Addressing Standards include standardized names for common unit identifiers, line by line acceptance requirements for mail services, and overall address format guidance that has been specifically designed to support labelling of mail items for acceptance by the U.S. Postal Service automated sorting processes. We acknowledge the potential for its use within health IT to improve patient matching. However, while the U.S. Postal Service Postal Addressing Standards include a single representation for certain data elements (such as rendering apartment as apt, building as bldg, floor as fl, etc.) they also allow variations for other data elements, such as ''acceptable'' and ''preferred'' spellings and abbreviations for street and city names. This may result in multiple ''valid'' addresses. To reconcile this variation, the U.S. Postal Service provides a file listing preferred

[30] *http://www.hl7.org/about/davinci/index.cfm.*

[31] 77 FR 54163, 54268–69 (September 4, 2012).

[32] U.S. Postal Service: Postal Addressing Standards (Publication 28) available at *https://pe.usps.com/text/pub28/welcome.htm.*

city and State combinations as well as a file of street name and zip code combinations and the resulting aggregated address would then require manual reconciliation. We believe the U.S. Postal Service Postal Addressing Standards may be useful guidance for health IT developers. However, because of the variation, the required use of reference files, and the manual reconciliation necessary for implementation, we have not adopted the U.S. Postal Service Postal Addressing Standards as a required standard for the address Data Elements within the USCDI. We encourage the use of standardized elements to accurately represent patient address including use of standardized references in the U.S Post Service Postal Addressing Standards where applicable. In addition, we will continue to work with standards developing organizations to evaluate potential solutions to improve patient matching, including considering the potential adaptability of the U.S. Postal Service formats for health IT use cases.

The U.S. Postal Service also maintains web based tools for address validation services and provides implementation guidance to integrate these tools into technical workflows for IT systems in e-commerce and other industries. We agree that these address validation tools have the potential to greatly improve address data quality, and we encourage health IT developers and other relevant health IT users such as health information networks to explore mechanisms by which such address validation might support patient matching. While not specifically designed for patient matching and other health care related applications, USPS address validation has been piloted in these settings. To adapt the address validation tool to a health care purpose requires the services of a third party with licensing of the tool and the development of a bespoke process to execute the tool. The aggregated patient address could then be compared against the USPS address on file and the patient data could be amended where inaccurate, appended where incomplete, or a linked record of secondary address data could be created depending on the percent of confidence in the specific match. This process would then require manual reconciliation. The results of these pilots indicate significant complexity and burden associated with implementation of this process. Given these burdens, we believe it would not be appropriate to require the integration of this distinct functionality into certified health IT at this time. We again encourage the further development and use of standardized approaches for address validation and will continue to monitor and analyze such efforts for consideration in future rulemaking.

iii. Pediatric Vital Signs

As proposed (84 FR 7442), the USCDI v1 included the pediatric vital sign data elements, which are specified as optional health information in the 2015 Edition CCDS definition. The proposed pediatric vital signs included: head occipital-frontal circumference for children less than 3 years of age, BMI percentile per age and sex for youth 2–20 years of age, weight for age per length and sex for children less than 3 years of age, and the reference range/scale or growth curve, as appropriate. As explained in section VI.A.2 of this final rule, the inclusion of pediatric vital sign Data Elements in the draft USCDI v1 align with the provisions of the Cures Act related to health IT to support the health care of children. Prior to the publication of the Proposed Rule, stakeholders emphasized the value of pediatric vital sign data elements to better support the safety and quality of care delivered to children. We also note in our Proposed Rule and in the 2015 Edition proposed rule (80 FR 16818 and 16819) that the Centers for Disease Control and Prevention (CDC) recommends as part of best practices the use of these pediatric vital signs for settings of care in which pediatric and adolescent patients are seen. The availability of a reference range/scale or growth curve would help with proper interpretation of the measurements for the BMI percentile per age and sex and weight for age per length and sex.

Further, we noted our belief that the inclusion of this health information in the USCDI v1 was the appropriate next step after first specifying them as optional in the CCDS definition as part of the 2015 Edition rulemaking (80 FR 62695), and as a means of supporting patient access to their EHI in a longitudinal format through certified health IT (see section 3009(e)(2)(A)(i) of the PHSA as amended by the Cures Act). We recognized, however, that certain health IT developers and their customers may not find these capabilities and information useful. Therefore, we requested comment on the inclusion of pediatric vital signs in the USCDI v1, including the potential benefits and costs for all stakeholders stemming from its inclusion in the USCDI v1.

Comments. Commenters generally supported the inclusion of the pediatric vital signs Data Elements in the USCDI v1. Some commenters opposed their inclusion or believed the inclusion of these Data Elements should be optional since pediatric vital signs are not applicable to all specialties and would add implementation burden and cost without benefit. One commenter stated that only the measurements and associated metadata (units of measure, date/time measurement taken, method of measurement), not the calculated percentiles according to applicable pediatric growth charts, should be required as part of the exchange of patient data. One commenter recommended adding the nutritional status Data Element ''mid-arm circumference.'' Finally, several commenters suggested or requested clarification on the pediatric vital signs Data Elements we proposed (84 FR 7442). Specifically, stakeholders in the pediatric community asked for clarification of the proposed pediatric vital sign ''weight for age per length and sex for children less than 3 years of age,'' noting it does not correspond to any existing pediatric growth charts. Rather, they noted that there is a growth chart ''weight-for-length'' for children less than 3 years of age.

Response. We recognize that the adoption of these Data Elements has the potential to add burden and cost for some health IT products, but we believe the inclusion of these Data Elements can contribute significantly to the longitudinal care of patients. Pediatric care is not isolated to a single specialty or setting of care, and clinicians providing health care for children—especially those providing care for children with complex conditions—may practice in a wide range of settings using a wide range of health IT systems. Many key stakeholders believe that the ability to capture, calculate, and transmit key pediatric growth data using health IT is critical to providing care to these populations as well as communicating with other providers, parent/guardians, and patients. We also note that adoption of the USCDI standard and its Data Classes and elements is not specific as to its usage within a setting of care, a health care specialty, or by a specific category of health IT user; rather it applies to certified health IT's ability to send and receive those Data Elements without requirements regarding functionality, user interface, or the use of those Data Elements in exchange. While some users may find few opportunities to exchange these Data Elements, many will exchange these Data Elements frequently. As we have noted previously, we believe that the adoption

of USCDI for all certified health IT will advance interoperability by ensuring compliance with new data and vocabulary codes sets that support the data.

We also appreciate the commenter's suggestion for an additional Data Element. As we have noted, ONC will establish and follow a predictable, transparent, and collaborative process to expand the USCDI, which will provide stakeholders with the opportunity to advance additional Data Classes and Data Elements relevant to a wide range of use cases related to health care.

Regarding the request to clarify and better define these proposed pediatric vital signs, we note that these Data Elements, as written and proposed, were previously included as optional health information in the 2015 Edition CCDS definition. The discrepancy between the adopted pediatric vital signs and standardized pediatric growth charts was not identified previously. Therefore, we wish to clarify that the above-referenced pediatric vital signs include both the vital measurements and the percentiles used in the following growth charts currently recommended by the Centers for Disease Control and Prevention: [33] for infants birth to 36 months of age: Weight-for-length; and head occipital-frontal circumference for age; and for children 2–20 years of age: Body mass index (BMI) for age.

In consideration of these comments, we have finalized the following pediatric Data Elements in the Vital Signs Data Class of the USCDI v1: Head occipital-frontal circumference percentile (Birth to 36 Months); weight-for-length percentile (Birth to 36 Months); body mass index (BMI) percentile (2–20 Years of Age); and the reference range/scale or growth curve, as appropriate.

iv. Clinical Notes

We proposed (84 FR 7442) to include in the USCDI v1 a new Data Class entitled ''clinical notes.'' ''Clinical notes'' was included in the proposed USCDI v1 based on significant feedback from the industry since the 2015 Edition final rule. We also received similar feedback during the Trusted Exchange Framework and Common Agreement (TEFCA) stakeholder sessions and public comment period. As we noted, ''clinical notes'' have been identified by stakeholders as highly desirable data for interoperable exchange. The free text portion of the clinical notes was most often relayed by clinicians as the data they sought, but were often missing during electronic health information exchange. We additionally noted that clinical notes can be composed of text generated from structured (pick-list and/or check the box) fields as well as unstructured (free text) data. We explained that a clinical note may include the assessment, diagnosis, plan of care and evaluation of plan, patient teaching, and other relevant data points.

We recognized that a number of different types of clinical notes could be useful for stakeholders. We indicated our understanding that work is being done in the community to focus on a subset of clinical notes. We considered three options for identifying the different ''note types'' to adopt in USCDI v1. The first option we considered allowed for the community to offer any and all recommended notes. The second option we considered set a minimum standard of eight note types. This option was derived from the eight note types identified by the Argonaut Project participants.[34] The third option we identified looked to the eleven HL7 Consolidated Clinical Document Architecture (C–CDA) document types identified in the C–CDA Release 2.1, which also included the note types being identified by the Argonaut Project participants. We ultimately proposed the second option because it unites public and private interests toward the same goal. We indicated that the eight selected note types were a minimum bar and, in the future, the USCDI could be updated to include other clinical notes. Specifically, we proposed to include the following clinical note types for both inpatient and outpatient (primary care, emergency department, etc.) settings in USCDI v1 as a minimum standard: (1) Discharge Summary note; (2) History & Physical; (3) Progress Note; (4) Consultation Note; (5) Imaging Narrative; (6) Laboratory Report Narrative; (7) Pathology Report Narrative; and (8) Procedures Note (84 FR 7442). We requested comment on whether to include additional note types as part of the USCDI v1.

Comments. Commenters broadly supported adding ''clinical notes'' as a new Data Class to the USCDI v1, in particular to enable the use of free text for data exchange. Several commenters requested clarity as to whether the proposal to adopt this new Data Class would require the capture and exchange of unstructured, or ''raw'' or ''free'' text, narrative clinical information or more comprehensive documents such as those defined by C–CDA. Some commenters recommended adding certain note types—including continuity of care, operative, and nursing notes—while others recommended removing some of the proposed note types. In particular, Laboratory/Pathology Report Narrative note types were thought to be duplicative of content in the Laboratory Data Class and element Value/Results. Some commenters recommended Imaging Narrative not be used, but added to a new Data Class, Diagnostic Tests, which would combine Laboratory and Radiology tests and results.

Response. We thank commenters for their support and recommendations. While we recognize that there may be alternative methods of organizing different clinical note types, we believe there is value in grouping all clinical notes into a single Data Class within the USCDI. As we noted above and in the Proposed Rule, we have adopted the eight note types identified by the Argonaut Project participants because it unites public and private interests toward the same goal. As we indicated, the eight selected note types are a minimum bar and, in the future, the USCDI could be updated to include other clinical note types. The eight selected note types reflect the most clearly and consistently recommended set of clinical note type. While a variety of additional note types were recommended, there was no consensus for additional note types beyond these eight. In consideration of these comments, we have finalized the clinical notes as a Data Class in the USCDI v1, with only the following eight clinical note types for both inpatient and outpatient (primary care, emergency department, etc.) settings as a minimum standard as proposed: (1) Discharge Summary Note; (2) History & Physical; (3) Progress Note; (4) Consultation Note; (5) Imaging Narrative; (6) Laboratory Report Narrative; (7) Pathology Report Narrative; and (8) Procedures Note.

We wish to further clarify that we have adopted the new Clinical Notes Data Class in order to enable capture and exchange of free text clinical information categorized by the above clinical note types. We refer commenters to our response in section IV.B.1.d of the final rule—Clinical Notes C–CDA Implementation Specification—that addresses the relationship of the clinical notes Data Class to C–CDA implementation specification.

We also seek to clarify two points. First, that these clinical note types are content exchange standard agnostic. They should not be interpreted or associated with the specific C–CDA Document Templates that may share the

[33] *https://www.cdc.gov/growthcharts/index.htm.*

[34] Link to the Clinical Notes Argonaut Project identified (to clarify: Seven bullets are listed, however, we split laboratory and pathology note types into their own note) *http://wiki.hl7.org/index.php?title=201805_Clinical_Notes_Track.*

same name. Secondly, we clarify that these note types are required to be represented in their plain-text form when included in various content exchange standards (*e.g.,* C–CDA, FHIR) as may be applicable to the certification criteria in which the USCDI is referenced.

v. Provenance

We proposed (84 FR 7442) for the USCDI v1 to include a new Data Class, entitled ''provenance.'' As we indicated, stakeholders [35] have identified ''provenance'' as valuable for interoperable exchange. Stakeholders also referenced the provenance of data as a fundamental need to improve the trustworthiness and reliability of the data being exchanged. Provenance describes the metadata, or extra information about data, that can help answer questions such as who created the data and when.

In the Proposed Rule, we noted that the inclusion of ''provenance'' as a Data Class in the USCDI v1 would also complement the Cures Act requirement in section 4002(a) to support the exchange of data through the use of APIs. This approach differs from the exchange of data via the C–CDA. While C–CDAs are often critiqued due to their relative ''length,'' the C–CDA represents the output of a clinical encounter and includes relevant context. The same will not always be true in an API context. APIs facilitate the granular exchange of data and, as noted in the original 2015 Edition final rule, offer the potential to aggregate data from multiple sources using a web or mobile application (80 FR 62675). The inclusion of provenance would help retain the relevant context so the recipient can better understand the origin of the data.

We proposed to further delineate the provenance Data Class into three Data Elements: ''the author,'' which represents the person(s) who is responsible for the information; ''the author's time stamp,'' which indicates the time the information was recorded; and ''the author's organization,'' which would be the organization the author is associated with at the time they interacted with the data (84 FR 7442). We indicated that we identified these three Data Elements as fundamental for data recipients to have available and noted that they are commonly captured and currently available through standards. We requested comment on the inclusion of these three Data Elements and whether any other provenance Data Elements, such as the identity of the individual or entity the data was obtained from or sent by (sometimes discussed in standards working groups as the provenance of the data's ''last hop''), would be essential to include as part of the USCDI v1 standard. We acknowledged that there is currently work to help define provenance in a standard robust manner, and that we anticipated adopting the industry consensus once it became available.

Comments. Commenters overwhelmingly supported the addition of provenance as a new Data Class for USCDI v1. Several commenters stated that the proposed elements were insufficient for the purpose of audit logs for use and disclosure of health data, citing the existing standard specification ASTM E2147.[36] Other commenters stated that these proposed elements did not apply to all use cases of exchanged data and requested clarification regarding applicability, including whether provenance would have to be created for elements created before the implementation deadline of USCDI v1. Because this is a new Data Class, some commenters also requested additional time to adopt and implement this new requirement. Some commenters stated that there could be ambiguity in designating ''author'' for certain clinical information such as patient-reported medications, while in certain other cases, there could be multiple authors for the same clinical information, such as clinical notes. Additionally, some commenters suggested that the ''author'' be limited to only a limited set of Data Elements and not to all the Data Elements. Another commenter specifically addressed several concerns related to the definition of ''author'' for this purpose. Commenters specifically stated they understood author to be the person entering the data into the EHR, but noted that data may also be historical, captured from a device, started by a patient and completed by clinical staff, entered by a patient, entered by resident/students working under a supervising physician, or reported by a patient. The commenter noted that there are additional documentation scenarios such as dictation to scribes or other medical staff, which conflate ''responsibility'' for authorship, and that defining author for every Data Element can be complex. Finally, one health IT developer recommended a 36-month implementation period to begin only after test procedures, implementation guides, and test and validation tools are available and after ONC has consulted at least five CEHRT developers.

Response. We acknowledge that these Data Elements may not be able to fully support the needs of all use cases, but we believe their adoption will improve the trustworthiness and reliability of data being exchanged. For this Data Class, it appears that many commenters over-interpreted our proposal and the effect of having these data in the USCDI. As we noted earlier, the adoption of the USCDI standard and its Data Classes and elements is not specific as to its usage within a setting of care, a health care specialty, or by a specific category of health IT user. Rather it applies to certified health IT's ability to send and receive those Data Elements without requirements regarding functionality, user interface, or the use of those Data Elements in exchange. Therefore, with respect to our reference to provenance data in the USCDI, we have no preset notion or explicit upfront requirement for how this data should be used. We believe that having provenance data is highly impactful, essential for trustworthy interoperability, and will generate greater value for stakeholders as they identify new ways to put this data to use.

Regarding ''author'' as a Data Element within the provenance Data Class, we agree that significant practical scope challenges may arise. Our analysis of the concerns raised by commenters identified a risk of unintended burden and potential risk of error and misattribution associated with this particular Data Element. In most use cases, the inclusion of author organization and author time stamp is sufficient to convey provenance. As a result, we have not finalized the ''author'' as a required Data Element within the provenance Data Class in USCDI. However, we understand that for exchanging certain data elements, such as ''clinical notes,'' it is critical to also send the ''author'' information if available. Our analysis of the various content exchange standards and specifications (*e.g.,* C–CDA and FHIR) indicates that even though the ''author'' Data Element is not explicitly required in USCDI, the health IT specifications in which USCDI Data Elements are represented also set specific data element requirements for certain contexts. For example, in the context of clinical notes, these content exchange standards require health IT systems to be capable of exchanging ''author'' information when it is available. Further, ''author'' is treated as a ''Must Support'' data element in the FHIR US Core Implementation Guide STU 3.1.0 and has a ''SHALL'' constraint (with

[35] *https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement.*

[36] *https://www.astm.org/Standards/E2147.htm.*

appropriate null flavor value) in the C–CDA 2.1. As we have noted previously, we believe that the proposed 24-month timeline for updating certified health IT to comply with the new USCDI standard in § 170.213 is an adequate implementation timeline and will maintain this requirement as finalized earlier in this section.

Therefore, in consideration of the comments received, we have finalized the provenance Data Class in the USCDI v1 and the following two Data Elements:

- ''author time stamp,'' which indicates the time the information was recorded; and
- ''author organization,'' which would be the organization the author is associated with at the time they interacted with the data.

We believe these two provenance Data Elements, ''author organization'' and ''author time stamp,'' within the USCDI v1, which are also used in the C–CDA and FHIR-based certification criteria we have adopted that incorporate the USCDI, will serve as a foundation on which industry stakeholders can subsequently work together to build out additional provenance data requirements in the USCDI. As noted above, we have not finalized the proposed Data Element ''the author,'' which represents the person(s) who was responsible for the information.

vi. Medication Data Request for Comment

In the Proposed Rule, we proposed (84 FR 7443) that the USCDI v1 ''Medication'' Data Class include two constituent Data Elements within it: Medications and Medication Allergies. With respect to the latter, Medication Allergies, we requested comment on an alternative approach. This approach would remove the Medication Allergies Data Element from the Medication Data Class and add it to a new Data Class titled ''Substance Reactions,'' which would include the concept of ''Medication Allergies.'' The new ''Substance Reactions'' Data Class would include the following Data Elements: ''Substance'' and ''Reaction,'' and include SNOMED CT as an additional applicable standard for non-medication substances.

Comments. The majority of commenters supported the creation of a new Data Class ''Substance Reactions'' but requested we preserve the Medication Allergy element because of patient safety concerns related to the adoption of an entirely new Data Element. One commenter supported the change but recommended the new Data Class name be aligned with the HL7 FHIR resource ''AllergyIntolerance.'' This would also be consistent with the C–CDA 2.1 ''Allergy and Intolerance'' section.

Response. We thank the commenters for their input. While we appreciate that there may be some risk associated with the adoption of a new Data Element, we believe this alternative approach better aligns with other standards representing substance reactions, including medication allergies, and this alignment enhances patient safety. Additionally, we agree with the commenter who suggested renaming this new Data Class to align with FHIR and C–CDA approaches.

In consideration of comments, we have finalized the creation of a Data Class in USCDI v1 entitled ''Allergies and Intolerances,'' instead of ''Substance Reactions'' from the original USCDI v1 proposal. The Allergies and Intolerances Data Class in USCDI v1 consists of the following Data Elements: ''Substance—(Medication),'' ''Substance—(Drug Class),'' and ''Reaction.'' ''Substance—(Medication)'' must be represented by RxNorm codes and ''Substance—(Drug Class)'' must be represented by SNOMED CT codes. The addition of the ''Substance—(Drug Class)'' better represents when an individual may have a reaction to an entire drug class as opposed to a specific medication. Additionally, we believe having the Allergy and Intolerances Data Class separated from the Medication Class will accommodate potential additions of other substance Data Elements such as food, environmental, and biologic agents. The Data Element ''Reaction'' is meant to include, but is not limited to, medication allergies. As the USCDI is updated over time to include substances other than medications, we can also see the need to have substance reactions updated as part of this Data Class. To reflect this change, we have updated the terminology in the regulatory text in § 170.315 to remove ''medication allergy'' and replace with ''allergy and intolerance.''

c. USCDI Standard—Relationship to Content Exchange Standards and Implementation Specifications

In recognition of the evolution of standards over time and to facilitate updates to newer versions of standards, we proposed (84 FR 7443) that the USCDI v1 (§ 170.213) would be agnostic as to ''content exchange'' standard. As we noted, the USCDI v1 establishes ''data policy'' and does not directly associate with the content exchange standards and implementation specifications which, given a particular context, may require the exchange of the entire USCDI, a USCDI Data Class, or some or all of the Data Elements within a given Data Class or classes. We further indicated that, to our knowledge, all Data Classes in the USCDI v1 can be supported by commonly used ''content exchange'' standards, including HL7 C–CDA Release 2.1 and FHIR.

We received no comments on this specific proposal and we have finalized our proposal to make USCDI v1 agnostic as to ''content exchange standard'' as described.

2. Clinical Notes C–CDA Implementation Specification

In conjunction with our proposal to adopt the USCDI v1, we proposed to adopt the HL7 CDA® R2 IG: C–CDA Templates for Clinical Notes R1 Companion Guide, Release 1 in § 170.205(a)(5) (''C–CDA Companion Guide''). The C–CDA Companion Guide provides supplemental guidance and additional technical clarification for specifying data in the C–CDA Release 2.1.[37] As we noted in the Proposed Rule (84 FR 7443), the proposed USCDI v1 included new Data Classes, such as ''clinical notes,'' which were further supported through the C–CDA Companion Guide. For example, the C–CDA Companion Guide provides specifications for clinical notes by indicating that clinical notes should be recorded in ''note activity'' and requires references to other discrete data, such as ''encounters.'' The C–CDA Companion Guide also enhances implementation of the updated 2015 Edition certification criteria that reference the C–CDA Release 2.1 (§ 170.205(a)(4)). As noted by stakeholders, the C–CDA Release 2.1 includes some optionality and ambiguity with respect to Data Element components, such as the locations and value sets. We attempted to address some of this optionality by clarifying requirements using Certification Companion Guides (CCGs)[38] and by specifying in the CCDS definition where certain data should be placed in the C–CDA Release 2.1 templates (*e.g.,* ''goals'' in the goals section).[39] The C–CDA Companion Guide, which was released in August, 2015, provides similar, but additional C–CDA implementation structure. For example, race and ethnicity are required Data Elements in the USCDI and must be included in C–CDA exchanges if known, or they may be marked with a nullFlavor value ''UNK'' (unknown) if not known. The

[37] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=447.*

[38] *https://www.healthit.gov/topic/certification-ehrs/2015-edition-test-method.*

[39] *https://www.healthit.gov/sites/default/files/topiclanding/2018-04/2015Ed_CCG_CCDS.pdf.*

C–CDA Release 2.1 is unclear on the location and value set, but the C–CDA Companion Guide clarifies the location and value set. We noted in the Proposed Rule that the adoption of the C–CDA Companion Guide would align with our goal to increase the use of consistent implementation of standards among health IT developers and improve interoperability. We proposed to adopt this C–CDA Companion Guide to support best practice implementation of USCDI v1 Data Classes and 2015 Edition certification criteria that reference C–CDA Release 2.1 (§ 170.205(a)(4)). The criteria include:

- ''transitions of care'' (§ 170.315(b)(1));
- ''clinical information reconciliation and incorporation'' (§ 170.315(b)(2));
- ''care plan'' (§ 170.315(b)(9));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6)); and
- ''application access—all data request'' (§ 170.315(g)(9)).

We proposed, as a Maintenance of Certification requirement for the real world testing Condition of Certification requirement, that health IT developers with health IT certified to the six above-identified certification criteria prior to the effective date of a subsequent final rule would have to update such certified health IT to the proposed revisions (84 FR 7443).[40] We further proposed as a Maintenance of Certification requirement for the real world testing Condition of Certification requirement, that health IT developers would be required to provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the effective date of a final rule (84 FR 7443). For the purposes of meeting that compliance timeline, we indicated that we expected health IT developers to update their certified health IT without new mandatory testing and notify their ONC–ACB on the date at which they have reached compliance. Developers would also need to factor these updates into their next real world testing plan as discussed in section VII.B.5 of the Proposed Rule.[41]

Comments. One commenter supported the use of C–CDA for Clinical Notes. One commenter sought clarity on testing for Clinical Notes conformance to C–CDA 2.1, noting that all C–CDA documents are the same except for the document header. Two commenters recommended review of the Common Well Concise Consolidated CDA white paper.

Response. We thank the commenters for their suggestions and support. During the past few months, industry stakeholders updated the C–CDA Companion Guide to a newer version to best address how clinical notes should be handled in the C–CDA. In consideration of the update to the C–CDA Companion Guide and the comments, we have finalized the adoption of the most up-to-date version, HL7 CDA R2 IG: C–CDA Templates for Clinical Notes STU Companion Guide, Release 2 in § 170.205(a)(5) (''C–CDA Companion Guide'') and have incorporated by reference in § 170.299. This includes adoption of the USCDI v1 and the associated Data Classes.

In order to align ''clinical information reconciliation and incorporation'' (§ 170.315(b)(2)) with the updated Data Classes in the USCDI v1 as proposed in 84 FR 7441, we have replaced the ''medication allergies'' data element in § 170.315(b)(2)(iii)(D)(2) criterion to ''Allergies and Intolerances'' Data Class and require reconciliation of all the data elements in ''Allergies and Intolerances'' Data Class, which includes Substance (Medication), Substance (Drug Class), and Reaction Data Elements. We have revised the regulation text (§ 170.315(b)(2)) to align with this change. We decline to accept the recommendation to adopt the CommonWell specification as we believe the criterion is best met following the C–CDA specification published by HL7.

We have additionally finalized the timeline for the update to the use of the C–CDA companion guide of 24 months after the publication date of this final rule for the following criteria:

- ''transitions of care'' (§ 170.315(b)(1));
- ''clinical information reconciliation and incorporation'' (§ 170.315(b)(2));
- ''care plan'' (§ 170.315(b)(9));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6)); and
- ''application access—all data request'' (§ 170.315(g)(9)).

3. Unique Device Identifier(s) for a Patient's Implantable Device(s) C–CDA Implementation Specification

We noted in the Proposed Rule (84 FR 7443) our awareness of a recently published implementation guide (IG) by HL7 that provides further guidance on the unique device identifier (UDI) requirements. The Health Level 7 (HL7) CDA R2 Implementation Guide: C–CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1–US Realm (UDI IG Release 1), identifies changes needed to the C–CDA to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. The UDI components include the Device Identifier (DI) and the following individual production identifiers: The lot or batch number, serial number, manufacturing date, expiration date, and distinct identification code. As this new IG had been recently published, we requested comment on whether we should add this UDI IG as a requirement in § 170.299(f)(35) for health IT to adopt in order to meet the requirements for content exchange using C–CDA. In addition, we indicated that we did not have a reliable basis on which to estimate how much it would cost to meet the requirements outlined in the UDI IG; and, therefore, we requested comment on the cost and burden of complying with this proposed requirement.

Comments. Commenters unanimously supported adoption of the UDI IG Release 1 as a new requirement for health IT to meet the requirements for the USCDI UDI Data Class. One commenter requested additional guidance regarding the determination of the ''person responsible for the information'' contained in the ''Device'' entry. None of the commenters provided a basis of estimate for the cost to meet the requirements outlined in the UDI IG Release 1.

Response. We thank the commenters for their support. As we noted earlier, the adoption of the USCDI standard and its Data Classes and elements is not specific as to its usage within a setting of care, a health care specialty, or by a specific category of health IT user; rather it applies to certified health IT's ability to send and receive those Data Elements without requirements regarding functionality, user interface, or the use of those Data Elements in exchange. Therefore, we do not specify who must enter such data.

We note also that the C–CDA Companion Guide referenced in subsection (d) below of this final rule now includes the content of the UDI IG Release 1 named in the Proposed Rule. In consideration of comments, we have finalized the proposed UDI Data Class within the USCDI v1, and have adopted the UDI Organizer Template defined in the UDI IG Release 1 and subsequently published as Appendix B of the HL7®

[40] We proposed to codify this requirement in § 170.405(b)(4) (84 FR 7596).

[41] The finalized real world testing plan requirements, codified in § 170.405(b)(2) are discussed in section VII.B.5 of this final rule.

CDA® R2 IG: C–CDA Templates for Clinical Notes, Release 2.1 Companion Guide, Release 2—US Realm, October 2019, as a new requirement for Health IT Modules to meet the requirements for C–CDA-based exchange. We note that the UDI Organizer Template, though subsequently published in Appendix B of the HL7 CDA R2 IG: C–CDA Templates for Clinical Notes STU Companion Guide, Release 2, September 2019, remains substantially unchanged from its previous publication in the UDI IG Release 1 in November 2018 and has been thoroughly reviewed and subjected to balloting and a public comment process.

4. Electronic Prescribing Criterion

We proposed to adopt a new version of the NCPDP SCRIPT standard in 45 CFR 170.205(b)(1), specifically NCPDP SCRIPT standard version 2017071 (84 FR 7444). Because we proposed to adopt a new standard for electronic prescribing (e-Rx), we also proposed to adopt a new certification criterion in § 170.315(b)(11) for the proposed e-Rx standard to replace the old standard in § 170.315(b)(3). The proposed new certification criterion reflected our proposed adoption of NCPDP SCRIPT standard version 2017071 as well as all transactions adopted for the CMS Medicare Part D E-prescribing Program (84 FR 23832). These proposals were made to realign ONC's Health IT Certification Program (Program) policies with those of CMS' Part D E-prescribing rules. ONC and CMS have historically aligned standards adopted under their programs such as those for e-Rx and medication history (MH) to ensure that entities regulated under both schemes can comply with the different programs' requirements. For this reason, we stated that should our proposal to adopt the new e-Rx criterion (§ 170.315(b)(11)) be finalized prior to January 1, 2020, we also proposed to permit continued certification to the current 2015 Edition ''electronic prescribing'' criterion (§ 170.315(b)(3)) that references NCPDP SCRIPT standard version 10.6 for the period of time in which that version of the NCPDP SCRIPT standard would continue to be used in the CMS Medicare Part D E-prescribing Program or the CMS Promoting Interoperability Programs. Finally, we proposed in 84 FR 7445 that once NCPDP SCRIPT standard version 10.6 is no longer used in those Programs, we would no longer permit certification to that criterion and would remove it from the Code of Federal Regulations, and that we would consider setting an effective date for such actions in a subsequent final rule based on stakeholder feedback and CMS policies at the time.

In addition to continuing to reference the current transactions included in § 170.315(b)(3), in keeping with CMS' Modernizing Part D and Medicare Advantage To Lower Drug Prices and Reduce Out-of-Pocket Expenses final rule (84 FR 23832), we also proposed in 84 FR 7445 and in § 170.315(b)(11) to require the support of all of the NCPDP SCRIPT standard version 2017071 transactions CMS has adopted for the Part D E-prescribing regulations in 42 CFR 423.160(b)(2)(iv). Given the January 1, 2020 effective date in CMS rulemaking (83 FR 16440) and the effective date of this final rule, we have finalized our proposed update to the new version of the standard for the electronic prescribing criterion in § 170.315(b)(3) instead of creating a new criterion as proposed in 84 FR 7427 in § 170.315(b)(11). Unlike other criteria in this final rule that allow testing to either version of a required standard until 24 months after the publication date of this final rule, we will not allow certification testing to version 10.6 of the NCPDP SCRIPT standard, as the implementation date for CMS' new Part D E-prescribing Program of January 1, 2020 has passed. However, based on stakeholder feedback, we have finalized a transition period in 45 CFR 170.405(b)(4)(ii) of 24 months from the date of publication of this final rule for certification so developers may test and certify to the updated criterion with all associated transactions.

Comments. The majority of commenters were supportive of our proposal and recommended moving to the NCPDP SCRIPT standard version 2017071 for the e-Rx certification criterion in alignment with CMS' adoption of the standard for the Part D E-prescribing Program. However, a number of commenters expressed concern that while EHRs or other electronic prescribing systems may become certified, pharmacy information systems (PIS) lack a similar certification program and associated standards and technical capability requirements, thus creating a mismatch between the e-prescribing system requirements for EHR users and PIS users. Several commenters specifically noted that PIS, which send or receive these transactions, are not required to adopt the capability to support these transactions as they are out of scope for the Program.

Response. First, we note that the comments suggesting that pharmacies on the sending or receiving end of Part D e-Rx transactions are not required to utilize NCPDP SCRIPT standard version 2017071 transactions are inaccurate. To the extent that a pharmacy conducts electronic prescribing with prescribers e-prescribing Part D covered drugs for Part D eligible individuals, those pharmacies are required to use the NCPDP SCRIPT version 2017071 standard. While there may not be 2015 Edition certification criteria to which pharmacy information systems can be certified, the Part D rules require support of the standard under the Part D E-prescribing Program. Thus, we believe the mismatch concerns raised by commenters are unfounded. As a general matter, Part D prescribers need health IT systems capable of conducting compliant transactions (regardless of ONC certification) and so too do Part D receiving pharmacies. ONC health IT certification will provide an added layer of assurance for Part D prescribers that their e-Rx systems have been tested and certified as being capable of accurately conducting the adopted NCPDP SCRIPT standard version 2017071 transactions.[42]

In addition, we received several comments related to the readiness of PIS for specific transactions beyond those defined for Part D. We include these comments as applicable in the discussion of each transaction below. We reiterate that PIS are outside the scope of the ONC Health IT Certification Program, and we acknowledge the challenge of pharmacy readiness to support all transactions at this time, but if they conduct e-Rx for part D covered drugs prescribed to Part D eligible Medicare beneficiaries, they will be required to use the standard we are adopting for our program by the Medicare Part D e-Rx Program—so if they do e-prescribing at all, we expect that they will be able to conduct transactions using the standard adopted here. Generally, the goal of certification is to ensure that Health IT Modules voluntarily submitted for the Program are capable of conducting the transactions as specified. This ensures that providers have the capability to use the certified product for these transactions where feasible. For this reason, we have finalized the transactions as described below for certified Health IT Modules and encourage pharmacy information system developers to advance their capacity to support a nationwide network of fully interoperable pharmacy information systems.

Comments. As noted, the majority of commenters were supportive of the proposal to remove the 2015 Edition

[42] *https://www.govinfo.gov/content/pkg/FR-2015-10-16/pdf/2015-25597.pdf.*

certification criterion (codified in § 170.315(b)(3)) that references NCPDP SCRIPT standard version 10.6 and replace it with an updated e-Rx criterion (proposed to be codified in § 170.315(b)(11)). Commenters requested that ONC work with CMS on a smooth transition and timeline that would allow adequate time for the development, testing, and full adoption of these updates. A number of commenters stated that the NCPDP SCRIPT standard version 2017071 is not backward compatible with NCPDP SCRIPT standard version 10.6, and therefore there should be no transition period where both standards are applicable. Commenters sought clarity on the timing of the change and expressed concerns that developers and providers may face operational issues in their adoption of version 2017071 of the NCPDP SCRIPT standard by January 1, 2020. Commenters recommended that ONC allow certification timelines that support compliance with Part D while allowing adequate time to mitigate the risk associated with the additional requirements for certification to the proposed criterion.

Response. We appreciate the support expressed by commenters as well as the concern about maintaining alignment between required standards across HHS. We note that the CMS requirement for Part D e-Rx transactions includes a compliance date of January 1, 2020, and that industry feedback notes a consistent and deliberate move toward readiness for the adoption of the new standard for Part D e-Rx, including by health IT industry leaders supporting pharmacy implementation. We believe that this overall industry readiness supports our adoption of the update to the standard for certification purposes and to be in alignment with the required standard update for Part D e-Rx purposes. In response to the request for a smooth transition and continuity of certification for health care providers, we have finalized a revision to the existing criterion in § 170.315(b)(3) rather than removing and replacing the criterion. In order to support the transition to the new standard for Part D, at the request of stakeholders, ONC issued guidance [43] in the third quarter of CY2019 stating, ''. . . developers of 2015 Edition certified Health IT Modules certified to the e-prescribing criterion adopted at 45 CFR 170.315(b)(3) are permitted to update their products to use the NCPDP SCRIPT standard version 2017071 to meet CMS' compliance requirements . . .'' This guidance also noted that ONC would discontinue certification of new products to the electronic prescribing certification criterion using version 10.6 of the NCPDP SCRIPT standard as of January 1, 2020.

In consideration of the comments we received, we have finalized our proposal to update the electronic prescribing (e-Rx) NCPDP SCRIPT standard used for electronic prescribing in the 2015 Edition to NCPDP SCRIPT standard version 2017071, which results in a new e-Rx standard becoming the baseline for certification. As the effective date of this final rule will occur after January 1, 2020, we have not finalized our proposal to permit new products to continue to be certified to the prior standard until the January 1, 2020 date. Instead, we discontinued certification of new products to the former electronic prescribing criterion using the NCPDP SCRIPT standard version 10.6 to align with CMS requirements. We have finalized this update as a modification to the existing certification criterion rather than as a separate new certification criterion to allow for a smooth transition, and to allow for continuity with the certification(s) issued to Health IT Modules for § 170.315(b)(3) prior to January 1, 2020 that are updated under the ONC guidance. This approach will also continue to allow for compliance with the January 1, 2020 timeline for CMS' Medicare Part D e-Rx and Medication History standards.

As noted by commenters, we understand that there is a lack of backward compatibility between the two standards. In order to allow for a reasonable transition period to certification to the full set of NCPDP SCRIPT transactions and other requirements defined in the updated e-Rx certification criterion, we have framed our Maintenance of Certification in section 45 CFR 170.405(b)(5)(ii) with flexibility that will allow health IT developers up to 24 months from the date of publication of this final rule to test and certify to the updated criterion reflective of all NCPDP SCRIPT 2017071 transactions to demonstrate full conformance with the updated criterion. After January 1, 2020, use of the NCPDP SCRIPT 10.6 standard will be prohibited under the Part D program, so we do not expect or anticipate health IT systems certified to § 170.315(b)(3) will conduct Part D transactions using that standard. We also recognize, however, for the purposes of maintaining a product certificate with § 170.315(b)(3) in its scope, that these 24 months from the date of publication from this final rule enable continued compliance and oversight associated with other capabilities in § 170.315(b)(3) that are not applicable for Part D, and for which conformance is still required.

We have finalized this 24-month period for the update for this criterion under the real world testing provisions in § 170.405(b)(5) as follows:

- *Electronic Prescribing.* A health IT developer with health IT certified to § 170.315(b)(3) prior to June 30, 2020, must:
  - Update their certified health IT to be compliant with the revised versions of this criterion adopted in § 170.315(b)(3)(ii); and
  - Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(5)(i) of this section by May 2, 2022.

a. Electronic Prescribing Standard and Certification Criterion

Comments. Commenters expressed concerns about standardization generally within the context of e-prescribing. Several commenters expressed concern about using the NCPDP SCRIPT standard version 2017071, the RxNorm standard, as a requirement for e-prescribing, and other standards such as Fast Healthcare Interoperability Resources (FHIR). One commenter further stated that only inventory (packaging or unit dose strength) codes are standardized in RxNorm, and that drug regimens should be standardized and made computable in RxNorm for safety reasons. Another commenter noted that RxNorm does not index brand names exhaustively with a single unique ID for each branded drug, but that current indexing only allows for generic-level interoperability and only at unit dose level. One commenter expressed concern that the criterion as proposed does not appear to support medication assisted treatment (MAT) for opioid use disorder (OUD) and other long-acting medications. Another commenter stated a hope that standards such as the NCPDP SCRIPT version 2017071 standard can ease data integration into the workflow, lessen burden, and help achieve greater compliance with policy and legal requirements for querying State prescription drug monitoring programs (PDMP). Another commenter supported the adoption of the NCPDP SCRIPT standard version 2017071 because the standard supports the prescribing of compound medications and the sig (*i.e.,* instructions) field is not limited to 140 characters.

[43] For Part D covered drugs prescribed for Part D eligible individuals. ONC Electronic Prescribing Certification Companion Guide: *https://www.healthit.gov/test-method/electronic-prescribing.*

Some commenters also provided suggestions to improve the NCPDP SCRIPT 2017071 standard and its availability to the public by the standards developing organization. Another commenter stated that today's NCPDP standards are not in an API-ready format, and recommended CMS and ONC collaborate with NCPDP to explore API FHIR standards specific to the HL7 Da Vinci Project for a January 2022 effective date or later. A few commenters stated that because many NCPDP standards are not openly accessible and require a paid membership to obtain the technical specifications, our adoption could limit widespread adoption and a standardized implementation nationwide. Several commenters suggested that ONC adopt FHIR as a standard for the Program, and for the e-Rx criterion specifically. We also received several comments that are out of scope which are not addressed in this rulemaking.

Response. We appreciate the commenters' consideration of the standards. We note that RxNorm is a standard maintained by the National Library of Medicine (NLM). ONC adopted RxNorm to represent medication information as a vocabulary standard in § 170.207(d) (80 FR 62612). We encourage all developers who have experience with, and feedback relevant to, RxNorm to contact NLM. As a reminder, RxNorm is considered a minimum standard code set under the Program, and developers are permitted to upgrade their products to comply with a newer version of RxNorm without adversely affecting a product's certification status pursuant to 45 CFR 170.555(b)(2) as long as no other law prohibits such action.

In reference to the OUD prevention and treatment-related concerns that commenters expressed, we note that the NCPDP SCRIPT 2017071 standard does support the exchange of medicines used in medication-assisted treatment (MAT) for opioid use disorder treatment purposes. An electronic prescription of controlled substances transaction containing a MAT drug such as buprenorphine can be sent from a prescriber to a pharmacy through the specified transactions, and the updated § 170.315(b)(3) criterion also requires the inclusion of a reason for the prescription using <Diagnosis><Primary> or <Secondary> elements, or optionally, the technology must be able to receive and transmit the reason for the prescription using the <IndicationforUse> element. In addition, the RxHistoryRequest transaction contains a patient consent indicator that the receiving entity must evaluate for accurate reporting. We are also aware that many PDMPs across the country accept reporting of medication history transactions containing buprenorphine, naltrexone, and other medications that could be used in the treatment of OUD.

We thank commenters for their input related to improvements that could be made to the NCPDP SCRIPT version 2017071 standard, however NCPDP is a member-driven standards developing organization that requires membership in order to participate in standards developing and to access standards and implementation guides. We appreciate the suggestion to provide a direct link to the appropriate NCPDP SCRIPT standard implementation guide, but we have no authority over the business processes of standards developing organizations like NCPDP. We encourage any and all participants with an interest in improving the standard to engage with NCPDP. Regarding the recommendation for ONC to collaborate with NCPDP to explore FHIR, we appreciate the suggestion and support any advancements in technical standards and frameworks that support interoperability. At this time, NCPDP SCRIPT standard version 2017071 has not been mapped to FHIR, but ONC will continue to monitor the industry for opportunities to align the ONC Health IT Certification Program with industry developments.

Comments. Five commenters fully supported all proposed transactions and requirements detailed in the Proposed Rule. The vast majority of commenters noted concerns about the proposed criterion specific to the transactions proposed for adoption in the § 170.315(b)(11) e-Rx certification criterion; details in support or not in support of adoption as proposed are further detailed for each type of transaction below. As a whole, the primary concerns for the transactions and requirements as proposed include the following: (1) EHRs are required to comply with the new transactions and requirements, while receiving pharmacy information systems are not; (2) lack of pharmacy adoption and readiness, as sufficient adoption should occur prior to making the transactions required; and (3) implementation of the proposed transactions and requirements is resource intensive, if not prohibitive, in order to meet the January 1, 2020 deadline set by CMS. Several commenters suggested either an extension or that certain transactions should be made optional.

Response. We appreciate all of the public comments and have modified the transactions to specify which transactions are finalized as required for Health IT Modules for purposes of obtaining or retaining certification to § 170.315(b)(3), which are optional for Health IT Modules for purposes of obtaining or retaining certification to § 170.315(b)(3), and any other § 170.315(b)(3) requirements below. Additional public comment received and related responses are grouped below based on the comment's relation to the specific transactions. We note that ''optional'' for the purposes of certification does not mean, and should not be interpreted as, ''optional'' for Part D E-prescribing Program compliance. To the extent that prescribers and pharmacies conduct electronic prescribing with Part D covered drugs prescribed for Part D eligible individuals they will be required to use the NCPDP SCRIPT 2017071 standard to conduct those transactions under the Part D E-prescribing Program. Thus, a transaction designated as ''optional'' for the purposes of certification means a health IT developer can elect to have that transaction explicitly tested as part of certification for its product or can choose not to do so—either will allow its product to be certified to § 170.315(b)(3). We reiterate that comments regarding CMS' January 1, 2020 timeline are out of scope as we cannot change CMS' policy or its timeline.

b. Electronic Prescribing Transactions

In addition to adopting the NCPDP SCRIPT version 2017071 standard for the transactions that are listed in the current ''electronic prescribing'' criterion (§ 170.315(b)(3)), we also proposed to adopt and require conformance to all of the NCPDP SCRIPT version 2017071 standard transactions CMS adopted in 42 CFR 423.160(b)(2)(iv). We proposed this updated 2015 electronic prescribing criterion to therefore include the following transactions:

i. Create and Respond to New Prescriptions (NewRx, NewRxRequest, NewRxResponseDenied)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transactions for NewRx, NewRxRequest and NewRxResponseDenied. A NewRx transaction is a new prescription from a prescriber to a pharmacy so that it can be dispensed to a patient. A NewRxRequest is a request from a pharmacy to a prescriber for a new prescription for a patient. A NewRxResponseDenied is a denied response to a previously sent NewRxRequest (if approved by the

prescriber, a NewRx would be sent instead). A NewRxResponseDenied response may occur when the NewRxRequest cannot be processed or if information is unavailable.

Comments. While the NewRx transaction received unanimous support as a required transaction for adoption in the updated § 170.315(b)(3) criterion, the vast majority of commenters opposed adopting the NewRxRequest and NewRxResponseDenied transactions as required transactions primarily due to a lack of adoption by the PIS involved in the exchange. Several commenters stated that the NewRxRequest and NewRxResponseDenied is not yet in broad use. A commenter who supported adoption of NewRxRequest and NewRxRequestDenied believed that they may be beneficial for electronic prescribing of controlled substances (EPCS) and noted that pharmacies have expressed interest in implementation.

Response. In consideration of public comments, we have adopted NewRx as a required transaction, and NewRxRequest and NewRxResponseDenied as optional transactions in the updated § 170.315(b)(3) electronic prescribing criterion. We have finalized these latter two transactions as optional in response to commenters' concerns regarding a lack of adoption by the PIS that would be involved in the exchange. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the NewRx transaction.

ii. Request and Respond to Change Prescriptions (RxChangeRequest, RxChangeResponse)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transactions for RxChangeRequest and RxChangeResponse. An RxChangeRequest transaction originates from a pharmacy and may be sent to a prescriber to: Request a change in the original prescription (new or fillable); validate prescriber credentials; request a review by a prescriber of the drug requested; or obtain prior authorization from the payer for the prescription. An RxChangeResponse transaction originates from a prescriber to respond to: A prescription change request from a pharmacy; a request for a prior authorization from a pharmacy; or a prescriber credential validation request from a pharmacy.

Comments. Most commenters supported the proposed adoption of the RxChangeRequest and RxChangeResponse transactions. One commenter recommended against adoption until industry adoption is more widely spread across retail pharmacies and demonstrates value.

Response. Because the majority of commenters were in support of adoption of the RxChangeRequest and RxChangeResponse transactions as proposed, we have included these transactions as required in the updated § 170.315(b)(3) electronic prescribing criterion. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the RxChangeRequest and RxChangeResponse transactions.

iii. Request and Respond to Cancel Prescriptions (CancelRx, CancelRxResponse)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transactions for CancelRx and CancelRxResponse. A CancelRx transaction is a request from a prescriber to a pharmacy to not fill a previously sent prescription. A CancelRx must contain pertinent information for the pharmacy to be able to find the prescription in their system (patient, medication (name, strength, dosage, form), prescriber, and prescription number if available). A CancelRxResponse is a response from a pharmacy to a prescriber to acknowledge a CancelRx, and is used to denote if the cancellation is approved or denied.

Comments. The majority of public comments reflected support for finalizing CancelRx and CancelRxResponse as required transactions. One commenter stated that the CancelRx transaction will reduce cost and improve patient safety, as patients may have remaining refills available that are subsequently modified based on a physician's new assessment. Another commenter noted that certified technology currently supports CancelRx transactions in version 10.6 of the NCPDP SCRIPT standard and encouraged developers to upgrade their technology to support CancelRx transactions in NCPDP SCRIPT standard version 2017071, as these transactions provide great value to end users. One commenter expressed concern for pharmacy readiness for CancelRx, and felt there should be sufficient industry adoption in place before it is a certification requirement.

Response. We thank commenters for their overall support of the proposed CancelRx and CancelRxResponse transactions. In light of the commenters' overall support for the proposed CancelRx transactions and in order to support patient safety and the free flow of communication between prescribers and pharmacies, we have included these transactions as required in the revised § 170.315(b)(3) electronic prescribing criterion. We reiterate that although PIS are outside the scope of the ONC Health IT Certification Program, we encourage pharmacy information system developers to advance their capacity to support a nationwide network of fully interoperable PIS. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the CancelRx transaction.

iv. Request and Respond to Renew Prescriptions (RxRenewalRequest, RxRenewalResponse)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transactions for RxRenewalRequest and RxRenewalResponse. An RxRenewalRequest transaction originates from a pharmacy to request additional refills beyond those originally prescribed. An RxRenewalResponse transaction originates from a prescriber to respond to the request from the pharmacy.

Comments. Commenters supported adoption of the RxRenewalRequest and RxRenewalResponse transactions as proposed. One commenter stated that these transactions could be implemented after the CMS deadline of January 1, 2020 without loss of current functionality. Another commenter said that these transactions are widely used in the industry and provide great value to end users.

Response. We appreciate the support for the RxRenewalRequest and RxRenewalResponse transactions and have included these transactions as required in the updated § 170.315(b)(3) electronic prescribing criterion. We reiterate that the entire updated § 170.315(b)(3) criterion and requirements must be met before certification can be granted. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the

updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the RxRenewalRequest and RxRenewalResponse transactions.

v. Receive Fill Status Notifications (RxFill, RxFillIndicatorChange)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transactions for RxFill and RxFillIndicatorChange. An RxFill transaction is sent from a pharmacy to a prescriber or long term and post-acute care (LTPAC) facility indicating the FillStatus (dispensed, partially dispensed, not dispensed or returned to stock, or transferred to another pharmacy) of the new, refill, or resupply prescriptions for a patient. RxFillIndicator informs the pharmacy of the prescriber's intent for fill status notifications for a specific patient/medication. An RxFillIndicatorChange is sent by a prescriber to a pharmacy to indicate that the prescriber is changing the types of RxFill transactions that were previously requested, and in which the prescriber may modify the fill status of transactions previously selected or may cancel future RxFill transactions.

Comments. While the RxFill transaction received unanimous support as a required transaction, the vast majority of comments opposed adopting the RxFillIndicatorChange as proposed due to a lack of industry adoption and broad use by PIS. One commenter stated that there has not been a significant use case for the RxFillIndicatorChange transaction to prescribers. A few commenters suggested that ONC wait to require the RxFillIndicatorChange until this transaction is more widely adopted by both prescribers and pharmacies and value is realized in the industry, and suggested either removing RxFillndicatorChange from the proposed criterion or making this transaction optional. Another commenter argued that RxFillIndicatorChange should be optional as development to support this transaction in NCPDP SCRIPT standard version 2017071 would be resource intensive. Commenters in support of the adoption of the RxFillIndicatorChange transaction stated it is the only way to alter the prescriber notification preferences in an ambulatory or acute setting outside of a fillable message. Commenters supporting adoption of the RxFillIndicatorChange transaction further noted that, historically, the lack of prescriber control over notification messages may have had an impact on hindering adoption. One commenter suggested that, in lieu of the RxFillIndicatorChange transaction, EHRs receive all fill notifications and subsequently use logic to bring the clinician's attention to only important indicators.

Response. We appreciate all of the comments that supported the RxFill transaction and the RxFillIndicatorChange transaction. After consideration of comments received on the RxFill and RxFillIndicatorChange transactions, we have adopted the RxFill transaction as required and the RxFillIndicatorChange transaction as optional in the updated § 170.315(b)(3) electronic prescribing criterion. We encourage further development and innovation to address the concerns that we heard from commenters, and we will continue to monitor advancements in standards and technology for future rulemaking. We reiterate that PIS are outside the scope of the ONC Health IT Certification Program and encourage pharmacy information system developers to advance their capacity to support a nationwide network of fully interoperable PIS. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the RxFill transaction.

vi. Request and Receive Medication History (RxHistoryRequest, RxHistoryResponse)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transactions for RxHistoryRequest and RxHistoryResponse. An RxHistoryRequest transaction is a request from a prescriber to a pharmacy for a list of medications that have been prescribed, dispensed, claimed, or indicated by a patient. An RxHistoryResponse is a response to an RxHistoryRequest containing a patient's medication history. It includes the medications that were dispensed or obtained within a certain timeframe, and optionally includes the prescriber that prescribed it.

Comments. Commenters supported adoption of the RxHistoryRequest and RxHistoryResponse transactions as proposed. One commenter also stated that both transactions could facilitate EHR and other health IT data integration with PDMP systems, yet noted that in many cases, State law or policy prohibits data integration between EHRs and PDMPs. Another commenter stated that these transactions are widely used in the industry and provide great value to end users.

Response. We appreciate all comments we have received on the use of the RxHistoryRequest and RxHistoryResponse transactions. We agree with the commenter that the RxHistoryRequest and RxHistoryResponse transactions support data integration between health IT systems such as EHRs and other information technology systems such as PDMPs, and encourage any efforts made by developers to fully integrate prescription and other health data into a provider's workflow within allowable law. We reiterate that ONC does not have control over State laws that govern PDMPs. We will continue to monitor regulatory and industry advancements in this area and will take them into consideration in future rulemaking. We have adopted these transactions as required in the updated § 170.315(b)(3) electronic prescribing criterion. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the RxHistoryResponse transaction.

vii. Ask the Mailbox If There Are Any Transactions (GetMessage)

We proposed in 84 FR 7444 to enable a user to perform the electronic transaction GetMessage for Ask the Mailbox. This transaction is used by the prescriber or pharmacy when asking the mailbox if there are any transactions. It is the basis for the mechanism used by a prescriber or pharmacy system to receive transactions from each other, from a payer, or from the Risk Evaluation and Mitigation Strategy (REMS) Administrator via a switch acting as a mailbox.

Comments. Approximately half of commenters opposed adoption of the GetMessage transaction and the other half supported adoption in the updated § 170.315(b)(3) electronic prescribing criterion. Commenters not in support of the GetMessage transaction asserted that it is not in use by prescribers and that it is an obsolete method of message retrieval. Commenters in support of adoption argued that it is applicable when not transacting with real-time messaging, and should be adopted as an optional transaction.

Response. We thank commenters for their input. After careful consideration of all comments received, and in our ongoing efforts to align with CMS Part D requirements, we have determined to adopt the GetMessage transaction as optional for the updated § 170.315(b)(3) electronic prescribing criterion.

viii. Relay Acceptance of a Transaction Back to the Sender (Status)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transaction to relay acceptance of a transaction back to the sender. A Status transaction in response to any applicable transaction other than GetMessage indicates acceptance and responsibility for a request. A Status transaction in response to GetMessage indicates that no mail is waiting for pickup. A Status transaction cannot be held in an electronic mailbox and may not contain an error.

Comments. Commenters supported adoption of the Status transaction as proposed. Two commenters noted that since the transaction is an acknowledgement, it would not contain the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D).

Response. We appreciate all comments in support of the Status transaction and have included this transaction as required in the updated § 170.315(b)(3) electronic prescribing criterion. As an acknowledgement, we agree that the NCPDP SCRIPT version 2017071 standard does not support the conveying the reason for the prescription in the Status transaction, and have modified the requirement to reflect this.

ix. Respond That There Was a Problem With the Transaction (Error)

We proposed in 84 FR 7444 to enable a user to perform the related electronic transaction for Error response. This transaction indicates an error has occurred and that the request was terminated. An Error can be generated when there is a communication problem or when the transaction actually had an error. An Error can be held in an electronic mailbox, as it may be signifying to the originator that a transaction was unable to be delivered or encountered problems in the acceptance. The Error must be a different response than a Status, since the communication between the system and the mailbox must clearly denote the actions taking place. An Error is a response being delivered on behalf of a previous transaction, while Status signifies no more mail.

Comments. Commenters supported adoption of the Error transaction as proposed. Two commenters noted that since the transaction is an acknowledgement, it would not contain the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D).

Response. We appreciate all comments in support of the Error transaction and have included this transaction as required in the updated § 170.315(b)(3) electronic prescribing criterion. As an acknowledgement, we agree that the NCPDP SCRIPT version 2017071 standard does not support the reason for the prescription in the Error transaction, and we have modified that requirement to reflect this.

x. Respond That a Transaction Requesting a Return Receipt Has Been Received (Verify)

We proposed in 84 FR 7445 to enable a user to perform the related electronic transaction for Verify. This transaction is a response to a pharmacy or prescriber indicating that a transaction requesting a return receipt has been received. Verifications result when a ''return receipt requested'' flag is set in the original request. Upon receiving a transaction with ReturnReceipt set, it is the responsibility of the receiver to either generate a Verify in response to the request (recommended), or generate a Status in response to this request, followed subsequently by a free-standing Verify transaction. This transaction notifies the originator that the transaction was received at the software system. It is not a notification of action taking place, since time may elapse before the ultimate response to the transaction may take place.

Comments. Commenters supported adoption of the Verify transaction as proposed. Two commenters noted that since the transaction is an acknowledgement, it would not contain the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D).

Response. We appreciate all comments in support of the Verify transaction and have included this transaction as required in the updated § 170.315(b)(3) electronic prescribing criterion. As an acknowledgement, we agree that the NCPDP SCRIPT standard version 2017071 does not support the reason for the prescription in the Verify transaction, and we have modified that requirement to reflect this.

xi. Request to Send an Additional Supply of Medication (Resupply)

We proposed in 84 FR 7445 to enable a user to perform the related electronic transaction for Resupply. This transaction is a request from a Long Term and Post-Acute Care (LTPAC) organization to a pharmacy to send an additional supply of medication for an existing order. An example use case is when a medication supply for a resident is running low (*e.g.,* 2–3 doses) and a new supply is needed from the pharmacy. In such a circumstance, the LTPAC organization sends the Resupply transaction as a way to notify the pharmacy that an additional supply for the medication is needed.

Comments. Commenters expressed concern over adopting this transaction as a required transaction for a few reasons. Some commenters noted that the Resupply transaction is only applicable to LTPAC practice settings for management of on-site pharmacy inventory and for communication between a LTPAC facility and a contracted pharmacy. Other commenters mentioned that PIS on the sending or receiving end of the transaction are not required to support this transaction. Some commenters stated that this transaction is not widely adopted among prescribers, and that it should not be adopted until this occurs. Two commenters requested that we either remove the transaction from the final rule or make the Resupply transaction optional. Other commenters stated that while this transaction may be beneficial in the future, it was their opinion that it is premature to require the Resupply transaction in the electronic prescribing criterion at this time.

Response. We appreciate all comments related to the Resupply transaction and have included this transaction as optional in the updated § 170.315(b)(3) electronic prescribing criterion. We are aware of several ONC-certified EHRs and other health IT that were either designed exclusively for, or were expressly designed to support, LTPAC providers in addition to other institutions, and encourage those and other developers to undergo certification testing to the Resupply transaction. Additionally, we note that pursuant to the certification criterion, health IT presented for certification must be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) in the Resupply transaction. We reiterate that PIS are outside the scope of the ONC Health IT Certification Program and encourage pharmacy information system developers to advance their capacity to support a nationwide network of fully interoperable PIS.

xii. Communicate Drug Administration Events (DrugAdministration)

We proposed in 84 FR 7445 to enable a user to perform the related electronic transaction for DrugAdministration.

This transaction communicates drug administration events from a prescriber or care facility to the pharmacy or other entity. It is a notification from a prescriber or care facility to a pharmacy or other entity that a drug administration event has occurred (*e.g.,* a medication was suspended or administration was resumed).

Comments. Commenters expressed concern over adopting this transaction as a required transaction for a few reasons. Some commenters noted that the DrugAdministration transaction is only applicable to LTPAC practice settings and is therefore not relevant to the scope of all certified health IT products, though one commenter noted that there could be possible value of this transaction in ambulatory and acute care settings as well. In addition, one commenter reported LTPAC organizations interested in potentially using e-prescribing transactions rated DrugAdministration as a low priority transaction type, meaning there may not be a wide user base interested in implementing it.

Response. We appreciate comments related to the DrugAdministration transaction and have included this transaction as optional in the updated § 170.315(b)(3) electronic prescribing criterion. We are aware of several ONC-certified EHRs and other health IT that were either designed exclusively for, or are used in support of, LTPAC providers, and encourage those and other developers to undergo certification testing to the DrugAdministration transaction. In light of the commenters' concerns, we have adopted the DrugAdministration transaction as optional because the ONC Health IT Certification Program is agnostic to care settings and programs, yet still supports many different use cases. This allows the ONC Health IT Certification Program to support multiple program and setting needs, including but not limited to the Promoting Interoperability Programs and long term and post-acute care. Because the transaction will be optional in the updated (b)(3) criterion, developers whose clients do not support long term care settings will not be required to demonstrate their capacity to send this transaction.

xiii. Request and Respond to Transfer One or More Prescriptions Between Pharmacies (RxTransferRequest, RxTransferResponse, RxTransferConfirm)

We proposed in 84 FR 7445 to enable a user to perform the related electronic transactions for RxTransferRequest, RxTransferResponse and RxTransferConfirm. The RxTransferRequest transaction is used when the pharmacy is asking for a transfer of one or more prescriptions for a specific patient to the requesting pharmacy. The RxTransferResponse transaction is the response to the RxTransferRequest which includes the prescription(s) being transferred or a rejection of the transfer request. It is sent from the transferring pharmacy to the requesting pharmacy. The RxTransferConfirm transaction is used by the pharmacy receiving (originally requesting) the transfer to confirm that the transfer prescription has been received and the transfer is complete.

Comments. The vast majority of commenters expressed concerns with the proposal to adopt RxTransferRequest, RxTransferResponse, and RxTransferConfirm transactions as proposed because they are only used in pharmacy-to-pharmacy transactions and are not applicable to EHRs. Further, two commenters noted that PIS are not required to support these transactions. Conversely, the two commenters that supported these transactions cited the benefit of allowing pharmacies to transfer unfilled controlled substance prescriptions, including Schedule 2, between pharmacies.

Response. We thank commenters for their input. We proposed to require all of the NCPDP SCRIPT 2017071 standard transactions CMS adopted in 42 CFR 423.160(b)(2)(iv) to illustrate our continued dedication to establish and maintain complementary policies to ensure that the current standard for certification to the electronic prescribing criterion permits use of the current Part D e-Rx and MH standards. With consideration of comments, and because it was not the intent of this certification criterion to include pharmacy specific transactions for the purposes of certification, we have adopted RxTransferRequest, RxTransferResponse, and RxTransferConfirm as optional in the updated § 170.315(b)(3) electronic prescribing criterion. We reiterate that PIS are outside the scope of the ONC Health IT Certification Program and encourage pharmacy information system developers to advance their capacity to support a nationwide network of fully interoperable PIS.

xiv. Recertify the Continued Administration of a Medication Order (Recertification)

We proposed in 84 FR 7445 to enable a user to perform the related electronic transaction for Recertification. This transaction is a notification from a LTPAC facility, on behalf of a prescriber, to a pharmacy recertifying the continued administration of a medication order. An example use is when an existing medication order has been recertified by the prescriber for continued use.

Comments. Commenters expressed concern over adopting the Recertification transaction as proposed primarily because it is only applicable to LTPAC practice settings. One commenter stated that LTPAC organizations interested in potentially using e-prescribing transactions rated Recertification as a low priority transaction type, suggesting that there may not be a wide user base interested in using it.

Response. We appreciate all comments in support of the Recertification transaction. In light of commenters concerns, we have adopted this transaction as optional in the updated § 170.315(b)(3) electronic prescribing criterion. We are aware of several ONC-certified EHRs and other health IT that were either designed expressly for or in support of LTPAC providers, among other institutions, and encourage those and other developers to undergo certification testing to the Recertification transaction.

xv. Complete Risk Evaluation and Mitigation Strategy (REMS) Transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse)

We proposed in 84 FR 7445 to enable a user to perform the related electronic transactions for REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse. With CMS' adoption of these transactions in their recently issued final rule associated with e-Rx for Medicare Part D (42 CFR 423.160(b)(2)(iv)(W)–(Z)), we believe that it will be beneficial to include these four REMS transactions as part of this certification criterion: REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse.

Furthermore, under the Food and Drug Administration Amendments Act (FDAAA) of 2007 (Pub. L. 110–85), the Food and Drug Administration (FDA) requires REMS from a pharmaceutical manufacturer if the FDA determines that a REMS is necessary to ensure the benefits of a drug outweigh the risks associated with the drug. In support of our sister agencies' work, we therefore proposed to include the REMS transactions as part of this certification criterion.

Comments. The vast majority of commenters supported adoption of REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse as optional, not required, transactions. Those in support of the transactions as proposed suggested that ONC should develop strategies to encourage providers to consciously consider and appropriately act on alerts to reduce the risk that these messages can easily be clicked through and missed, particularly if that provider is experiencing alert fatigue. Multiple reasons were provided by commenters who stated that the proposed REMS transactions should be adopted as optional in the proposed certification criterion. These reasons included the state of system readiness and adoption by manufacturers, REMS administrators, and pharmacy information systems. Another commenter stated that these REMS transactions are not yet in widespread use and should be piloted before being required as they require extensive design and development effort.

Response. Given comments in support of the REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse transactions, we have included these transactions as optional in the updated § 170.315(b)(3) electronic prescribing criterion. We encourage commenters, developers, and other stakeholder to review and provide feedback on sections related to REMS (*https://www.healthit.gov/isa/allows-a-prescriber-communicate-a-rems-administrator*) and all other electronic prescribing use cases on the ONC Interoperability Standards (ISA) and post suggested edits and updates on these transactions as the industry advances. We encourage manufacturers, REMS administrators, and pharmacy information system developers to adopt these and other NCPDP SCRIPT standard version 2017071 transactions to improve safe prescribing practices and patient safety, and encourage developers to test their capacity to send and receive REMS messages by utilizing the testing tools that are available.

xvi. Electronic Prior Authorization

The Part D E-prescribing prior authorization process in 84 FR 28450 through 28458 requires that providers supply additional clinical information to verify that the medication can be covered under the Medicare Part D benefit. The prior authorization process is intended to promote better clinical decision-making and ensure that patients receive medically necessary prescription drugs. We are looking for ways that would streamline the process for exchanging clinical and financial data amongst prescribers and payers for prior authorization and improve patients' access to needed medications. Electronic prior authorization (ePA) automates this process by allowing providers to request and respond to electronic prior authorization transactions within their workflow. Using electronic prior authorization (ePA) transactions in the NCPDP SCRIPT standard version 2017071 provides a standard structure for exchanging prior authorization (PA) questions and answers between prescribers and payers, while allowing payers to customize the wording of the questions. Electronic prior authorization transactions will additionally support the automation of the collection of data required for PA consideration, allowing a health IT developer to systemically pull data from a patient's medical record. The efficiency gains offered by the ePA transactions in the NCPDP SCRIPT standard version 2017071 are the primary driver behind the development of this new capability. We believe the adoption of the ePA transactions included in version 2017071 of the NCPDP SCRIPT standard as optional transactions aligns with CMS' proposals for Part D ePA, and therefore, will not be adopting NCPDP SCRIPT standard version 2013101 as suggested by the commenter. On June 17, 2019, CMS issued the Secure Electronic Prior Authorization for Medicare Part D proposed rule (84 FR 28450), including a proposed new transaction standard for the Medicare Prescription Drug Benefit program's (Part D) e-prescribing program. Under this proposal, Part D plan sponsors would be required to support version 2017071 of the NCPDP SCRIPT standard for four ePA transactions, and prescribers would be required to use that standard when performing ePA transactions for Part D covered drugs they wish to prescribe to Part D eligible individuals. While not currently adopted as part of the Part D eRx standard, the NCPDP SCRIPT standard version 2017071 includes eight transactions that would enable the prescribers to initiate medication ePA requests with Part D plan sponsors at the time of the patient's visit. The eight transactions are: PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse.

Comments. Several commenters recommended the adoption of the ePA transactions available in the NCPDP SCRIPT standard version 2017071 for a variety of reasons, including improving efficiencies in the prior authorization process, improving patient outcomes, reducing point-of-sale rejections, increasing health IT developer adoption, and improving the Medicare Part D member experience. Several commenters indicated that lack of vendor support for the ePA transactions is a major barrier to physician use of the transactions. One commenter also suggested ONC adopt the NCPDP SCRIPT standard version 2013101 prior authorization transactions.

Response. We thank commenters for their feedback. In consideration of comments, we have adopted the ePA transactions in the NCPDP SCRIPT standard version 2017071 as optional for the updated § 170.315(b)(3) electronic prescribing criterion. We believe the adoption of the ePA transactions included in version 2017071 of the NCPDP SCRIPT standard as optional transactions aligns with CMS' proposals for Part D ePA. We note that this final rule allows only for the voluntary certification of Health IT Modules by health IT developers to support these transactions, and does not require the certification, adoption, or use of such Health IT Modules by health care providers for this or any other purpose. We also note that development, testing, and implementation to support these transactions are important first steps toward integrating pharmacies in the prior authorization process for Part D prescriptions, while supporting widespread industry adoption and reducing burden on providers. We refer readers to the ONC Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs,[44] drafted in partnership with CMS, for further discussion of potential opportunities to ease related clinician burden through improved health IT enabled processes.

xvii. Reason for the Prescription

For each transaction specified, the technology must be able to receive and transmit the reason for the prescription.

Comments. Commenters supported continued adoption of the reason for the prescription in specific electronic prescribing transactions. Some commenters noted that some of the proposed transactions would not contain the reason for the prescription as referenced in the updated

[44] *https://www.healthit.gov/topic/usability-and-provider-burden/strategy-reducing-burden-relating-use-health-it-and-ehrs.*

§ 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D).

Response. We thank commenters for their feedback. We reiterate our decision to require Health IT Modules seeking certification to the updated electronic prescribing certification criterion to be capable of including the reason for the prescription as referenced in the updated § 170.315(b)(3)(ii) or § 170.315(b)(3)(ii)(D) within relevant electronic prescription transactions to support patient safety and align with HHS goals to expand safe, high quality health care. Health IT certified to the updated § 170.315(b)(3) criterion must have the capacity to enable a user to receive and transmit the reason for the prescription using the diagnosis elements: <Diagnosis><Primary> or <Secondary>, or optionally, the technology must be able to receive and transmit the reason for the prescription using the <IndicationforUse> element, and be consistent with the International Statistical Classification of Diseases and Related Health Problems (ICDs) sent in the diagnosis element(s). The <IndicationforUse> element defines the indication for use of the medication as meant to be conveyed to the patient, and is included in the Sig. This requirement would apply to the following NCPDP SCRIPT standard version 2017071 transactions that we have adopted in this criterion (see discussion above): NewRx, RxChangeRequest, RxChangeResponse, CancelRx, RxRenewalRequest, RxRenewalResponse, RxFill, RxHistoryResponse, Resupply, RxTransferRequest, RxTranferResponse, REMSInitiationRequest, REMSInitiationResponse, REMSRequest, REMSResponse, PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse.

xviii. Oral Liquid Medications

Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.,* not cc).

Comments. While not within the scope of the Proposed Rule, one commenter did not support the continued requirement to prescribe oral liquids in ''mL'' units. The commenter supported the use of metric units, but did not agree with the requirement of the ONC Health IT Certification Program to limit this to only milliliters. The commenter recommended that the unit of measure used by a prescriber be at their discretion, as long as it is appropriate for the dosage.

Response. We thank the commenter for the input. Because this requirement is out of scope for the Proposed Rule in that we did not propose to change this conformance requirement, we decline to relax or retire the requirement for oral liquid medications to be prescribed in mL units. When we first adopted this requirement for the 2015 Edition Proposed Rule, several commenters were supportive of improving patient safety through use of the metric standard for dosing, but recommended that this requirement only apply to oral liquid medications. Incorrect dosage is a common error with liquid medication, often resulting from confusion between different dose measurements (*e.g.,* mL and teaspoons). If these measurements are confused with each other, too much or too little of the medicine can be given. This requirement is also in alignment with NCPDP SCRIPT implementation recommendations.

xix. Signatura (Sig) Element

The Signatura (Sig) element is used to support electronic prescribing for the consistent expression of patient directions for use by relaying this information between a prescriber and a pharmacist. It must be legible, unambiguous, and complete to ensure the prescriber's instructions for use of the medication are understood. For each transaction, the technology must be able to receive and transmit the reason for the prescription using the indication elements in the SIG Segment.

Comments. One commenter requested that the Sig element be required rather than optional to aid in future medication reconciliation and clinical reporting. Another commenter noted that the NCPDP SCRIPT standard version 2017071 allows for an increase in Sig length.

Response. Given the lack of attention paid to and support for modifying the electronic prescribing criterion for Sig from optional to required, we have decided to retain Sig as optional in the updated § 170.315(b)(3) criterion. As discussed in the Reason for Prescription section, health IT may optionally seek certification to the updated electronic prescribing criterion by demonstrating their capacity to receive and transmit the reason for the prescription using the Sig element.

xx. Real Time Pharmacy Benefit

While development is still currently underway by NCPDP, the Real-Time Pharmacy Benefit (RTPB) standard is not yet complete. When complete, the RTPB standard is expected to facilitate the ability for pharmacy benefit payers/processors to communicate formulary and benefit information to providers. In the absence of that or another similar standard, CMS has adopted policies requiring the development and/or implementation of Real Time Benefit Transaction (RTBT) standards in the Part D e-Rx Program in the context of recent rulemaking. On May 16, 2019, CMS issued the Modernizing Part D and Medicare Advantage to Lower Drug Prices and Reduce Out-of-Pocket Expenses final rule, which includes a requirement under the electronic prescribing standards that Part D plan sponsors implement one or more electronic real-time benefit tools that are capable of integrating with at least one prescriber's electronic prescribing system or electronic health record no later than January 1, 2021 (84 FR 23832). One commenter recommended that CMS and ONC coordinate with NCPDP on requirements for real-time benefit functionality. We are also aware of industry efforts to develop a consumer-facing real-time pharmacy benefit functionality FHIR®-based implementation guide that we anticipate will be balloted in 2020. ONC will continue to monitor these efforts and consider proposing the NCPDP RTPB standard or a similar standard to enable real-time benefit transactions in future rulemaking.

xxi. Other Comments Received Outside the Scope of This Rule

We note that we received several comments specifically addressing the electronic prescribing of controlled substances and prescription drug monitoring programs. We note that these specific comments are outside the scope of the proposals finalized in this rule. However, we note that we included a discussion of these topics in relation to the discussion of the RFI on OUD prevention and treatment in the Proposed Rule in 84 FR 7461.

5. Clinical Quality Measures—Report Criterion

In the 2015 Edition final rule, ONC adopted four clinical quality measure (CQM) certification criteria, § 170.315(c)(1) CQMs—record and export, § 170.315(c)(2) CQMs—import and calculate, § 170.315(c)(3) CQMs—report, and § 170.315(c)(4) CQMs—filter (80 FR 62649 through 62655). These four criteria were adopted with the intent to support providers' quality improvement activities and in electronically generating CQM reports for reporting with certified health IT to programs such as the EHR Incentive Programs, Quality Payment Program, and Comprehensive Primary Care plus initiative. The ''CQMs—report''

certification criterion (§ 170.315(c)(3)) included an optional certification provision for demonstrating that the health IT can create Quality Reporting Document Architecture (QRDA) reports in the form and manner required for submission to CMS programs, which is in accordance with CMS' QRDA Implementation Guide (IGs).

The CMS QRDA IGs provide technical guidance and specific requirements for implementing the HL7 QRDA Category I (QRDA I) and Category III (QRDA III) standards for reporting to CMS quality reporting programs.[45] The CMS QRDA IGs include the formal template definitions and submission criteria for submitting QRDA documents to the Comprehensive Primary Care Plus (CPC+) and Merit Based Incentive Payments System (MIPS) Programs. Some of the conformance statements in the HL7 QRDA standards have been further constrained to meet the specific requirements from these CMS programs. The CMS QRDA IGs also only list the templates specifying CMS-specific reporting requirements from the base HL7 QRDA standards. QRDA I is an individual-patient-level report. It contains quality data for one patient for one or more electronic clinical quality measures (eCQMs). QRDA III is an aggregate quality report. A QRDA III report contains quality data for a set of patients for one or more eCQMs.

Since the 2015 Edition final rule was published, we have gained additional certification experience and received feedback from the industry that health IT certified to the ''CQMs—report'' criterion (§ 170.315(c)(3)) are only/primarily being used to submit eCQMs to CMS for participation in CMS' programs. Therefore, as a means of reducing burden, we proposed to remove the HL7 CDA® Release 2 Implementation Guide: QRDA I; Release 1, Draft Standard for Trial Use (DSTU) Release 3 (US Realm), Volume 1 (§ 170.205(h)(2)), as well as the QRDA Category III, Implementation Guide for CDA® Release 2 (§ 170.205(k)(1)) and the Errata to the HL7 Implementation Guide for CDA® Release 2: QRDA Category III, DSTU Release 1 (US Realm), September 2014 (§ 170.205(k)(2)) standard requirements (HL7 QRDA standards) from the current 2015 Edition CQMs—report criterion in § 170.315(c)(3), and we also proposed to require that health IT certified to the current 2015 Edition CQMs—report criterion support the CMS QRDA IGs (84 FR 7446). We stated that this change would directly reduce burden on health IT developers and indirectly providers as they would no longer have to develop and support two forms of the QRDA standard.

We also solicited comment in the Proposed Rule on the future possibility of FHIR-enabled APIs replacing or complementing QRDA-based quality reporting. We also noted in the Proposed Rule that the Fast Health Interoperability Resources (FHIR®) standard offers the potential for supporting quality improvement and reporting needs, and holds the potential of being a more efficient and interoperable standard to develop, implement, and utilize to conduct quality reporting through APIs. We believe until the potential benefits of FHIR® APIs can be realized for quality reporting, and that solely requiring the CMS QRDA IGs for the updated 2015 Edition ''CQMs—report'' criterion will balance the burden on developers, while still ensuring module users' abilities to meet their quality reporting obligations to CMS (84 FR 7446).

To support the proposal, we proposed to incorporate by reference in § 170.299 the latest annual CMS QRDA IGs, specifically the 2019 CMS QRDA I IG for Hospital Quality Reporting[46] (§ 170.205(h)(3)) and the 2019 CMS QRDA III IG for Eligible Clinicians and Eligible Professionals (§ 170.205(k)(3)).[47] We noted in the Proposed Rule that developers would be able to update certified health IT to newer versions of the CMS QRDA IGs through the real world testing Maintenance of Certification provision for standards and implementation specification updates in § 170.405(b). We also proposed that a Health IT Module would need to be certified to both standards to ensure flexibility for Health IT Module users. We solicited comment on whether to consider an approach that would permit certification to only one of the standards depending on the care setting for which the Health IT Module is designed and implemented.

Comments. The majority of commenters were supportive of the proposal to remove the HL7 QRDA standard requirements from the 2015 Edition CQMs—report criterion in § 170.315(c)(3), and to require that health IT certified to the criterion support the proposed CMS QRDA IGs. Some commenters observed that the main use cases for the certified QRDA export functionality (which is specific to CMS eCQMs) are to support direct data submission to CMS at the conclusion of reporting periods, to enable use of third party data submission Health IT Modules to meet CMS reporting requirements, and to support data extraction for registry reporting for participation in CMS programs such as MIPS. Commenters noted that while in some cases the extraction of data using a QRDA may also support other use cases—for example for a registry—because of the specificity of the criteria to the CMS eCQMs, such a transaction using the certified functionality is primarily for CMS reporting. Commenters noted the use of the CMS QRDA IG does not impede use of the data for other purposes. Finally, commenters noted that ONC should continue to provide health IT developers the flexibility to offer a non-certified QRDA functionality that could support eCQMs beyond those included for CMS programs. One commenter observed that while some health IT systems also provide tools for internal quality performance monitoring, those tools often do not rely on the generation of QRDA exports.

Some commenters reported that the technical support of multiple versions of QRDA standards is unnecessary. Other commenters recommended maintaining only the HL7 standard or offering certification to the HL7 standard as an optional alternative to the CMS QRDA IG. One commenter who recommended maintaining both the HL7 standard and the CMS QRDA IGs suggested that ONC cite the CMS version(s) of the QRDA IG as a technical resource in the same manner the C–CDA companion guide is cited for the transition of care criteria and only require certifying to the HL7 version. These commenters agreed that developers should not have to certify to both HL7 QRDA and CMS QRDA IGs, but suggested if a developer passed certification for the CMS QRDA IGs, they should be deemed to have achieved certification to the HL7 QRDA standard as well. Commenters noted that the CMS QRDA apply specifications to the HL7 QRDA to support CMS eCQM reporting requirements.

Other commenters specifically stated that the HL7 QRDA should remain as an optional certification criterion, since other organizations (*e.g.,* certain hospital accreditation organizations such as The Joint Commission) use the

[45] The following resources provide additional information on the differences between the CMS QRDA and the HL7 QRDA standards: *https://ecqi.healthit.gov/system/files/QRDA_HQR_2019_CMS_IG_final_508.pdf* (pg. 38) and *https://ecqi.healthit.gov/sites/default/files/2019-07/2020-CMS-QRDA-III-Eligible-Clinicians-and-EP-IG-07182019-508.pdf* (pg. 18).

[46] *https://ecqi.healthit.gov/system/files/QRDA_HQR_2019_CMS_IG_final_508.pdf.*

[47] *https://ecqi.healthit.gov/system/files/2019_CMS_QRDA_III_Eligible_Clinicians_and_EP_IG-508.pdf.*

HL7 QRDA, and there is need to assure the same style for submission across programs. They recommended that the HL7 QRDA IG persist as a continuing option in the Program to enhance alignment with other standards and C–CDA, and to encourage a base standard alignment across implementers such as CMS and The Joint Commission. They stated that citing only to the CMS QRDA IG may lead to misalignment with the base standards and reduce incentives to update the base standard.

Some commenters expressed concern over the proposed removal of HL7 QRDA standards from the original 2015 Edition CQMs, stating it may undermine private sector efforts to self-regulate and stated that the removal of the HL7 QRDA may not achieve the envisioned burden reduction through the mere elimination of developers' need to certify and maintain multiple standards. While some commenters suggested that removing HL7 QRDA from the certification criteria could simplify the reporting process by recognizing the widespread use of CMS' QRDA IGs, they noted that the HL7 QRDA is currently the standard for most EHR systems and questioned how ONC proposed to implement this change given the prominence of HL7 standards in EHR systems. Several commenters noted that the disconnect between what the certification testing required, and how the standard was really being used in the industry (primarily but not exclusively to meet the CMS QRDA IG) created unnecessary certification testing burden, and asserted that the adoption of the CMS proprietary IG was more appropriate than to maintain HL7 QRDA.

Response. We thank commenters for their support for the proposal and comments regarding the versions of standards. We understand the concerns expressed in opposition to this proposal, and we appreciate specifically the identification of potential risk for the elimination of the HL7 standard as applicable for other use cases. As noted previously, since the 2015 Edition final rule was published (October 16, 2015), we have gained received feedback from the industry that health IT certified to the ''CQMs—report'' criterion (§ 170.315(c)(3)) are only or primarily being used to submit eCQMs to CMS for participation in CMS' programs. In addition, we note that while the HL7 QRDA may be used for other purposes, the ''CQMs—report'' criterion (§ 170.315(c)(3)) is specific to the CMS eCQMs specified for participation in CMS reporting programs and no other eCQMs are tested under that criterion. This specificity applies not only to the current 2015 Edition ''CQMs—report'' criterion, but also to the other 2015 Edition CQM criteria and the prior 2014 Edition CQM criteria. This specificity is intended to provide assurances through testing and certification of the accuracy and standardization of CMS program measures across platforms, while recognizing that it would not be possible to specifically test to the entire universe of potential eCQMs in use by health care providers. Because of this dependency, testing and certification of both the HL7 QRDA for CQMs-report and the CMS QRDA IG is redundant to support eCQM data reporting.

This has a dual impact on our considerations to finalize our proposal to require only the CMS QRDA IG. First, for use cases that are not related to CMS eCQM reporting, the certified functionality would not specifically support third party non-CMS eCQM reporting requirements, and so the modification to the functionality does not change the inability to use the certified version of the functionality for such purposes. Second, for those use cases involving registries or other third parties that are implementing or supporting CMS eCQM reporting, use of the CMS QRDA IG could additionally support such purposes. In addition, we are not restricting health IT developers from creating and providing to customers a non-certified functionality that supports the HL7 QRDA for the extraction of data for eCQMs that are not CMS eCQMs. We note that this is not a change from the prior policy allowing such flexibility. The prior certification for the QRDA IG included testing of CMS eCQMs only and it neither supported nor restricted any development of a QRDA functionality for non-CMS eCQMs.

We also agree that this approach will support closer alignment between the testing to the CMS QRDA IG specifications for a certified health IT module and the technical requirements for CMS program reporting. As part of the development of the CMS QRDA IGs, CMS strives to use the annual update process to resolve issues with CQMs based on updates to clinical guidelines and to advance the requirements as the standard for reporting eCQM data matures. In this way, aligning the criterion to the CMS program requirements that it specifically supports allows for alignment between these efforts as well as allowing for continued updates through the standards version advancement process. We also believe our finalized proposal will not impede private sector initiatives as the CMS IGs support the continued efforts by public/private collaboration through standards developing organizations (SDOs) to refine standards.

Therefore, as a means of reducing burden, we have finalized our proposal to remove the HL7 QRDA standard requirements from the 2015 Edition CQMs—report criterion in § 170.315(c)(3). We maintain our position that this would directly reduce burden on health IT developers and indirectly for health care providers as there would no longer be a requirement to develop and support two forms of the QRDA standard. We note that this does not preclude developers from continuing to support the underlying standard, especially where such standard may support reporting or health information exchange for other quality or public health purposes. Instead, we are simply not requiring testing and certification of any such standards, thereby eliminating testing and certification burden from a criterion that is at this time scoped to the purpose of reporting for CMS quality programs.

Comments. A few commenters did not support the proposal but instead recommended that CMS adopt the HL7 QRDA standard and do away with its own. However, several commenters offered suggestions to CMS on the development of the CMS QRDA IG and the alignment to the HL7 QRDA standard. A number of commenters noted the National Technology Transfer and Advancement Act of 1995 principle that Federal agencies are generally required to use technical standards that are developed by voluntary consensus standards bodies rather than a proprietary standard specific to an HHS program. Commenters also stated if CMS wanted to retain certain aspects of its standard, it should work with HL7 to get these vetted, balloted and approved for inclusion within the HL7 standard. Commenters also recommended working with SDOs or other organizations to sufficiently support CMS QRDA IGs. Some commenters suggested that consolidation of QRDA standards would be more likely result in reducing provider burdens than what ONC proposed.

Response. We thank the commenters for their recommendations to improve the CMS QRDA IGs, or for CMS to work toward including the aspects of CMS QRDA IGs that they require for their program operations in SDO-balloted and approved consensus standards. Specific suggestions for CMS IG development are outside the scope of this rule. ONC had previously included the HL7 QRDA standards for certification in the 2015 Edition in order to potentially support a broader range of use cases than

reporting for CMS programs. However, the specificity of the criterion to the CMS eCQMs limits the utility of the certified functionality beyond use with CMS eCQMs and as stated in the Proposed Rule, since the 2015 Edition final rule, ONC and CMS received significant stakeholder feedback that health IT modules certified to the ''CQMs—report'' criteria at 170.314(c)(3) in the 2014 Edition and 170.315(c)(3) for the 2015 Edition are used only or primarily for reporting to CMS programs. While we reiterate that these comments are outside the scope of this rule, we will continue to take this and other feedback into consideration and will continue to work with CMS, standards developing organizations, and health IT industry partners to explore the concerns raised in relation to reducing burden and promoting interoperable standards for quality reporting.

Comments. Commenters provided mixed feedback on whether the updated 2015 Edition ''CQMs—report'' criterion should require adherence to both CMS QRDA IGs, specifically the 2019 CMS QRDA I IG for Hospital Quality Reporting [48] and the 2019 CMS QRDA III IG for Eligible Clinicians and Eligible Professionals.[49] The majority of commenters recommended that to reduce burden, ONC should consider a certification approach that permits developers to seek certifications based on the care setting(s) their health IT modules are intended serve. For example, commenters suggested that ONC should only require certification to the 2019 QRDA I IG for Hospital Quality Reporting if a Health IT Module is designed exclusively for the reporting of hospital measures, and only require certification to the 2019 QRDA III IG for Eligible Clinicians and Eligible Professionals when a Health IT Module is designed exclusively for the reporting of ambulatory measures. In instances in which both populations are served, the developer would then seek certification to both standards. Commenters suggested this approach would avoid the unnecessary burden of certifying to a standard that the Health IT Module was not intended to serve. Other commenters stated that the certification requirements should ensure that certified Health IT Modules can support quality measure reporting by all potential users, especially given the potential expansion of eligible participants in certain CMS programs (*e.g.,* should a program expand from hospital-based only to include ambulatory measures). These commenters recommended the adoption of a requirement for certified Health IT Modules to calculate and export both CMS QRDA I patient-level reports for Hospital Quality Reporting and CMS QRDA III aggregate summary reports for Eligible Clinicians and Eligible Professionals. These commenters noted that if a certified Health IT Module can only send an aggregate report without a patient level report, then this would greatly diminish the ability to verify the underlying calculations. However, commenters recommended that ONC clarify that the transition to CMS QRDA I IG-based reports (patient-level, QRDA I IG for Hospital Quality Reporting) does not necessarily mean that a hospital quality measure must be certified by any system (*i.e.,* an ambulatory Health IT Module can certify to only CMS QRDA III IG requirements). Commenters also sought clarity that the transition to QRDA III reports (aggregate-level, IG for Eligible Clinicians and Eligible Professionals) does not necessarily mean that an ambulatory quality measure must be certified by any system (*i.e.,* a hospital system can certify to only hospital measures). Finally, one commenter noted that certifying ambulatory quality measures for the QRDA I to a hospital IG is not effective and will interfere with the use case of using QRDA I to combine data between multiple ambulatory systems such as for group reporting.

Response. We thank commenters for their comments regarding whether a Health IT Module should be certified to both CMS QRDA IG standards or whether to consider an approach that permits certification to only one of the standards depending on the care setting for which the Health IT Module is designed and implemented. We agree with commenters that our certification approach should prevent unintended burden by tailoring the requirements to the type of measures being tested. This would mean that for the updated certification criterion ''CQMs—report'' in § 170.315(c)(3) a Health IT Module testing only ambulatory measures would test only with the CMS QRDA III IG for ambulatory measures and a Health IT Module testing only inpatient measures would test only with the QRDA I CMS IG for inpatient measures. A Health IT Module supporting both ambulatory and inpatient measures would be required to test to both the CMS QRDA I IG and the CMS QRDA III IG. We clarify that testing for the 2015 Edition ''CQM—capture and export'' criterion in § 170.315(c)(1) criteria includes demonstrating the capability to export a QRDA I report specific to the eCQM being tested—which would support use case noted by the commenter to combine data across multiple ambulatory systems. We have not proposed and have not finalized a change to the 2015 Edition ''CQM—capture and export'' criterion in § 170.315(c)(1). We further note that health IT developers may leverage QRDA file formats for a wide range of use cases and that our inclusion of the CMS QRDA I and QRDA III IGs does not prohibit the use of the QRDA standard for any other purpose. As noted above, we have finalized the adoption of the CMS QRDA IGs for the ''CQMs—report'' criterion in § 170.315(c)(3) for which the Health IT Module is presented for certification.

Comments. The majority of commenters supported the proposal to adopt the latest CMS QRDA IGs at the time of final rule publication, as CMS updates their QRDA IGs annually to support the latest eCQM specifications and only accepts eCQM reporting to the latest version. However, a few commenters recommended that ONC monitor this part of the certification process for unintended consequences since CMS' IGs are updated on a yearly basis. Some commenters noted that given the lack of alignment with timing, eCQM measures and standards will continue to lack testing. Other commenters recommended the IGs be updated in alignment with updates to the certification standards. A few commenters requested clarification of the effective dates and asked ONC to evaluate and propose a timeline for the implementation of an alignment between the programs. In addition, commenters asked for clarification on whether ONC will propose penalties for providers who may be unable to meet the timeline if it is insufficient.

Response. We thank commenters for their input and have adopted the latest CMS QRDA IG versions available at the time of publication of this final rule. For details on the latest CMS QRDA IGs, we refer readers to the CMS QRDA I Implementation Guide for Hospital Quality Reporting and CMS QRDA III Implementation Guide for Eligible Clinicians and Eligible Professionals available on the eCQI Resource Center website.[50] We note that CMS updates

[48] *https://ecqi.healthit.gov/system/files/QRDA_HQR_2019_CMS_IG_final_508.pdf.*

[49] *https://ecqi.healthit.gov/system/files/2019_CMS_QRDA_III_Eligible_Clinicians_and_EP_IG-508.pdf.*

[50] The Electronic Clinical Quality Improvement (eCQI) Resource Center. CMS QRDA I Implementation Guide for Hospital Quality Reporting and CMS QRDA III Implementation Guide for Eligible Clinicians and Eligible

Continued

the CMS eCQMs on an annual basis as well as the CMS QRDA IGs for reporting to CMS programs. As in prior years going back to the 2014 Edition, HHS will continue to update the Cypress testing tool to support health IT developer testing to the most recent annual update. We note that CMS has previously required that EHR technology used for eCQM reporting be certified to all eCQMs but does not need to be recertified each time it is updated to a more recent version of the eCQM electronic specifications, unless the EHR technology is supporting new eCQMs or functionality (such as the ''CQM—filter'' criterion in § 170.315(c)(4)) (84 FR 42505). This approach allows for continued updates to and testing of eCQMs while minimizing the burden on developers and providers to support those updates in time for each annual performance period. Finally, we note that ONC has no authority to set requirements, incentives, or penalties for health care providers related to the use of health IT, and we direct readers to CMS for information on health IT requirements in CMS programs.

Comments. The majority of commenters agreed with ONC's assessment in the Proposed Rule that quality reporting is not yet ready to transition to FHIR and that more testing and validation of FHIR is needed before requiring a new API-based reporting functionality as a part of the Program. Some commenters supported the adoption of FHIR Release 4-enabled APIs as a replacement for QRDA-based reports, but stated that published documentation aligning HL7 C–CDA, QRDA, and/or FHIR standards to CMS' ''Quality Data Model,[51]'' which is an information model that defines relationships between patients and clinical concepts in a standardized format to enable electronic quality performance measurement and that would allow for more consistent eCQM reporting and improved interoperability in clinical quality feedback between health systems and data registries. Other commenters stated that FHIR standards will likely strengthen standardized data element availability and flexibility to improve the types of eCQMs that may be developed, and suggested that CMS continue to work with the National Quality Forum, measure stewards, and measure developers to advance both existing evidence-based measures (*e.g.,* either administrative or hybrid measures) and evolving outcome measures that utilize population-based electronic clinical data.

Response. We thank commenters for their support. We believe there are potential benefits to be gained by exploring both near-term, program specific implementations of APIs to support current quality reporting submission mechanisms such as for CMS eCQM reporting as well as the long-term potential to reimagine quality measurement by leveraging API technologies. We believe that these technology approaches could help providers and payers, including CMS, move from the current approach, in which providers are required to calculate and submit results on specific quality measures, to one in which payers, including CMS, could obtain clinical data for quality measurement directly through an API. This could potentially include the ability to obtain clinical data for a defined group or sample set of patients to assess quality across patient populations, as well as to compare clinical data for patients over time to assess quality impacts through longitudinal measurement. We believe emerging innovative standards are now available to support such models, specifically the ability to respond with clinical data for a defined group or sample set of patients using the bulk data capabilities in FHIR Release 4. We note that readiness for such an approach, both for recipients of quality data and for health IT developers supporting quality improvement solutions, is not yet mature for adoption of such a criterion in the Program. However, we are committed to continuing to work with HHS partners, health care providers, health IT developers and SDOs to explore the potential for such solutions in the future.

Comments. Several commenters recommended additional changes not considered in the Proposed Rule. For example, one commenter recommended ONC require that to be certified in § 170.315(c)(1) ''CQMs—record and export,'' § 170.315(c)(2), ''CQMs—import and calculate,'' and § 170.315(c)(3) ''CQMs—report,'' a Health IT Module be certified in a minimum of 9 eCQMs instead of one eCQM and that the § 170.315(c)(1) criterion should require the ability to export all patients for a given eCQM. Currently, the ability to export a QRDA I file can be limited to one patient at a time. Commenters noted that this limitation defeats the purpose of data interoperability and does not advance the goals of ONC to increase access to data and the interoperability of Health IT Modules. And another commenter recommended that, in addition to the adoption of the CMS IGs under the § 170.315(c)(3) criterion, that the CMS IGs replace the corresponding HL7 QRDA IGs as ONC's Program standard under the § 170.315(c)(1) criterion (which currently references QRDA I exclusively) and § 170.315(c)(2) criterion (which currently references only QRDA I as standard, but also involves use of QRDA III for purposes of verifying appropriate calculation of measures from imported QRDAs).

Response. We thank commenters for input and clarifications. While we appreciate comments suggesting changes to § 170.315(c)(1) ''CQMs—record and export,'' and § 170.315(c)(2) ''CQMs—import and calculate,'' the recommended changes are outside the scope of our proposal. Therefore, while we may consider these recommendations for future Program rulemaking, we have not adopted the suggested changes to § 170.315(c)(1) ''CQMs—record and export,'' or § 170.315(c)(2) ''CQMs—import and calculate in this final rule.

As noted previously, we have finalized the update to the ''CQMs—report'' criterion in § 170.315(c)(3) to require that health IT developers use the CMS QRDA IG appropriate to the measures being submitted for testing and certification to read as follows: ''*Clinical quality measures—report.* Enable a user to electronically create a data file for transmission of clinical quality measurement data in accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in § 170.205(h)(3) and CMS QRDA, category III, for ambulatory measures in § 170.205(k)(3).''

6. Electronic Health Information (EHI) Export Criterion

We proposed to adopt a new 2015 Edition certification criterion referred to as ''EHI Export'' in § 170.315(b)(10). The criterion's conformance requirements were intended to support two contexts in which we believed that all EHI produced and electronically managed by a developer's technology should be made readily available for export as a capability of certified health IT. First, we proposed in § 170.315(b)(10)(i) at 84 FR 7447 that health IT certified to this criterion would support single patient EHI export upon a valid request by a patient or a user on the patient's behalf. Second, we proposed in § 170.315(b)(10)(ii) at 84 FR 7447 that the proposed criterion would support the export of all EHI when a health care

Professionals. Available at: *https://ecqi.healthit.gov/qrda.*

[51] *https://ecqi.healthit.gov/qdm.*

provider chooses to transition or migrate information to another health IT system. Third, we proposed in § 170.315(b)(10)(iii) that the export format(s) used to support the exports must be made available via a publicly accessible hyperlink, including keeping the hyperlink up-to-date with the current export format.

At the time of the Proposed Rule, we indicated our belief that this proposed certification criterion provided a useful first step toward enabling patients to have electronic access to their EHI and equipping health care providers with better tools to transition patient EHI to another health IT system. We noted that this criterion would create a baseline capability for exporting EHI. We requested comments regarding the proposed single patient EHI export and the proposed database export functionalities, as well as the proposed scope of data export and other criterion elements throughout the Proposed Rule section at 84 FR 7447 through 7449.

Comments. Commenters generally supported the intent of the proposed ''EHI export'' criterion to advance the access, exchange, and use of EHI. Commenters in favor of the criterion and its proposed conformance requirements stated that it would foster innovative export capabilities and inform areas where additional standards development could be needed. We also received a variety of comments asking for adjustments to proposed requirements. A majority of commenters requested revisions to the criterion, including calling for a defined set of data elements for export and specific data transport standards. Many commenters offered recommended standards or requested that we provide specific standards to reduce variation. These commenters indicated that no defined standard could lead to broad interpretation and potential inadequacies of the data export. Some commenters expressed a medical record keeping concern that the proposed standards-agnostic approach for the export functionality could be problematic, stating that the export could create a dissonance if the EHI renders health record content in a form or format that is different from what a provider produces or utilizes as output. Other commenters opposed the adoption of this proposed criterion. These commenters expressed concern that later implementation of standards, such as APIs, would make developers invest time and funding into the proposed requirements only for the work to be discarded in the future.

Response. We thank commenters for their feedback on the proposed ''EHI export'' criterion at 84 FR 7446 of the Proposed Rule (§ 170.315(b)(10)). We have considered commenters' concerns, support, and recommendations and adopted a revised version of this certification criterion. This final certification criterion is designed to align with section 4006(a) of the Cures Act, which requires the Secretary, in consultation with the National Coordinator, to promote policies that ensure that a patient's EHI is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient's health care providers and other individuals (84 FR 7447). In addition, this criterion complements other provisions that support patients' access to their EHI and health care providers use of EHI, such as the secure, standard-based API certification criterion (proposed in 84 FR 7427 and finalized in § 170.315(g)(10)), and also supports longitudinal data record development. Therefore, we have finalized the criterion with revisions. Notably, in response to comments on this criterion and the proposed information blocking policies, we have adopted a focused definition of EHI in § 170.102 and § 171.102. For context purposes, the EHI definition is focused on ''electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501'' with additional caveats not repeated here for briefness. Put simply, the EHI definition represents the same ePHI that a patient would have the right to request a copy of pursuant to the HIPAA Privacy Rule. This is a regulatory concept with which the industry has nearly 20 years of familiarity. Health IT developers' customer base includes health care providers who are HIPAA covered entities, and in many cases developers serve as HIPAA business associates to their covered-entity customers. Thus, health IT developers should be accustomed to identifying ePHI so that their products support appropriately securing it, the fulfillment of patient access requests, and the identification and reporting on breaches. They should, therefore, be well prepared to identify what EHI their product(s) would need to export in order to support a patient's HIPAA right of access. The finalized criterion requires a certified Health IT Module to include export capabilities for a single patient (§ 170.315(b)(10)(i)) and patient population (§ 170.315(b)(10)(ii)) related to EHI. More specifically, the export(s) will need to include the EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. We emphasize that such ''stored'' data applies to all EHI and is agnostic as to whether the EHI is stored in or by the certified Health IT Module or in or by any of the other ''non-certified'' capabilities of the health IT product of which the certified Health IT Module is a part. The scope of EHI applies across the product as a whole as a means to further promote the access, exchange, and use of EHI for the use cases required to be supported by this certification criterion. The finalized scope of data included in the criterion export is discussed in greater detail under the ''Scope of Data Export'' (IV.B.6.c) section below.

While the data that must be exported has been more specifically scoped, the certification criterion does not require a specific standard format be used for the purposes of representing the exported EHI. We also modified the certification criterion's documentation requirements in § 170.315(b)(10)(iii) to be more concise. As finalized, the documentation required for the export format(s) used to support (b)(10)(i) and (ii) functionality must be kept up-to-date and made available via a publicly accessible hyperlink. Additional information is included under ''Export Format'' below.

We appreciate the comments received regarding the specific data sets and data transmission standards for this certification criterion. We reiterate that the finalized certification criterion is specific to EHI, as defined, that can be stored at the time of certification by the product, of which the Health IT Module is part, and is not limited to a predefined data set or to specific data transmission standards. Developers are required to ensure the health IT products they present for certification are capable of exporting all of the EHI that can be stored at the time of certification by the product. We acknowledge that the amount of EHI exported and format in which such EHI is represented will differ by developer and products of which certified Health IT Modules are a part. Each product presented for certification, of which the Health IT Module is a part, will likely vary in the amount of EHI it can store. As a result, the amount of EHI that will need to be able to be exported in order to demonstrate conformance with this certification criterion will vary widely because of the diversity of products presented for certification. For example, small software components only capable of storing a certain scope of EHI (and only certified to a few certification criteria) will only need to be able to

export that stored EHI in order to meet this certification criterion. In contrast, a more comprehensive product with an EHI storage scope well beyond all of the adopted certification criteria would by its nature need to demonstrate it could export a lot more EHI. But even in this latter case, it is important to note that while that scope of EHI may be comprehensive for that product, it may still not be all of the health information for which a health care provider is the steward and that meets the EHI definition within the health IT products deployed within their organization. In other words, a health IT user may have other health IT systems with no connection to the Certification Program that store EHI and such EHI would still be in scope from an information blocking perspective. We note all of these distinctions to make clear for and to dissuade readers from jumping to an improper conclusion that the EHI export criterion in the Certification Program is a substitute for or equivalent to the EHI definition for the purposes of information blocking. We direct readers to the information blocking section (VIII) for additional information. Unless a health care provider (which is an ''actor'' regulated by the information blocking provision) only used a single health IT product to store EHI that was also certified to this certification criterion, the EHI definition will always be larger. Regardless of the amount of EHI each product has within its scope to export, the purpose of this certification criterion is to make the EHI already available in such health IT products more easily available for access, exchange, and use by patients and their providers, which is a fundamental principle established by the Cures Act.

As technology continues to advance, and as stated in the Proposed Rule at 84 FR 7447, this criterion may not be needed in the future. However, the comments suggesting we not adopt this certification criterion at all because it will be outmoded at some point in the future did not appear to acknowledge that all technology is eventually replaced for a variety of reasons. We too look forward to a day where standards-based APIs are the predominant method for enabling electronic health information to be accessed, exchanged, and used. We strongly encourage industry partners to engage in their own consortiums, with ONC and other Federal agencies, and other stakeholders in the health IT ecosystem to advance standards development, prototypes, and pilot testing in order to ultimately build a body of evidence that could accelerate the adoption and implementation timeline of technology that could either add more structure to or remove the need for this certification criterion in the future. However, we do not accept the promise of this future state as a reason to simply wait, nor do we believe that the potential of this future justifies delaying the incremental progress the industry can make. In this case, had we followed such commenters direction, we would be withholding from patients and health care providers the certainty that there would be technical capabilities within a defined time that could be used to enable the access, exchange, and use of EHI. We note that suggestions by commenters to structure the certification criterion to only move information within specific data sets or via specific standards-based export functionality would delay the ability of patients and users of health IT to access, exchange, and use the information they need and would run counter to the underlying principles supporting this certification criterion—that the electronic health information should be accessible for access, exchange, and use. For this reason, we have not included specific data set or export requirements in this certification criterion as some commenters suggested.

In consideration of comments, the finalized ''EHI export'' criterion in § 170.315(b)(10) is not included in the 2015 Edition Base EHR definition, which is a modification from what we proposed. We revised the policy in recognition of comments received, including comments regarding the structure and scope of the criterion as proposed and the development burden of the criterion. As finalized here, we believe that including this certification criterion in the Conditions and Maintenance of Certification is the best place to include the requirement associated with the criterion. Thus, we have finalized the § 170.315(b)(10) certification criterion as a general certification requirement for the ONC Health IT Certification Program, and have not included it in the 2015 Edition Base EHR Definition.

In general, we also note that those who use Health IT Module(s) certified to the ''EHI export'' criterion remain responsible for safeguarding the security and privacy of individuals' EHI consistent with applicable laws and regulations related to health information privacy and security, including the HITECH Act, HIPAA Privacy and Security Rules, 42 CFR part 2, and State laws. The existence of a technical capability to make EHI more accessible and useable by Health IT Module users does not alter or change any of their data protection responsibilities under applicable laws and regulations.

Comments. Comments received included concerns with the development and use of the certification criterion. Some commenters expressed support for the criterion's overall flexibility but cautioned ONC to be realistic regarding the goals and expectations for the certification criterion. These commenters also expressed concern that the proposed certification criterion would result in development for an ambiguous scope of data export and would divert from work needed to achieve other interoperability goals. Other commenters stated concerns that development costs could potentially be passed onto health IT users, such as health care providers. These commenters also anticipated use and implementation challenges for users that work with multiple systems.

Response. We thank commenters for sharing their concerns. In regards to the use of the capabilities required by this certification criterion, we interpreted from comments some confusion related to potential ''users'' of the health IT. As previously defined under the Program, ''user'' is a health care professional or their office staff; or a software program or service that would interact directly with the certified health IT (80 FR 62611, 77 FR 54168).

We also appreciate the comments and concerns regarding the potential development burden that could result to meet the requirements of the proposed criterion. In consideration of those expressed concerns, we have narrowed the scope of data that must be exported. This more focused scope should measurably reduce the stated ambiguity by commenters and development burden for health IT developers in contrast to what was proposed (84 FR 7448). We appreciate the concerns expressed for the potential user(s) of Health IT Modules, but note that the certification criterion is designed to advance the electronic movement of data out of a product while factoring in the current variability in health IT. As always, we encourage developers to seek innovative and expedient capabilities that, at minimum, meet the requirements of the certification criterion, as well as the developing needs of their health IT users.

Comments. Commenters provided alternative ideas for the criterion specific to USCDI. Some recommended amending the criterion to require the specific structure and applicable standards for USCDI elements, or starting this criterion with a minimum of USCDI data elements. Several commenters recommended expanding

the existing 2015 Edition ''data export'' criterion to include USCDI in lieu of the proposed ''EHI export'' criterion.

Response. We thank commenters for sharing these ideas. We have finalized the ''EHI export'' criterion as described above. Our intent under this finalized criterion is to advance export functionality for single patient and patient population EHI exports, while leaving flexibility in regard to format and without assigning specific data sets due to the different scopes of data that health IT may include. Toward those ends, limiting the scope of this certification criterion to solely the data represented by the USCDI would make it no different than other USCDI bounded certification criteria already adopted and would not advance the policy interests we have expressed. In regards to comments on the existing 2015 Edition ''data export'' criterion (§ 170.315(b)(6)), we refer readers to our discussion of the criterion below.

Comments. Some comments expressed confusion and asked for guidance on how this certification criterion would apply to health IT that is no longer certified. Commenters also asked for guidance on how this criterion applies to other systems that interact with Health IT Modules certified to this criterion based on the proposed scope of data for export.

Response. We thank commenters for requesting clarification. We first clarify that the export functionality under this certification criterion applies to Health IT Modules presented for certification under the Program. More specifically, if a health IT developer presents for certification a health IT product of which a Health IT Module is a part and the product electronically stores EHI, certification to § 170.315(b)(10) is required. As noted in our response above, this would include the EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. This includes all EHI stored by the product's certified and ''non-certified'' capabilities. For example, if a health IT product includes a component(s) that is presented for certification and that component stores EHI, then that EHI must be made available for export, in accordance with § 170.315(b)(10). Importantly, the scope of data required to be exported in accordance with § 170.315(b)(10) includes only to the EHI that can be stored at the time of certification by the product. We emphasize that such ''stored'' data applies to all EHI and is agnostic as to whether the EHI is stored in or by the certified Health IT Module or in or by any of the other ''non-certified'' capabilities of the health IT product of which the certified Health IT Module is a part. The scope of EHI applies across the product as a whole as a means to further promote the access, exchange, and use of EHI for the use cases required to be supported by this certification criterion.

a. Single Patient Export To Support Patient Access

As part of this criterion, we proposed a functionality for single patient EHI export at 84 FR 7447 which would enable a user of certified health IT to timely create an export file(s), with the proposed scope of data export of all of the EHI the health IT product produces and electronically manages on a single patient. The functionality would also require a user to be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate. In addition, we proposed that health IT certified to this criterion would be required to enable the ability to limit the users who could create such export file(s) in at least one of two ways: To a specific set of identified users, and (2) as a system administrative function. We also proposed that the export file(s) created must be electronic and in a computable format and that the export file(s) format, including its structure and syntax, must be included with the exported file(s).

Comments. We received many comments in support of the proposal for single patient export to support patient access under the certification criterion. The majority of these commenters provided recommended revisions, including suggested transmission formats and data export content standards. Some commenters recommended the addition of this certification criterion to the list of criteria subject to real world testing.

Response. We thank commenters for their feedback. We have finalized the single patient export functionality in § 170.315(b)(10)(i) with some modifications. We finalized a focused data export scope, which applies to the data expected to be available for export under the single patient export capability. We defined the scope of data that needs to be exported to EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. Thus, we have modified the title of § 170.315(b)(10)(i) to ''single patient electronic health information export'' to reflect the scope of this data export. We finalized that the capability for a user to execute a single patient export must be able to be limited at least one of two ways: To a specific set of identified users, and as a system administrative function. While we finalized as proposed in § 170.315(b)(10)(i)(D) that the export files must be electronic and in a computable format, we modified in § 170.315(b)(10)(ii)(E) that the publicly accessible hyperlink of the export's format must be included with the exported file(s). This modification clarifies that the user is able to access the format, and that the developer will keep their hyperlink up-to-date.

We appreciate commenter's recommendations for specific data transmission formats and data content standards, and considered the range of recommendations when developing the finalized scope of data export required for this criterion. We believe the definition of EHI as focused in § 171.102, as well as the modifications to the scope of data export, addresses the data ambiguity concerns received by commenters. We direct readers to our detailed discussion of the scope of data export below. As finalized, the certification criterion's export, for both single and patient population EHI Export, remain standards-agnostic. We believe that the finalized certification criterion will serve as an initial step towards increased access, exchange, and use of electronically available data. We will continue working alongside industry stakeholders and will revisit export strategies as standards continue to develop and mature. We appreciate confirmation that commenters support inclusion of the criterion in § 170.315(b)(10) alongside the rest of the care coordination criteria in § 170.315(b), and have finalized that this certification criterion is part of the real world testing Condition of Certification requirement.

Comments. Some commenters asked ONC to clarify how health IT developers may limit the users' ability to access and initiate the export function in § 170.315(b)(10)(i), and to include examples of potential permissible and non-permissible behaviors.

Response. We appreciate the comments received. We again clarify that ''user'' is a health care professional or their office staff; or a software program or service that would interact directly with the certified health IT (80 FR 62611, 77 FR 54168). In regards to questions on permissible behaviors for developers, the ability to limit the health IT users' access to the single patient EHI export functionality in § 170.315(b)(10)(i) is intended to be used by and at the discretion of the organization implementing the technology. We reiterate that similar to the 2015 edition ''data export'' criterion in § 170.315(b)(6), this cannot be used by health IT developers as a way to

thwart or moot the overarching user-driven aspect of this capability (80 FR 62646). We do not wish to limit this functionality to specific permissible or non-permissible behaviors at this time, but reaffirm in § 170.315(b)(10)(i)(B) that a user must be able to execute the single patient EHI export capability at any time the user chooses and without subsequent developer assistance to operate. To be clear, the user must be able to execute the export without the intervention of the developer. We also finalize, as proposed, in § 170.315(b)(10)(i)(C) that this capability must limit the ability of user who create such export files(s) in at least one of two ways; (1) to a specific set of identified users, and (2) as a system administrative function.

Comments. The majority of comments received asked for further clarity on ''timely'' regarding a health IT user's request to create an export file(s).

Response. We thank commenters for the questions. We specify that ''timely'' means near real-time, while being reasonable and prudent given the circumstances.

Comments. Commenters also sought clarity on data in electronic health records that may be shared between patients and possibly included in the export. These commenters asked if under the proposed criterion, patients have a right to information about others that may be contained in their medical record.

Response. We thank commenters for submitting these questions. In regards to shared patient data concerns, we note that the export functionality requirements apply to what a product with a Health IT Module certified to this criterion must be able to do regardless of whether the developer is operating the export for a health care provider or a health care provider is maintaining and operating the technology in their own production environment. Under the HIPAA Privacy Rule, when a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual's family medical history, this information may become part of the medical record for that individual and thus be included in the ''designated record set'' (defined at 45 CFR 164.501)). Thus, if the family medical history becomes part of the designated record set, the individual/patient may exercise the right of access (45 CFR 164.524) under the HIPAA Privacy Rule to this information in the same fashion as any other information in the medical record. The HIPAA Privacy Rule does not prevent individuals, themselves, from gathering medical information about their family members or from deciding to share this information with family members or others, including their health care providers. Thus, individuals are free to provide their doctors with a complete family medical history or communicate with their doctors about conditions that run in the family. To the degree that, for example, Patient A's medical record include that their mother had breast cancer, that information would be accessible to Patient A because it was provided by Patient A and included as part of their medical record. Under this criterion, patients would not have a ''right'' to other patient's records, consistent with existing laws. In general, with respect to patient access to information, we note that Health IT Module users must ensure that any disclosures of data conform to all applicable laws and regulations, including but not limited to alignment between this rule and the HIPAA Privacy Rule, as discussed in IV.B.6 above. We also refer readers to the information blocking section at VIII in this preamble, as well.

Comments. Commenters requested clarity on how ONC will monitor a developer's compliance with exporting in a timely manner and what penalties ONC will impose if there is a delay in regards to a Health IT Module user's request. Commenters requested ONC release sub-regulatory guidance that describes how users may file complaints and recommended ONC work with the HHS Office for Civil Rights (OCR) on patient education.

Response. Any noncompliance by developers with the finalized ''EHI export'' certification criterion (§ 170.315(b)(10)) or the associated Conditions and Maintenance of Certification requirements (*e.g.,* § 170.402(a)(4) and (b)(2)) would be subject to review, corrective action, and enforcement procedures under the Program. We refer readers to the enforcement (VII) and information blocking (VIII) sections of this preamble for further information. We do not believe there is a general need to work with OCR further on this particular issue or to issue further sub-regulatory guidance. The functionality of the ''EHI export'' criterion in § 170.315(b)(10) provides a user (*e.g.,* a health care provider) with the ability to export a file for a single patient and multiple patients. If a user or other stakeholder has concerns about ongoing compliance of health IT certified to this criterion, with the required functionality of the criterion, or the associated Conditions and Maintenance of Certification requirements, they may file a complaint with the health IT developer, an ONC–ACB, or ONC.

Comments. Some commenters requested specific stakeholder exemptions from this requirement, such as health plans.

Response. We thank commenters for the recommendations. We note that the ''EHI export'' criterion is applicable only to health IT products presented by developers for certification under the Program that meet the criterion and ''Assurances'' Condition of Certification requirements in § 170.402. In addition, we note that the information subject to the export requirements is EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part.

i. EHI Export for Patient-Initiated Requests

In the Proposed Rule, we reiterated that the ''user'' of the single patient export functionality would typically be a provider or their office staff on behalf of the patient (80 FR 62611, 77 FR 54168). We also recognized that in service to innovative and patient-centric approaches, a health IT developer could develop a method that allows a patient to execute the request for data export without needing a provider to do so on their behalf. Under this scenario, we sought comments on whether the single patient export functionality should be made more prescriptive and require that the developers design the health IT to allow only the patient and their authorized representative to be the requestor of their EHI (84 FR 7447).

Comments. In the scenario of patient-centric approaches created by developers, the majority of commenters were in favor of developers designing the export capability to make the patient and their authorized representative able to be the direct requestors of their EHI without needing a provider to execute this capability on their behalf. We also received recommended terms to further define ''authorized representative'' under this scenario. Several commenters advised against specifying or restricting the potential additional user roles able to initiate a single patient export. Some commenters recommended additional requirements for developers, including requiring developers to create this capability to enable the patient or their ''proxy'' to request their information through and receive information from the patient's health portal or an application. Commenters asked for the final rule to include clarification on what the patient and their authorized representative can access. We did receive some comments that requested clarification of this potential approach.

We also received comments expressing confusion with the patient and authorized representative requests applying across the certification criterion, as opposed to the proposed and previously defined ''users'' of health IT that will typically perform the request on behalf of a patient.

Response. We thank commenters for their input and requests for clarification. In response to the concerns and potential confusion, we clarify the following. This certification criterion does not require ''direct-to-patient'' functionality in order to demonstrate conformance. Providing such a capability and demonstrating conformance to this certification criterion with such a capability would be at the sole discretion of the health IT developer. In general, just like with the ''data export'' criterion in § 170.315(b)(6), the capability to execute this certification criterion can be health care provider/health care organization initiated (presumably upon that organization receiving a request by patient for their EHI). In instances where the functionality certified to this criterion is implemented in a ''direct-to-patient'' way such that the patient can request and accept EHI export without assistance from a user, we recognize that further configuration of the functionality or product in which it is implemented may be needed in order to account for applicable laws related to the patient's information access rights and other privacy and information blocking policies that apply to the configuration and use of the Health IT Module. While this specific capability within the certification criterion emphasizes health IT developer assistance must not be needed to operate the export, we recognize that user assistance (*e.g.,* a provider) may be necessary to initiate such capability in the user's product.

b. Patient Population EHI Export for Transitions Between Health IT Systems

In addition to the single patient export functionality in § 170.315(b)(10)(i), we proposed in § 170.315(b)(10)(ii) that health IT certified to this criterion would also facilitate the migration of EHI to another health IT system. We proposed that a health IT developer or health IT certified to this criterion must, at a user's request, provide a complete export of all EHI that is produced or electronically managed (84 FR 7447 through 7448) by means of the developer's certified health IT.

Comments. We received many comments in support of the functionality under this criterion for transitions between health IT systems. Many commenters recommended format and content specifications, such as the use of bulk FHIR®-based APIs for export transmission. Some commenters stressed that ONC should determine and require standards, as well as clarify the scope of data export specific to this use case. Some commenters expressed concerns, including gathering patient consent and the developer burden that may exist with gathering data from disparate systems under the proposed scope terminology. One commenter was against the transitions between health IT systems capability, citing that data structured for one system will not necessarily work in another.

Response. We thank commenters for their feedback specific to the functionality of transitions between health IT systems under this criterion. We finalized this export functionality with modifications. First, this functionality is now referred to as ''patient population electronica health information export'' in § 170.315(b)(10)(ii) to better reflect the policy intent of patient data transitions in instances of providers switching health IT systems, and to reflect the finalized scope of data that a product with a certified Health IT Module must be capable of exporting. Similar to the modifications in § 170.315(b)(10)(i), we finalized in § 170.315(b)(10)(ii)(A) that the export files must be electronic and in a computable format and we modified in § 170.315(b)(10)(ii)(B) that the publicly accessible hyperlink of the export's format must be included with the exported file(s). This modification clarifies that the user is able to access the format, and that the developer will keep their hyperlink up-to-date.

In response to comments on defining a separate scope of data export specific to the patient population export functionality, it is our final policy for this certification criterion to align both the single patient and patient population export data to EHI, as defined in this rule, that can be stored at the time of certification by the product, of which the Health IT Module is a part. This narrower scope also addressed concerns received regarding development burden expressed regarding gathering data from disparate systems under the proposed scope terminology.

In regards to the comments on enforcing format and standards for data transmission, it is our intent under this certification criterion that health IT developers have flexibility regarding how the export outcome is achieved. We again encourage the industry to work together toward this common goal and to create an industry-wide approach. We do acknowledge the comments received that data structured for one system may not necessarily seamlessly align with another, and refer commenters to the export format requirements of this certification criterion. As finalized in § 170.315(b)(10)(ii)(A), the export created must be electronic and in a computable format. In contrast with the single patient EHI export capability, which must be available to a user without subsequent developer assistance to operate, the patient population EHI export capability of this criterion could require action or support on the part of the health IT developer. We acknowledged in the Proposed Rule (84 FR 7448) that because of anticipated large volume of electronic health information that could be exported under this specific proposed capability, developer action or support could be needed. Our thinking remains the same post-public comments even with the narrowed scope of data export. While exporting one patient's data on an as-needed basis is a capability that should be executable by a user on their own, orchestrating an entire export of EHI for migration to another health IT system is an entirely different task and dependent on a variety of factors such as the organization's overall infrastructure and deployment footprint. Additionally, developers of health IT certified to this criterion are required to provide the assurances in § 170.402, which include providing reasonable cooperation and assistance to other persons (including customers, users, and third-party developers) to enable the use of interoperable products and services. Thus, while developers have flexibility regarding how they implement the export functionality for transitions between systems, they are ultimately responsible for ensuring that the capability is deployed in a way that enables a customer and their third-party contractors to successfully migrate data. Such cooperation and assistance could include, for example, assisting a customer's third-party developer to automate the export of EHI to other systems. We refer readers to the export format section below for additional details.

We note that the narrowed scope of data that certified Health IT Modules must be capable of exporting does not reduce contractual obligations of health IT developers to continue to support providers if they do want to change systems, and direct readers to the information blocking section (VIII) for additional information.

c. Scope of Data Export

We proposed in 84 FR 7448 and in § 170.315(b)(10) that for both use cases supported by this criterion, the scope of data that the certified health IT product must be capable of exporting would encompass all the EHI that the health IT system produces and electronically manages for a patient or group of patients. Our intention was that ''produces and electronically manages'' would include a health IT product's entire database. In the Proposed Rule, our use of the term EHI was deliberate. At the time of rulemaking, the proposed definition of the EHI term in § 171.102 was intended to support the consistency and breadth of the types of data envisioned by this proposed criterion. We requested comment on the terminology used (''produces and electronically manages'') or whether there were alternatives to the proposed language.

Comments. Some commenters were supportive of our proposed scope of data export requirements, while a few others offered alternative specific terminology options. Those commenters suggested terminology such as all EHI the health IT system ''collects and retains,'' or ''produces or can electronically access, exchange, or use.'' A majority of commenters, however, stated that the proposed terminology, including the proposed EHI definition, left broad interpretations of the scope of data a Health IT Module would have to be capable of exporting under this criterion. These commenters expressed concerns that the ambiguity and potentially vast amounts of data would create undue burden on health IT developers for development and upkeep of export capabilities, as well as compliance issues with other applicable laws. A majority of commenters requested and highlighted a need for further specificity regarding the terminology used to define data exported under this criterion. Some commenters expressed concerns that a developer presenting a Health IT Module for certification may not know all systems a user may later connect to the health IT capabilities. We also received many comments reflecting varied thoughts on what should or should not be included in the criterion's data export. Some commenters strongly opposed any data limits, citing existing regulations such as the HIPAA Privacy Rule right of access, while others proposed alternatives to constrain data export requirements, citing development infeasibility.

Recommendations to constrain the proposed criterion's scope included alignment with other regulations and data standards, such as the USCDI. We also received a recommended requirement for health IT developers to provide a plain language definition of the EHI typically included in their Health IT Module's export. Some commenters expressed confusion on how the criterion's proposed scope of data export may apply to EHI ''produced or electronically managed'' by both the product's certified and ''non-certified'' capabilities as well as data from third parties.

Response. We thank commenters for feedback on our proposed terms and for specific recommendations. The finalized criterion draws the upper bound of its data scope from the focused definition of EHI as finalized. The criterion export includes the EHI, as defined, that can be stored at the time of certification by the product, of which the Health IT Module is a part. As defined in this rule, EHI means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501 (other than psychotherapy notes as defined in 45 CFR 164.501 or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding), regardless of whether the actor is a covered entity as defined in 45 CFR 160.103. In response to comments received, this revised scope of data for export provides a more manageable and less administratively burdensome certification criterion for health IT developers for several reasons.

We agree with commenters that our proposed terms of all EHI a health IT system ''produces and electronically manages'' (84 FR 7448) raised the potential for broad variance in interpretations and concerns about the breadth of data intended for export under this criterion and potential development burden. We also considered the comments noting that a developer presenting a Health IT Module for certification may not, at the time of certification, know all systems a user will later connect to the health IT capabilities. Ultimately, we considered several approaches to better reflect the policy intent and to alleviate confusion related to the proposed criterion. In consideration of the public comments and the policy outcome we sought to address, we revised the final criterion's phrasing to describe what information health IT products with Health IT Module(s) certified to the criterion must be capable of exporting. The revised scope of data export applies to both the single patient and patient population export functionalities as well as the Conditions and Maintenance of Certification requirements tied to this criterion.

First, we agree with comments received and acknowledge that a health IT developer is best positioned to know (and would be solely responsible for only) the EHI that can be stored by the health IT product at the time the Health IT Module is presented for certification. In response to comments regarding the applicability of the scope of export to the product's certified and ''non-certified'' capabilities, as well as data from third parties, we clarify and reiterate the following from our prior responses. We emphasize that such ''stored'' data applies to all EHI and is agnostic as to whether the EHI is stored in or by the certified Health IT Module or in or by any of the other ''non-certified'' capabilities of the health IT product of which the certified Health IT Module is a part. To be clear, conformance ''at the time of certification'' means the combined data that can be stored by the product, of which the Health IT Module is a part, at the time the Health IT Module is presented for certification. As such, for the purposes of this certification criterion, the EHI that must be exported does not include any data generated from unique post-certification in response to a particular customer (though such data could meet the definition of EHI for the purposes of information blocking). Such modifications could include custom interfaces and other data storage systems that may be subsequently and uniquely connected to a certified Health IT Module post-certification. Additionally, to remain consistent with ''at the time of certification,'' we clarify that any new EHI stored by the product due to ongoing enhancements would need to be included within the scope of certification only when a new version of the product with those new EHI storage capabilities is presented for certification and listing on the CHPL. In consideration of comments, we believe that this approach to define storage at the time the product is presented for certification of a Health IT Module will make the certification requirements more clear for health IT developers and more efficient to administer from a Program oversight perspective.

In addition, the use of ''can be stored by'' refers to the EHI types stored in and by the health IT product, of which the Health IT Module is a part. This is meant to be interpreted as the combination of EHI a heath IT product stores itself and in other data storage locations. Thus, the cumulative data

covered by these storage techniques would be in the scope of data export.

Per our policy intent, by focusing the definition of EHI and defining the data for export under this criterion, users of certified Health IT, such as health care providers, will have the ability to create ''readily producible'' exports of the information of a single patient upon request by the user, which increases patient access as reflected in the Cures Act. Lastly, in support of the second functionality we finalized for patient population export, the EHI exported (within the Health IT product's scope of data export) would likely be of significant importance to health care providers for the purposes of transitioning health IT systems and maintaining continuity of care for patients, and also helps remove potential barriers to users switching systems to meet their needs or their patient's needs.

In finalizing this policy, we emphasize that health IT developers may provide the export of data beyond the scope of EHI and for functionalities beyond those discussed under this criterion. In such cases, for additional export purposes, it is advised that health IT developers and users discuss and agree to appropriate requirements and functionalities. We again emphasize that health IT product users must ensure that any disclosures of data conform to all applicable laws, including the HIPAA Rules and 42 CFR part 2. Stakeholders should review applicable laws and regulations, including those regarding patients' right of access to their data, in order to determine the appropriate means of disclosing patient data. We also refer readers to the information blocking section at VIII.

i. Image, Imaging Information, and Image Element Export

In the Proposed Rule, we noted at 84 FR 7448 that clinical data would encompass imaging information, both images and narrative text about the image. However, we addressed that EHRs may not be the standard storage location for images. We solicited additional feedback and comments on the feasibility, practicality, and necessity of exporting images and/or imaging information. We requested comment on what image elements, at a minimum, should be shared such as image quality, type, and narrative text. We did not make any proposals in 84 FR 7448.

Comments. Most commenters were supportive of sharing images and/or related data elements, expressing that interoperability should include electronic ordering of imaging studies, which they asserted would assist health care providers in delivering care. Other commenters expressed burden concerns with data image export, particularly challenges around the movement and storage of large amounts of data and accumulating data from disparate health IT systems. A few commenters requested specific exclusion of images or videos created as a byproduct of procedures. As for minimum image data elements to share, recommendations varied and included Digital Imaging and Communications in Medicine (DICOM™) data elements or file type recommendations. Comments included additional policy recommendations, such as making Picture Archiving and Communication Systems (PACS) developers subject to certification rules and requiring EHI export data to include links for remote authorized access to externally hosted images.

Response. We thank commenters for their shared insight and recommendations regarding the export of images, imaging information, and image elements. Health IT Modules certified to the finalized criterion must electronically export all of the EHI, as defined, that can be stored at the time of certification by the product, of which the Health IT Module is a part. Thus, any images, imaging information, and image elements that fall within this finalized scope of EHI that can be stored at the time of certification in or by the product, of which the Health IT Module is a part will need to be exported under this certification criterion. We appreciate the recommendations received for image transfer methods and encourage the stakeholder community to continue exploring innovative image transfer methods, including for image transfer that would fall outside of this certification criterion. We appreciate the policy recommendations, such as including PACS developers. The ''EHI export'' certification criterion only applies to developers of health IT seeking or maintaining certification under the Program. To the extent such providers are developers of health IT under the Program they would be included. If they are not developers under the Program, they would not be included.

We also thank commenters for their suggestions to require data export to include links for remote authorized access to externally hosted images. We note that the export requirements of this certification criterion refers to the EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. In the context of imaging, if the only EHI stored in or by the product to which this certification criterion applies are links to images/imaging data (and not the images themselves, which may remain in a PACS) then only such links must be part of what is exported. We encourage developers to work with their customers to achieve innovative ways to share all relevant data, including situations outside of the scope of data export under this criterion where images could be made more accessible.

ii. Attestation of Information a Health IT Developer Cannot Support for Export

In the Proposed Rule (84 FR 7448), we also solicited comment on whether we should require, to support transparency, health IT developers to attest or publish as part of the export format documentation the types of EHI they cannot support for export. We did not have any specific proposals.

Comments. The majority of commenters supported public attestation regarding the information a Health IT Module is unable to export. Some commenters requested that we add to the regulatory text to state that developers attest to information they cannot support for export ''and/or ingestion.'' Some commenters questioned if it is fair for EHI developers to delineate what is in their Health IT Module's scope of data for export under this criterion. Another felt that this requirement should be extended to health care delivery organizations and that the attestation should be included within patient portals or other communications.

Response. We thank commenters for their feedback. We again note the revised scope of data export under this finalized criterion. Under the finalized approach, which focuses on the export of the EHI that can be stored at the time of certification by the product, we have determined that our final requirements provide sufficient clarity and have not included any additional requirements such as those on which we sought comment. Additionally, we believe the recommendation for ingestion would be impracticable as part of this certification criterion due to the flexibility we permit for the output format(s). It would not be possible from a regulatory enforcement perspective to administer a certification criterion that included within its scope a conformance requirement for a Health IT Module's capability to import any proprietary format that may exist without prior knowledge of such formats.

iii. Export Exclusion Request for Comments

In the Proposed Rule, we proposed metadata categories at 84 FR 7448 for

exclusion from this criterion. We also requested feedback on what metadata elements should remain included for export or added to the list of excluded data. Metadata proposed for exclusion from the criterion included metadata present in internal databases used for physically storing the data, metadata that may not be necessary to interpret the EHI export, and metadata that refers to data that is not present in the EHI export. Examples of these proposed exclusions are provided at 84 FR 7448.

Comments. Commenters offered varied recommendations for metadata elements to remain excluded, or to be included under the scope of data export for this criterion. We received several comments strongly supporting the inclusion of audit log metadata. Commenters noted that the inclusion of audit log metadata had potential legal utility and could aid in the patient's ability to have all of their data and knowing who has accessed their data. Commenters also requested increased clarity on the definition of metadata, audit log, and access log in regards to this rulemaking, and requested the use of standards to further clarify policy intentions. We note, however, that other commenters were against the inclusion of audit log data as part of the EHI export. Those against inclusion stated that this information was not necessary to interpret the EHI export, could be burdensome for development of export capabilities, and potentially contain personally identifiable information of the health care staff.

Response. We thank commenters for their input on potential metadata exclusions. As noted above, we have finalized that EHI that can be stored at the time of certification by the product is the scope of data that must be included in exports pursuant to § 170.315(b)(10). Under this revised and specified scope of data export, it is no longer necessary to list specific metadata exclusions or inclusions. We direct readers to the discussion of scope of data export (IV.B.6.c) under this criterion for further details.

d. Export Format

We did not propose a content standard for the export. However, we did propose to require documentation in § 170.315(b)(10)(iii) that health IT developers include the export file(s) format, including its structure and syntax, such as a data dictionary or export support file, for the exported information to assist the user requesting the information in processing the EHI (84 FR 7448). This was to prevent loss of information or its meaning to the extent reasonably practicable when using the developer's certified Health IT Module(s). We also proposed in § 170.315(b)(10)(iii) that the developer's export format must be made available via a publicly accessible hyperlink and kept up-to date.

Comments. Comments received were in favor of this proposal in § 170.315(b)(10)(iii). Several commenters were supportive of the flexibility of export format for developers, as long as export documentation is provided as specified in the Proposed Rule, citing specifically how this would support the export capability in § 170.315(b)(10)(ii). Some commenters recommended additional clarification for the publicly accessible hyperlink, specifically to ensure that information is available without login or other associated requirements. Commenters also provided export format suggestions.

Response. We thank commenters for their feedback regarding developers' export format. We have finalized § 170.315(b)(10)(iii) with modifications to clarify the regulatory text. We finalized that the export format(s) used to support § 170.315(b)(10)(i) and § 170.315(b)(10)(ii) of this section must be kept up-to-date.

We clarify that the documentation for the export format(s) in § 170.315(b)(10)(iii) consists of information on the structure and syntax for how the EHI will be exported by the product such as, for example, C–CDA document(s) or data dictionary for comma separated values (csv) file(s), and not the actual EHI. The user will use the export format documentation to process the EHI after it is exported by the product. We also require that health IT developers keep the export format(s) used to support § 170.315(b)(10)(i) and § 170.315(b)(10)(ii) must be ''up-to-date.'' For example, if the health IT developer had previously specified the C–CDA standard as the export format for meeting the criterion, but subsequently updated their product to use the FHIR standard and stopped supporting C–CDA export format then the documentation for export format would need to be updated so that users are able to continue to accurately process the EHI exported by the product. We appreciate suggestions received regarding ensuring that such information is available without login or other associated requirements. In response to these comments, our policy intent to foster transparency, and in alignment with other certification criterion requirements set forth in this rule, we note our modifications in § 170.315(b)(10)(i)(E) and § 170.315(b)(10)(ii)(B) that the publicly accessible hyperlink of the export's format must be included with the exported file(s). We clarify that the hyperlink must allow any person to directly access the information without any preconditions or additional steps. We note that the export format need not be the same format used internally by the certified health IT and the health IT developer does not need to make public their proprietary data model. This certification criterion also does not prescribe how (*i.e.,* media/medium) the exported information is to be made available to the user, as this may depend on the size and type of information to be exported. While file formats and related definitions are not finalized as specific certification requirements, we encourage developers to continue to foster transparency and best practices for data sharing, such as machine-readable format, when they create and update their export format information.

e. Initial Step Towards Real-Time Access

In the Proposed Rule at 84 FR 7449, we offered a clarifying paragraph to highlight that the criterion in § 170.315(b)(10) was intended to provide a step in the direction of real-time access goals, as well as a means to, within the confines of other applicable laws, encourage mobility of electronic health data while other data transfer methods were maturing. In that section, we clarified that ''persistent'' or ''continuous'' access to data is not required to satisfy the proposed ''EHI export'' criterion's requirements, and that the minimum requirement of developers presenting Health IT Module(s) for certification to this criterion is for a discrete data export capability. In this clarification section, we did not have specific proposals or requests for comments.

Comments. We received recommendations to further specify the use of ''persistent'' and ''continuous'' in context of access to EHI. Additional commenters recommended specifying Representational state transfer (REST) or ''RESTful'' transfer, or specifying data transport methods.

Response. We thank commenters for their input. We first clarify that this section was added to the Proposed Rule for additional clarification and to provide prospective context on the proposed certification criterion. However, we recognize from the comments received that our reference to ''persistent'' or ''continuous'' access in the Proposed Rule may have created confusion. We again note that ''persistent'' or ''continuous'' access is not required by health IT developers

presenting Health IT Module(s) to satisfy the requirements of this certification criterion. We have finalized the ''EHI export'' criterion as described above in response to comments received on proposals we have made. We appreciate the responses to our future looking points in the Proposed Rule but have not made further revisions to the final certification criterion in response.

f. Timeframes

We requested input and comments on the criterion and timeframes at 84 FR 7449. In particular, beyond the proposal to export all the EHI the health IT system produces and electronically manages, we sought comment on whether this criterion should include capabilities to permit health care providers to set timeframes for the EHI export, such as only the ''past two years'' or ''past month'' of EHI (84 FR 7449).

Comments. A majority of commenters were against the concept of allowing providers to set timeframes for the export functionality. Commenters were concerned that creating the capability to limit timeframes would involve significant technical complexity for health IT developers. Commenters also expressed concern that allowing providers the capability to limit timeframes would not align with the HIPAA Privacy Rule right of access at 45 CFR 164.524 and could potentially implicate information blocking. Commenters provided alternative approaches and concepts to implement timeframe capabilities for this criterion, including use of APIs, granting flexibility to developers, allowing intervals or dynamic timeframe requirements, and considering permitted fees. Commenters asked for clarification on how far back the data request capabilities could go and requested clarification regarding how this criterion aligns with other API-related criteria within this rule.

Response. We thank commenters for their feedback. We will not require the Health IT Module support a specific or user-defined timeframe range or time limit capability for the purposes of demonstrating conformance to this certification criterion. We agree with commenters concerns regarding potential development complexity for health IT developers if we included such a requirement upfront. What this means, however, is that for the purposes of testing and certification, a health IT developer will need to prove that the product, of which a Health IT Module is part, can perform the capabilities required by the certification criterion, inclusive of all EHI that could be exported. In turn, when these capabilities are deployed in production they will need to be capable of exporting all of the EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. We also agree with the points received regarding the HIPAA Privacy Rule right of access at 45 CFR 164.524 and emphasize the importance of HIPAA covered entities aligning with applicable law regarding patient access to health information.

g. 2015 Edition ''Data Export'' Criterion in § 170.315(b)(6)

We proposed to remove the ''data export'' criterion (defined in § 170.315(b)(6)) from the 2015 Edition Base EHR definition in § 170.102 and to replace ''data export'' with the proposed ''EHI export'' criterion (defined in § 170.315(b)(10)) by amending the third paragraph of the 2015 Edition Base EHR definition in § 170.102. We did not propose a transition period for the ''data export'' criterion. Rather, we proposed to remove the criterion from the 2015 Edition Base EHR definition upon the effective date of a final rule. We also proposed to modify the 2015 Edition Base EHR definition to include the new proposed export criterion (defined in § 170.315(b)(10)), with an implementation date 24 months from the effective date of the final rule. We welcomed comments on this approach.

Comments. Some commenters were in favor of immediate removal of this criterion (§ 170.315(b)(6)) from the 2015 Edition Base EHR definition, stating it would reduce burden. However, the majority of commenters were against a potential gap in functionality due to the compliance timeline for the new export criterion (§ 170.315(b)(10)) and requested that we keep the ''data export'' criterion until the new criterion in § 170.315(b)(10) and other standardized data transmission methods were fully implemented. Some commenters supported an indefinite retention of the ''data export'' criterion, regardless of the proposed addition of § 170.315(b)(10). Several commenters also recommended to expand the current § 170.315(b)(6) criterion through USCDI as an alternative approach to the proposed ''EHI export'' criterion in § 170.315(b)(10). In addition, some commenters expressed concern that that the ''data export'' criterion is inconsistent with CMS Quality Payment Program (QPP) requirements such as View, Download, and Transmit (VDT) at 83 FR 59814 of the CY 2019 Physician Fee Schedule final rule.

Response. In consideration of public comments in support of the retention of the ''data export'' certification criterion, we have maintained the ''data export'' certification criterion in § 170.315(b)(6) as available for certification until 36 months after this final rule's publication date. To implement this decision, we have finalized in § 170.550(m) that ONC–ACBs are permitted to issue certificates to ''data export'' in § 170.315(b)(6) until, but not after, 36 months after the publication date of this final rule. However, we note the ''data export'' certification criterion has been removed from the 2015 Edition Base EHR definition (in § 170.102) as of the general effective date of this final rule (60 days after its publication in the **Federal Register**). During the 36 months immediately following publication of this final rule, developers will be able to maintain the certification to § 170.315(b)(6) as a standardized means of exporting the discrete data specified in the CCDS, but the criterion will not be updated to the USCDI. Given that certification to the § 170.315(b)(6) criterion will no longer be available after 36 months, we do not believe an update to the USCDI is the best path. Rather, § 170.315(b)(6) will remain an unchanged criterion in the Program for the 36 months immediately following publication of this final rule in the **Federal Register**. After that timeframe, the EHI export criterion in § 170.315(b)(10), including that certification criterion's scope of data export, will remain an available data export certification criterion for health IT developers that present for certification a Health IT Module that is part of a heath IT product which electronically stores EHI. This approach will support prior investments in § 170.315(b)(6) by developers and their customers, and also encourage movement toward the interoperability opportunities afforded by new criteria.

Regarding commenter concerns that the ''data export'' criterion is inconsistent with CMS QPP requirements, such as View, Download and Transmit (VDT), we do not believe that this criterion would be inconsistent with QPP program requirements. In the CY 2019 Physician Fee Schedule final rule, CMS removed the VDT measure in § 170.315(e)(1) (83 FR 59814). However, the Promoting Interoperability performance category of QPP currently includes the measure entitled Provide Patients Electronic Access to their Health Information (83 FR 59812 through 59813), and CMS has identified technology certified to the ''View, Download and Transmit to 3rd party'' criterion at 45 CFR 170.315(e)(1) as required to meet this measure (83 FR

59817). The Data Export criterion in § 170.315(b)(6) is not required for the Provide Patients Electronic Access to their Health Information measure included in the Promoting Interoperability performance category, nor have we proposed to change the ''View, Download and Transmit to 3rd party'' criterion in § 170.315(e)(1) required for this measure, thus we do not believe this final policy will conflict with CMS requirements for QPP.

7. Standardized API for Patient and Population Services Criterion

We proposed to adopt a new API criterion in § 170.315(g)(10) at 84 FR 7449. In response to comments, we are adopting a Standardized API for Patient and Population Services criterion for Certification in § 170.315(g)(10) with modifications. The new criterion, will replace the old ''application access—data category request'' certification criterion (§ 170.315(g)(8)). In doing so, we are also adding the Standardized API for Patient and Population Services criterion to the updated 2015 Edition Base EHR definition and removing the application access—data category request criterion (§ 170.315(g)(8)). This finalized Standardized API for patient and population services certification criterion requires the use of the FHIR Release 4 and several implementation specifications. The new criterion focuses on supporting two types of API-enabled services: (1) Services for which a single patient's data is the focus and (2) services for which multiple patients' data are the focus. Please refer to the ''Application Programming Interfaces'' section (VII.B.4) in this preamble for a more detailed discussion of the ''API'' certification criterion and related Conditions and Maintenance of Certification requirements.

8. Privacy and Security Transparency Attestations Criteria

In 2015, the HIT Standards Committee (HITSC) recommended the adoption of two new ''authentication'' certification criteria for the Program (81 FR 10635). The National Coordinator endorsed the HITSC recommendations for consideration by the Secretary, and the Secretary determined that it was appropriate to propose adoption of the two new certification criteria through rulemaking. To implement the Secretary's determination, we proposed two new criteria to which health IT would need to be certified (84 FR 7450). These would require the developer to attest to whether the Health IT Module for which they are seeking certification to the criteria encrypts authentication credentials (§ 170.315(d)(12)) and/or supports multi-factor authentication (§ 170.315(d)(13)). We did not propose to *require* that health IT have these authentication and encryption-related functions, but instead proposed that a health IT developer must indicate whether or not their certified health IT has those capabilities by attesting ''yes'' or ''no.'' We did, however, propose to include the two criteria in the 2015 Edition privacy and security certification framework (§ 170.550(h)). For clarity, attesting ''yes'' to either of these criteria indicates that the Health IT Module can support either Approach 1 or Approach 2 of the 2015 Edition privacy and security certification framework for these criteria.

We note that we received many comments on the proposed ''encrypt authentication credentials'' and ''multi-factor authentication'' criteria, but the majority of comments conflated the two proposals and provided collective responses. Therefore, we have responded to them in kind to preserve the integrity of the comments.

a. Encrypt Authentication Credentials

We proposed in 84 FR 7450 to adopt an ''encrypt authentication credentials'' certification criterion in § 170.315(d)(12) and include it in the P&S certification framework (§ 170.550(h)). We proposed to make the ''encrypt authentication credentials'' certification criterion applicable to any Health IT Module currently certified to the 2015 Edition and any Health IT Module presented for certification that is required to meet the ''authentication, access control, and authorization'' certification criterion adopted in § 170.315(d)(1) as part of Program requirements.

Encrypting authentication credentials could include password encryption or cryptographic hashing, which is storing encrypted or cryptographically hashed passwords, respectively. If a developer attests that its Health IT Module encrypts authentication credentials, we proposed in 84 FR 7450 that the attestation would mean that the Health IT Module is capable of protecting stored authentication credentials in accordance with standards adopted in § 170.210(a)(2), Annex A: Federal Information Processing Standards (FIPS) Publication 140–2, ''Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules.'' We posited that FIPS Publication 140–2 is the seminal, comprehensive, and most appropriate standard. Moreover, in the specified FIPS 140–2 standard, there is an allowance for various approved encryption methods, and health IT developers would have the flexibility to implement any of the approved encryption methods in order to attest ''yes'' to this criterion. We noted that health IT developers should keep apprised of these standards as they evolve and are updated to address vulnerabilities identified in the current standard.

We did not propose that a Health IT Module would be required to be tested to the ''encrypt authentication credentials'' certification criterion. Rather, by attesting ''yes,'' the health IT developer is attesting that if authentication credentials are stored, then the authentication credentials are protected consistent with the encryption requirements above. We proposed in 84 FR 7450 that the attestations ''yes'' or ''no'' would be made publicly available on the Certified Health IT Product List (CHPL). We proposed in 84 FR 7450 that, for health IT certified prior to the final rule's effective date, the health IT would need to be certified to the ''encrypt authentication credentials'' certification criterion within six months after the final rule's effective date. For health IT certified for the first time after the final rule's effective date, we proposed that the health IT must meet the proposed criterion at the time of certification.

We also noted that some Health IT Modules presented for certification are not designed to store authentication credentials. Therefore, we specifically requested comment on whether we should include an explicit provision in this criterion to accommodate such health IT. We stated that this could be similar to the approach we utilized for the 2015 Edition ''end-user device encryption'' criterion (§ 170.315(d)(7)(ii)), where we permit the criterion to be met if the health IT developer indicates that their health IT is designed to prevent electronic health information from being locally stored on end-user devices.

b. Multi-Factor Authentication

We proposed in 84 FR 7450 to adopt a ''multi-factor authentication'' (MFA) criterion in § 170.315(d)(13) and include it in the P&S certification framework (§ 170.550(h)). We proposed to make the ''multi-factor authentication'' certification criterion applicable to any Health IT Module currently certified to the 2015 Edition and any Health IT Module presented for certification that is required to meet the ''authentication, access control, and authorization'' certification criterion adopted in § 170.315(d)(1) as part of Program requirements. To provide clarity as to what a ''yes'' attestation for ''multi-factor authentication'' attestation would

mean, we provided the following explanation. MFA requires users to authenticate using multiple means to confirm they are who they claim to be in order to prove one's identity, under the assumption that it is unlikely that an unauthorized individual or entity will be able to succeed when more than one token is required. MFA includes using two or more of the following: (i) Something people know, such as a password or a personal identification number (PIN); (ii) something people have, such as a phone, badge, card, RSA token or access key; and (iii) something people are, such as fingerprints, retina scan, heartbeat, and other biometric information. Thus, we proposed in 84 FR 7451 that in order to be issued a certification, a health IT developer must attest to whether or not its Health IT Module presented for certification supports MFA consistent with industry-recognized standards (*e.g.,* NIST Special Publication 800–63B Digital Authentication Guidelines, ISO 27001).[52]

We proposed in 84 FR 7451 that, for health IT certified prior to the final rule's effective date, the health IT would need to be certified to the ''multi-factor authentication'' certification criterion within six months after the final rule's effective date. For health IT certified for the first time after the final rule's effective date, we proposed that the health IT must meet this criterion at the time of certification. We solicited comment on the method of attestation and, if the health IT developer does attest to supporting MFA, whether we should require the health IT developer to explain how they support MFA. In particular, we asked whether a health IT developer should be required to identify the MFA technique(s) used/supported by submitting specific information on how it is implemented, including identifying the purpose(s)/use(s) to which MFA is applied within their Health IT Module, and, as applicable, whether the MFA solution complies with industry standards.

Comments. The vast majority of commenters supported the adoption of the two proposed privacy and security transparency attestation certification criteria. A few commenters were opposed to the new criteria. Several supporters of the proposed criteria recommended that we make the criteria operative functional requirements (including testing), rather than yes/no attestations. Some of these commenters reasoned that MFA should be a requirement for all certified health IT, given the risks involved with single-factor authentication and how easy it is today to implement MFA. We also received a number of comments requesting that we clarify that the MFA proposal does not create a requirement for health care providers to implement MFA or encryption of authentication credentials. Similarly, we received several comments seeking clarification that a ''yes'' attestation would only require support of MFA, not that MFA would have to be implemented. Along these same lines, several commenters expressed concerns that the requirements could interfere with clinical care and urged that the requirements not contribute to provider burden.

Response. We have adopted both proposed privacy and security transparency attestation criteria and included both criteria (§ 170.315(d)(12) and § 170.315(d)(13)) in the P&S certification framework (§ 170.550(h)), with minor modifications. While some commenters recommended that MFA should be a requirement for all certified health IT, we did not propose such a requirement nor could health IT developers have foreseen such an outcome in this final rule based on our proposals, particularly considering the clarity provided with our proposals (84 FR 7450) and the complexities of such a requirement. For example, as noted by commenters below, MFA may not be appropriate or applicable in all situations and there is wide variation in authentication needs and approaches throughout the industry. These criteria will, however, still provide increased transparency, and if a developer attests ''yes'' to these criteria regarding a certified Health IT Module, that Health IT Module will then be subject to ONC–ACB surveillance for any potential non-conformity with the requirements of these criteria. Given the strong support expressed in public comments for these criteria as proposed, we believe this is the appropriate approach at this time.

While we believe that encrypting authentication credentials and MFA represent best practices for privacy and security in health care settings, we emphasize again that these criteria do not require certified health IT to have these capabilities or for health IT developers to implement these capabilities for a specific use case or any use case. Equally important, the criteria place no requirements on health IT users, such as health care providers, to implement these capabilities (if present in their Health IT Modules) in their health care settings. However, we note that information regarding the security capabilities of certified health IT provided by such transparency can aid health IT users in making informed decisions on how best to protect health information and comply with applicable security regulations (*e.g.,* the HIPAA Security Rule).

Comments. Some commenters who supported the proposed criteria requested clarification on the scope and intent of the criteria, including what level of authentication and which types of users and user roles the criteria apply to, as well as on how to attest for multiple sign-on paths. A number of commenters noted the wide variation in authentication needs and approaches throughout the industry, and they recommended that we permit health IT developers to describe how they support authentication, rather than simply attest ''yes'' or ''no.'' The commenters stated that such information would provide helpful clarity regarding what the certified health IT supports. Additionally, several commenters stated that we should require that health IT developers explain how they support MFA. A number of commenters stressed that MFA may not be appropriate or applicable in all situations, and in particular, several commenters noted that automated transactions, including some that may occur in the public health reporting context, cannot support MFA.

Response. In response to requests for modifications and clarifications, we have modified the ''encrypt authentication credentials'' criterion to permit a health IT developer that attests ''no'' for its Health IT Module(s) to indicate why the Health IT Module(s) does not support encrypting stored authentication credentials. A health IT developer that attests ''no'' to the ''encrypt authentication credentials'' criterion may explain, for example, that its Health IT Module is not designed to store authentication credentials, therefore there is no need for the Health IT Module to encrypt authentication credentials because it does not store, or have the capability to store, authentication credentials.

For the ''MFA'' criterion, consistent with our solicitation of comments and the comments received recommending that health IT developers explain how they support MFA, we have modified the criterion to require health IT developers that attest ''yes'' to describe the use cases supported. For example, a health IT developer could attest ''yes'' to supporting MFA and state that the Health IT Module supports MFA for remote access by clinical users, thus providing clarity on the user roles to which MFA applies for that particular Health IT Module. To be clear, health IT

[52] NIST Special Publication 800–63B: *https://pages.nist.gov/800-63-3/sp800-63b/cover.html*

developers are not expected to provide specific technical details about how they support MFA that could pose security risks. Again, the purpose is to enable health IT developers to give an indication of the types of uses for which their Health IT Module(s) support MFA. We note that health IT developers may wish to add new MFA use cases for their certified health IT over a period of time. In such instances, to provide the clarity sought in the Proposed Rule as to the MFA technique(s) used/supported and how MFA is implemented, including identifying the purpose(s)/use(s) to which MFA is applied within their Health IT Modules, any new MFA use cases are required to comply with this criterion's ''yes'' attestation provisions and be part of the quarterly CHPL reporting by health IT developers and ONC–ACBs under § 170.523(m).

If a health IT developer attests ''no,'' then it would not be required to explain why its Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. We did not propose to require an explanation for ''no'' attestation nor did we request comment on allowing health IT developers to provide an explanation for a ''no'' attestation like we did for ''yes'' attestations (84 FR 7450–7451). However, in an effort to provide transparency and consistency for these privacy and security attestation criteria, we will also permit developers to provide a reason for attesting ''no'' in order to provide more context. Such a reason may be due to MFA being inapplicable or inappropriate. In those cases, a developer could state, for example, that the Health IT Module does not support MFA because it is engaged in system-to-system public health reporting and MFA is not applicable.

Comments. We received several comments requesting adjustment to the deadline for compliance to meet these criteria. We also received a number of comments recommending that we only apply both of the proposed criteria to new certifications and new Health IT Modules, and not to Health IT Modules already in widespread use.

Response. Regarding the timeframe for compliance, and in response to comments recommending that we only apply the criteria to ''new certifications,'' we have determined that certification to these criteria as part of the updated 2015 Edition privacy and security certification framework (§ 170.550(h)) will only be necessary for Health IT Modules that are presented for certification. Thus, a new Health IT Module seeking certification for the first time to the criteria specified in the 2015 Edition privacy and security certification framework (§ 170.550(h)), after the effective date of this final rule, will need to meet these privacy and security transparency attestation criteria at the time of certification. Similarly, a previously certified Health IT Module that has undergone revision, such as removal of certain capabilities, and is presenting for revised certification to the criteria specified in the 2015 Edition privacy and security certification framework (§ 170.550(h)) after the effective date of this final rule, will need to meet these privacy and security transparency attestation criteria at the time of certification. We believe that this approach will still provide the intended transparency as health IT will need to be issued new certifications as Health IT Modules are updated or certified to other new or revised criteria adopted in this final rule. At the same time, this approach should reduce burden for health IT developers and allow them more time to plan and prepare to meet these new transparency requirements.

9. Security Tags and Consent Management Criteria

In the 2015 Edition final rule, we adopted two ''data segmentation for privacy'' (DS4P) certification criteria. One criterion, ''DS4P-send'' (§ 170.315(b)(7)), includes capabilities for applying security tags according to the DS4P standard in § 170.205(o) at the document-level of a summary care record formatted to the C–CDA 2.1 standard in § 170.205(a)(4). The other criterion, ''DS4P-receive'' (§ 170.315(b)(8)), includes capabilities for receiving a summary care record formatted to the C–CDA 2.1 standard in § 170.205(a)(4) with document-level security tags according to the DS4P standard in § 170.205(o). As noted in the 2015 Edition final rule (80 FR 62646), certification to these criteria is not required to meet the CEHRT definition for PI Programs.

Security tagging enables computer systems to recognize the existence of sensitive elements in data and properly protect the privacy and security of the data by ensuring that only the appropriate individuals and entities can access it. Security tagging capabilities do not compromise the availability or comprehensiveness of health information available for treatment or research purposes; rather, they enable appropriate access controls in accordance with existing policies, governance, and applicable laws. The DS4P standard describes a method for applying security tags to HL7 CDA documents to ensure that privacy policies established at a record's source can be understood and enforced by the recipient of the record.

The utility of the DS4P standard is not limited to data subject to the Federal regulations governing the Confidentiality of Substance Use Disorder Patient Records, 42 CFR part 2 (80 FR 62647). DS4P may be implemented to support other data exchange use cases in which compliance with State or Federal legal frameworks require special protections for sensitive health information. Security tagging capabilities are an initial step towards enabling an interoperable health care system to use technical standards to permit appropriate access, use, or disclosure of sensitive health information in accordance with applicable policies and patient preferences. We understand and acknowledge additional challenges related the prevalence of unstructured data, sensitive images, and potential issues around use of sensitive health information by clinical decision support systems. The adoption of document level data tagging for structured documents would not solve these issues, but could help move technology in the direction where these issues could be addressed (80 FR 16841).

Adoption of the 2015 Edition final rule DS4P criteria was consistent with earlier HIT Policy Committee (HITPC) recommendations for the use of security tagging to enable the electronic implementation and management of disclosure policies that originate from the patient, the law, or an organization, in an interoperable manner, so that electronic sensitive health information may be appropriately shared.[53] The HITPC recommendations consisted of a glide path for the exchange of 42 CFR part 2-protected data starting with the inclusion of Level 1 (document level tagging) send and receive functionality. The HITPC also recommended advancing the exchange of 42 CFR part 2-protected data, by outlining additional capabilities in sharing, viewing and incorporating privacy restricted data at a more granular level, as well as

[53] See HIT Policy Committee (HITPC) Recommendation Letter to ONC, July 2 014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf*; see also HITPC's Privacy and Security Tiger Team Public Meeting, Transcript, May 12, 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-12.pdf.*; Public Meeting, Transcript, May 27, 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-27.pdf.*

managing computable patient consent for the use of restricted data.[54]

Since the 2015 Edition final rule, the health care industry has engaged in additional field testing and implementation of the DS4P standard. As of the beginning of the fourth quarter of the 2019 calendar year, 34 Health IT Modules were certified to one or both of the current 2015 Edition DS4P certification criteria (Health IT Modules with multiple certified versions were counted once). Stakeholders have shared with ONC—through public forums, listening sessions, and correspondence—that document-level security tagging does not provide enough flexibility to address more complex privacy and security use cases. Stakeholders noted that certain provider types, such as pediatrics and behavioral health, often rely on burdensome manual workflows to appropriately segment and share sensitive health information according to State and local laws. Additionally, stakeholders expressed interest in ONC adopting health IT standards that work with DS4P to support electronic consent for the exchange of security tagged data over an API.

Therefore, in consideration of stakeholder feedback and HITPC recommendations to adopt DS4P certification criteria on a glide path, we proposed (84 FR 7452) to remove the 2015 Edition DS4P-send (§ 170.315(b)(7)) and DS4P-receive (§ 170.315(b)(8)) certification criteria. We proposed that the effective date of removal of these criteria would be the effective date of the final rule. We proposed to replace the removed DS4P criteria with two new 2015 Edition DS4P certification criteria in § 170.315(b)(12) and § 170.315(b)(13) that would support security tagging according to the DS4P standard at the document, section, and entry levels of C–CDA 2.1 formatted documents. Our primary purpose for proposing to remove and replace the criteria, in lieu of proposing to revise them, was to provide clarity to stakeholders about the additional functionality enabled by health IT certified to the new criteria. We also proposed a new 2015 Edition certification criteria for sharing patient consent information over an API using the Substance Abuse and Mental Health Services Administration's (SAMHSA) Consent2Share (C2S) IG a FHIR-based exchange standard, in § 170.315(g)(11). We noted resources released by ONC and OCR, such as the HHS Security Risk Assessment Tool [55] and the Guide to Privacy and Security of Electronic Health Information,[56] as well as the Office for Civil Rights' security risk analysis guidance [57] that entities may employ to make risk-based decisions regarding their implementation of the proposed DS4P criteria. We also noted the availability of the Electronic Consent Management Landscape Assessment, Challenges, and Technology report.[58] The report includes suggestions for overcoming barriers associated with implementing electronic consent management, which may be considered for further research and discussion.

We note that we received many comments on the proposed DS4P criteria and the proposed consent management for the API criterion but the majority of comments conflated the two proposals and provided a collective response. We tried to separate where possible, but in some instances, we kept them combined in order to preserve the integrity of the comments.

a. Implementation With the Consolidated CDA Release 2.1

In place of the removed 2015 Edition DS4P criteria, we proposed (84 FR 7452) to adopt new DS4P-send (§ 170.315(b)(12)) and DS4P-receive (§ 170.315(b)(13)) criteria that would remain based on the CDA 2.1 and the HL7 DS4P standard. These criteria would include capabilities for applying security tags according to the DS4P standard at the document, section, and entry level. We believe this offers more valuable functionality to providers and patients, especially given the complexities of the landscape of privacy laws for multiple care and specialty settings. We stated in the Proposed Rule that we believe health IT certified to these criteria would support multiple practice settings and use cases.

Comments. We received many comments both in support and against this proposal. In certain instances, commenters were supportive of our aims but felt there were too many barriers and challenges near term, including but not limited to the perceived cost involved with successful segmentation in practice and indicated we should delay our finalization of the proposal. Others felt immediate adoption of our proposal in the final rule was critical for patient care and the secure exchange of sensitive health information. Many commenters in favor of our proposal provided examples of use cases which it could support, such as helping to combat the opioid crisis by facilitating the secure exchange of sensitive health information across health care settings and including substance use disorder (SUD) information covered by 42 CFR part 2. We also received support of our proposal for the protection of women's health—the commenter explained that segmenting at the element level would protect individuals who have experienced intimate partner violence, sexual assault, and other sensitive experiences. Stakeholders shared with us that focusing certification on segmentation to only the document level does not permit providers the flexibility to address more granular segmentation needs. We received many comments on this proposal in the context of the following topics: provider and developer burden; readiness of the standard and C–CDA exchange; information blocking and EHI; future multidisciplinary activities (such as workgroups) and creating a vision for segmentation using health IT; safety; privacy policy conformity; suggested use cases; cost; and requests for specific clarifications. We describe these comments further below.

Response. We thank commenters for their input. To address the comments concerned about the cost and timing, at the current time, these criteria are voluntary and not required under the definition of CEHRT or to participate in any HHS program. For more information on the costs for the adoption of these criteria, please see the Regulatory Impact Analysis in section XIII. For the reasons noted above, in this final rule, we have finalized our proposal to support a more granular approach to privacy tagging data consent management for health information exchange supported by the C–CDA exchange standard. We do this not by removing and replacing the 2015 Edition DS4P criteria with new § 170.315(b)(12) and § 170.315(b)(13), but by revising the 2015 Edition DS4P criteria, DS4P criteria DS4P-send (§ 170.315(b)(7)) and DS4P-receive (§ 170.315(b)(8)), to include the full scope of the HL7 DS4P standard for

[54] For more details on the two glide paths for part 2-protected data, see *http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf.*

[55] HHS Security Risk Assessment Tool: *http://www.healthit.gov/providers-professionals/security-risk-assessment.*

[56] ONC Guide to Privacy and Security of Electronic Health Information: *http://www.healthit.gov/sites/default/files/ pdf/privacy/privacy-and-security-guide.pdf.*

[57] HHS Office for Civil Rights: *https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html;* and *https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.*

[58] *https://www.healthit.gov/sites/default/files/privacy-security/ecm_finalreport_forrelease62415.pdf.*

security tagging at the document, section and entry level with modifications as described below.

Comments. We received many comments regarding the perceived burden of segmentation on providers and developers including comments focused on workflow challenges. One commenter indicated a lack of system and explained that tagging is burdensome for implementers because it does not describe how to determine what information is sensitive and should be tagged. Another indicated that DS4P creates a permanent added burden of extensive and costly manual data curation to redact each page to meet overlapping Federal and State regulations. Commenters indicated end users would be required to flag each individual data element, a process that is time consuming and error prone. They further explained that granular level privacy tagging has the risk of adding additional data entry burden to provider workflows if users must tag each item individually.

Response. We appreciate the thoughtful comments submitted on the proposed criteria. Notably, with respect to the comments we received that expressed concern about the DS4P standard due to the burden, our analysis of the comments indicates that the concerns the commenters express are more closely related to the complexity of the privacy law landscape than to the specific functionality and standard in our proposal. As noted above, at the current time, these criteria are voluntary and not required under the definition of CEHRT or to participate in any HHS program. The DS4P standard is a tool and voluntary certification to these criteria is an initial step towards enabling an interoperable health care system to use technical standards to compute and persist security tags to permit access, use, or disclosure of sensitive health information. The criteria do not specify that a manual workflow is required to implement security tagging, and we understand from examples of DS4P use in practice that solutions may include the use of value sets to automate the tagging process. We reiterate that these criteria are intended to apply standards to the transmission of documents so that such security tags may be interoperable. Though the updated criteria would support a more granular approach to tagging the sensitive information, we recognize that this will not solve the whole problem of how to manage data segmentation for privacy and consent management. The recipient will still receive and can view the information that is tagged—the recipient will need to determine what they are going to do with that information. Policies and procedures for what to do with the information once it is received are outside the scope of these criteria and this final rule. However, we emphasize that health care providers already have processes and workflows to address their existing compliance obligations for State and Federal privacy laws, which could be made more efficient and cost effective through the use of health IT, rather than relying on case-by-case manual redaction and subsequent workarounds to transmit redacted documents. We believe this tool may be one part of innovative solutions to support health IT enabled privacy segmentation in care coordination workflows to significantly reduce the burden of these manual processes currently in practice.

Comments. Several commenters indicated that enhanced segmentation may unintentionally impact clinical care when providers are presented with an incomplete picture of patient data. Commenters stated there could be patient care risks involved with not sharing elements as users of downstream systems may not realize that a single element is filtered and act improperly, such as by prescribing a contraindicated medication due to missing information.

Response. DS4P is a technical standard for C–CDA that helps health care providers comply with existing, applicable laws. As such, health care providers should already have processes and workflows in place to address their existing compliance obligations. The DS4P standard does not itself create incomplete records. Under existing law, patients already have the right to prevent re-disclosure of certain types of data by withholding consent to its disclosure or to place restrictions on its re-disclosure. DS4P allows providers to electronically tag (mark) data as sensitive and express re-disclosure restrictions and other obligations in an electronic form. DS4P does not determine whether a segmentation obligation exists legally or what that legal obligation means to the recipient. Instead, DS4P allows for tagging and exchange of health information that has already been determined to be sensitive and in need of special protections under existing law.

Comments. We received comments in support of our proposal indicating that, without data segmentation, other mandatory criteria, such as the proposed ''EHI export'' criterion, would be difficult to implement without risking disclosure of sensitive data or information blocking. One commenter indicated that without this technical standard, it would be difficult for stakeholders to know whether appropriate consent has been obtained prior to releasing health information. Further, the commenter indicated concern that without such capabilities, hospitals and health systems could be accused of information blocking because they cannot verify that a patient has given consent for their EHI to be shared. They further commented that if ONC does not finalize this criterion, then we should provide an appropriate exception in the information blocking provisions so that an entity is not accused of information blocking because they do not know if another organization has obtained consent from patients. One commenter stated ONC should propose a new information blocking exception that specifically clarifies that a health IT developer's choice to not certify to an optional standard cannot be a practice that implicates information blocking.

Response. We thank commenters for their support of the DS4P standard. While we understand commenters' concerns, we first reiterate the DS4P capability enables sensitive health information to be exchanged electronically with security tags in a standardized format. It does not enable the full segmentation of a patient's record within an EHR, which may be necessary when responding to a request for EHI. Second, we have revised the Infeasibility Exception in the information blocking section of this final rule to provide that an actor is not required to fulfill a request for access, exchange, or use of EHI if the actor cannot unambiguously segment the requested EHI from other EHI: (1) Because of a patient's preference or because the EHI cannot be made available by law; or (2) because the EHI is withheld in accordance with the Harm Exception in § 171.201 (§ 171.204(a)(2)). For instance, an actor will be covered under this condition if the actor could not fulfill a request to access, exchange, or use EHI because the requested EHI could not be unambiguously segmented from patient records created by federally assisted programs (*i.e.,* Part 2 Programs) for the treatment of substance use disorder (and covered by 42 CFR part 2) or from records that the patient has expressed a preference not to disclose. We refer readers to the Infeasibility Exception discussion in section VIII.D.1.d of this final rule.

Comments. Many commenters noted a low level of adoption for these standards and concerns related to readiness expressing that the standard

utility is limited by lack of widespread developer implementation. Several commenters encouraged ONC to defer adoption of the DS4P criteria with a few commenters recommending that the optional 2015 Edition criterion should be maintained with document level tagging only until practical implementations at scale have been demonstrated at this level. One commenter suggested that organic adoption by end-user providers will help spark innovation in this emerging standard while expressing concern that C–CDA level data tagging for privacy is largely untested in real world scenarios. Others encouraged ONC to provide additional guidance on the adoption of the DS4P standards and certification criteria and forgo the inclusion of this requirement until additional real world testing is available. They also indicated ONC should first conduct use test cases to demonstrate how this functionality will be effectively used across a variety of environments.

Response. We appreciate the comments on the proposed criteria. In reference to the DS4P standard's maturity, we note that it is considered a ''normative'' standard from the HL7 perspective—a status which indicates the content has been enhanced and refined through trial use. While we recognize that to date the standard has not been widely adopted, the SAMHSA C2S application uses the standard to segment Part 2 information. Likewise, the U.S. Department of Veterans Affairs (VA) and private companies across the country have used the DS4P standard to support behavioral health and pediatric care models. In addition, as of the fourth quarter of 2019, 34 individual Health IT Modules obtained certification to one of or both of the prior 2015 Edition certification criteria. Our intent for adopting the updates to these criteria is that in the absence of adoption of consensus driven standards there is increased risk that single-use-case, proprietary solutions will be developed, which may increase fragmentation, provider burden, and cost while limiting interoperability. Further, the purpose of adopting these criteria is to encourage the use of interoperable standards, in this case to use technical standards to compute and persist security tags upon exchange of a summary of care document in an interoperable manner. In addition, the certification criteria using the DS4P standard are voluntary and therefore our intent is, as commenters noted, to support organic adoption of technology certified to the criteria by providers seeking to implement health IT solutions to replace burdensome manual privacy workflows.

Comments. Several commenters called for the need to increase conformity among Federal and State privacy provisions to achieve successful implementation of granular tagging. They noted the significant policy component involved with the successful implementation of the DS4P standard in practice, and in certain instances specifically noted support for HIPAA Privacy Rule and 42 CFR part 2 harmonization. Several commenters identified specific areas for technical development of IT supporting data segmentation for privacy based on Federal and State privacy provisions. One commenter indicated that ONC could map which clinical codes are associated with certain health conditions that receive special privacy protections in addition to the HIPAA Rules. Other commenters noted that mapping of privacy policy to technical specifications is not a sufficient or adequate approach given policy complexities. One commenter indicated a future approach should focus on development of criteria that support a data provenance driven method of sensitive data management as applicable under privacy laws.

Response. As we have stated, the DS4P standard enables sensitive health information to be exchanged electronically with security tags in a standardized format and we encourage health IT developers to include DS4P functionality and pursue certification of their health IT to these criteria in order to help support their users' compliance with relevant State and Federal privacy laws that protect sensitive health information. We recognize that the current privacy law landscape is complex. In light of the complexities of the privacy law landscape, we believe that supporting a standard that allows for increased granularity in security tagging of sensitive health information would better allow for the interoperable exchange of this information to support a wide range of privacy related use cases.

Comments. Many commenters offered an approach for next steps to advance the standard. To advance adoption and implementation of the standard, several commenters suggested that ONC work closely with clinicians, privacy subject matter experts and interoperability experts (notably the HL7 Privacy and Security workgroups) to develop a clear vision for implementing enhanced data segmentation. Many commenters specifically called for ONC to sponsor or lead a multidisciplinary workgroup of stakeholders to develop recommendations for industry adoption and implementation. One commenter in support of our proposal suggested such workgroup focus on including whether additional standards are needed, as well as data visualization of non-disclosed data and its utilization in clinical decision support algorithms. Several commenters cited existing work to help support potential new multidisciplinary efforts indicating that one SDO has already undertaken early work toward evolving DS4P implementation guidance via the HL7 V2 to FHIR mapping project sponsored by the HL7 Orders Work Group. One commenter, called for an ONC led public-private collaborative effort to reduce data entry burden. One commenter recommended that ONC stand up a multi-stakeholder workgroup to identify and define policy needs and functional requirements to address patient privacy and provider needs.

Response. We thank commenters for their recommendations. ONC believes that data segmentation is an integral capability for exchanging sensitive health data. ONC first studied policy considerations regarding data segmentation in electronic health information exchange in 2010 and informed ONC's launch of the DS4P Standards and Interoperability Framework (S&I Framework) Initiative in 2011.[59] The initiative focused on the development of a DS4P technical specification that would allow highly sensitive health information to flow more freely to authorized users while improving the ability of users of health IT to meet their obligations under State and Federal privacy rules. Recommendations from the initiative called for the use of metadata security tags to demonstrate privacy and security obligations associated with patient health information. It also advised that patients and providers be able to share portions, or segments, of records in order to maintain patient privacy. Pilot projects conducted under the DS4P S&I Framework Initiative demonstrated ways to enable the sharing of information that is protected by Federal and State laws, including the substance use disorder treatment confidentiality regulations, 42 CFR part 2. ONC's prior Federal Advisory Committee, the HITPC, also focused on the health IT certification needed to enable exchange of behavioral health data.[60] Additionally, ONC led a project on

[59] *https://archive.healthit.gov/providers-professionals/ds4p-initiative.*

[60] *https://www.healthit.gov/topic/Federal-advisory-committees/health-it-policy-committee-recommendations-national-coordinator.*

patient choice where the exchange of sensitive data was addressed.[61] ONC also led a project on the Behavioral Health Data Exchange (BHDE) Consortium. The purpose of the project was to facilitate and address barriers to the intra and interstate exchange of behavioral health data.[62] Currently, ONC's Leading Edge Acceleration Projects (LEAP) in Health Information Technology (IT) program seeks to address well-documented and fast emerging challenges inhibiting the development, use, and/or advancement of well-designed, interoperable health IT. In 2019, one of the two LEAP awards issued by ONC focused on the standardization and implementation of the Fast Healthcare Interoperability Resources (FHIR®) Consent resource. Under this project, a FHIR® Consent Implementation Guide (IG) and package of open-source prototypes and content to assist partners in using the FHIR® Consent Resource will become available.[63]

Also, ONC actively participates in HL7 International (HL7®) Workgroups and standards-development activities related to data segmentation and consent management. It is critical for sensitive health information to be included in health information exchange and we are exploring opportunities for additional collaboration in the future.

Comments. One commenter recommended a companion guide be developed to assist implementers with the standard. Another indicated ONC should provide guidance to facilitate adoption of the DS4P standards and certification criteria including dissemination of best practices to help ensure that providers can most effectively implement the standards and associated workflows. Another referred to a Query-Based Document Exchange IG which has further guidance on the ability to assert access policies and DS4P implementation considerations.

Response. The HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile, May 16, 2014 standard[64] § 170.205(o)(1) (HL7 DS4P standard) describes the technical means to apply security tags to a health record and data may be tagged at the document-level, the section-level, or individual data element-level. The HL7 DS4P standard also provides a means to express obligations and disclosure restrictions that may exist for the data. We appreciate commenters input on additional guidance beyond these certification requirements that may prove useful for developers. However, we reiterate that in this rule we address only that guidance that is required for those developers to voluntarily submit a Health IT Module for certification to our criteria. Additional guidance on best practices would be outside the scope of this rulemaking. However, as noted above, we are committed to continuing to work with stakeholders, including health IT developers and those involved in implementing privacy policy in the health care industry, to work toward interoperable solutions for privacy and consent management.

Comments. We received several comments seeking clarification on our proposal to remove the current 2015 Edition ''DS4P-send'' (§ 170.315(b)(7)) and ''DS4P-receive'' (§ 170.315(b)(8)) certification criteria and to replace these two criteria with three new 2015 Edition DS4P certification criteria (two for C–CDA and one for a FHIR-based API). As examples, one commenter sought clarification on whether our proposal was for DS4P send and receive to become mandatory for the revised 2015 Edition certification, or if they will remain voluntary criteria. One commenter sought clarification on whether the data protections apply to FHIR transmissions. Another indicated that they believe the DS4P implementation guide only focuses on data segmentation for C–CDA documents and not for HL7 FHIR and sought ONC clarification regarding whether or not we intend to apply data segmentation labeling to the HL7 FHIR resources in support of the USCDI as well. Another commenter recommended that we require FHIR Release 4 version but commented that a consistent approach of USCDI across HL7 CDA, C–CDA and HL7 FHIR is not attainable at this time. One commenter stated a similar need for clarification indicating that the standard for DS4P should be HL7 standards for CDA Version 2 and FHIR security tagging and not be the SAMHSA C2S stating that ONC should clarify this misunderstanding. Another commenter sought clarification by ONC to indicate that the IG is for CCDS and not FHIR, and also indicated confusion regarding STU4. One commenter noted that the DS4P criteria are only effective for C–CDA-based data exchange and recommended ONC add FHIR-based standard for tagging of sensitive data. Several commenters expressed concern over what they described as misalignment of this proposal with other ONC policies explaining that neither USCDI nor ARCH, nor HL7 FHIR US Core includes the FHIR Composition resource, which would be at the equivalent level of granularity as a C–CDA document.

Response. We thank commenters for their input and we appreciate the need for clarity requested by commenters. In the Proposed Rule (84 FR 7452), we proposed both to adopt an update to the HL7 DS4P standard for the existing 2015 Edition certification criteria to support security tagging of a C–CDA upon send and receive by removing DS4P-send (§ 170.315(b)(7)) and DS4P-receive (§ 170.315(b)(8)) and replacing them with DS4P-send (§ 170.315(b)(12)) and DS4P-receive (§ 170.315(b)(13)) and to also adopt a new criterion to support API exchange via consent management solutions using the FHIR standard. In other words, these were two separate proposals, the first to support security tags in summary of care documents and another to support consent management for specific use cases that leverage a FHIR-based API. As of this final rule, these criteria remain voluntary and not required under the definition of CEHRT or to participate in any HHS program. We proposed these several criteria in a single section of the Proposed Rule because of the relationship between them as two potential health IT tools that could be part of overarching solutions to manage privacy and consent in health information exchange. However, as stated earlier, we note that neither of these tools addresses the entirety of the scope of data segmentation for privacy. To address the comment on the DS4P implementation guide, we confirm that the HL7 DS4P standard in § 170.205(o)(1) describes the technical means to apply security tags to a health record and data may be tagged at the document-level, the section-level, or individual data element-level in the C–CDA and not for FHIR. Currently, we do not intend to apply data segmentation labeling to the HL7 FHIR resources in support of the USCDI because all FHIR resources already include the capability to apply security tags to the resource as metadata. We appreciate the recommendation to require FHIR Release 4 for consent management but as discussed below, we have decided not to finalize the proposal for consent management for APIs in this final rule. For further

[61] *https://www.healthit.gov/topic/patient-consent-electronic-health-information-exchange.*

[62] *https://www.healthit.gov/topic/health-it-health-care-settings/behavioral-health-data-exchange-primary-care-and-behavioral.*

[63] *https://www.healthit.gov/topic/leading-edge-acceleration-projects-leap-health-information-technology-health-it.*

[64] *https://www.hl7.org/implement/standards/product_brief.cfm?product_id=354.*

discussion of our FHIR-based consent management proposal, we direct readers to subsection b below.

For the updates to the existing DS4P criteria, to support greater clarity requested by public comment, rather than removing the existing 2015 Edition criteria and replacing them with new criteria as proposed, we instead finalized a simple update to the existing criteria to note the use of the full HL7 DS4P standard for tagging or applying security tags at the document, section, and entry level.

We further note that these updated criteria remain voluntary, and that we have finalized modifications in § 170.315(b)(7)(ii) and § 170.315(b)(8)(i)(B) to our proposed effective date for this change to allow for a longer glide path for health IT developers to update Health IT Modules to the full standard to better support clinical and administrative workflows. While certification to the updated standards will be available after the effective date of this final rule upon successful testing, we have finalized that document-level tagging remains applicable for up to 24 months after the publication date of this final rule. For certification and compliance of Health IT Modules certified after 24 months after the publication date of this final rule, only the full scope of the HL7 DS4P standard is applicable. We have finalized this 24 month period for the update for these criteria under the real world testing provisions in § 170.405(b)(6) as follows:

- *Security tags.* A health IT developer with health IT certified to § 170.315 (b)(7) and/or § 170.315 (b)(8) prior to June 30, 2020, must:
  - Update their certified health IT to be compliant with the revised versions of the criteria adopted in § 170.315(b)(7) and/or the revised versions of the criteria adopted in § 170.315(b)(8); and
  - Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(6)(i) of this section by May 2, 2022,

In addition, we have finalized these updated criteria with modifications to the criteria names to better describe the function the criteria support in interoperable health IT systems. The modifications to the criteria are as follows:

- Prior criterion: ''DS4P-send'' (§ 170.315(b)(7)) includes capabilities for creating a summary care record formatted to the C–CDA standard and document-level tagging as restricted (and subject to restrictions on re-disclosure) according to the DS4P standard.
- Revised criterion: ''Security tags—Summary of Care (send)'' (§ 170.315(b)(7)) includes capabilities for creating a summary of care record formatted to the C–CDA standard and that is tagged as restricted and subject to restrictions on re-disclosure according to the DS4P standard at the document, section, and entry (data element) level, or at the document-level for the period until May 2, 2022.
- Prior criterion: ''DS4P-receive'' (§ 170.315(b)(8)) includes capabilities for receiving a summary care record formatted to the C–CDA standard and document-level tagged as restricted (and subject to restrictions on re-disclosure) according to the DS4P standard.
- Revised criterion: ''Security tags—Summary of Care (receive)'' (§ 170.315(b)(8)) includes capabilities for receiving a summary of care record formatted to the C–CDA standard and that is tagged as restricted and subject to restrictions on re-disclosure according to the DS4P standard at the document, section, and entry (data element) level, or at the document-level for the period until May 2, 2022. We have finalized our proposal to include in the voluntary ''Security tags—Summary of Care (receive)'' (§ 170.315(b)(8)) criterion as a requirement that the Health IT Module has the capability to preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions as proposed.

b. Implementation With the Fast Healthcare Interoperability Resources (FHIR®) Standard

In collaboration with ONC, SAMHSA developed the C2Sapplication to address the specific privacy protections for patients with substance use disorders whose treatment records are covered by the Federal confidentiality regulation, 42 CFR part 2. C2S is an open source application for data segmentation and consent management. It is designed to integrate with existing FHIR systems. SAMHSA created a FHIR implementation guide (the Consent2Share Consent Profile Design, hereafter referred to as ''Consent Implementation Guide'') that describes how the Consent2Share application and associated access control solution (C2S platform) uses the FHIR Consent resource to represent and persist patient consent for treatment, research, or disclosure.[65] The implementation guide provides instructions for using the FHIR Consent resource to capture a record of a health care consumer's privacy preferences.

In section VII.B.4 of this final rule, we discuss policies related to the implementation of a standardized API to support the exchange of health information between providers and patients and among members of a care team. In the Proposed Rule, we anticipated that the proposed 2015 Edition ''standardized API for patient and population services'' certification criterion (§ 170.315(g)(10)) would result in a proliferation of APIs that will enable a more flexible and less burdensome approach to exchanging EHI. We stated our belief that the health care industry could leverage this API infrastructure to share segmented data in a secure and scalable manner. Therefore, we proposed to adopt a 2015 Edition certification criterion ''consent management for APIs'' in § 170.315(g)(11) to support data segmentation and consent management through an API in accordance with the Consent Implementation Guide.

Comments. Overall, the majority of commenters were supportive of the concept of consent management for APIs but many had concerns with the proposed criteria, specifically the adoption of the Consent Implementation Guide or the C2S platform as part of a certification criterion. Many commenters raised concerns that the Consent Implementation Guide has not been balloted as an HL7 standard and noted that C2S does not support a consenter's signature or specification to protect information content data requirements. A couple of commenters stated that the Consent Implementation Guide is a new emerging standard in pilot with feedback requested. Commenters also raised concern that the IG has not gone through an SDO process. Another commenter raised concern that SAMHSA no longer supports the C2S platform and the Consent Implementation Guide and it now lacks a steward. A couple of commenters suggested ONC defer the consent management criteria at least until an API FHIR standard version is finalized and the Consent Implementation Guide is revised to conform that to that version. One commenter supported the adoption of FHIR v3-based Consent resource, but urged ONC to also consider pediatric and geriatric use cases in its adoption. Other commenters stated that their understanding was that tagging will be

[65] The draft FHIR IG titled ''Consent2Share FHIR Profile Design.docx'' can be accessed through the Community- Based Care and Privacy (CBCP) HL7 workgroup, within the Package Name titled ''BHITS_FHIR_Consent_IG,'' at *https://gforge.hl7.org/gf/project/cbcc/frs/.*

a feature of FHIR Release 4, but were unclear how the proposal to move to FHIR Release 2 would work. One commenter questioned how if there are no standards-based approaches for identifying what in the record is sensitive, how one could feasibly implement privacy-tagging and consent management via FHIR at the Resource level and that tagging at a more granular level is too cumbersome and unrealistic. A number of commenters stated that the standards were premature and if adopted could have unintended negative effects. Commenters were not supportive of having two versions of FHIR but instead recommended the use of FHIR Release 4. Commenters recommended ONC focus on driving real-world implementation experience before adopting the standards.

On the other hand, a few commenters supported our proposal, and stated that the C2S platform and the Consent Implementation Guide is mature and already supports granular level security tagging and data segmentation and supports several API standards listed in the Proposed Rule. One commenter expressed support broadly for the C2S platform indicating that, though it was originally designed to satisfy 42 CFR part 2 consent for the substance use disorder data, it supports the other sensitive categories such as HIV and mental health. Several commenters stated that the criteria should be required in the Base EHR definition.

Many providers called for patient education and for ONC to work with SAMHSA, OCR, and CMS. It was also suggested that ONC coordinate with SAMHSA to establish a public-private project to advance the C2S platform and the Consent Implementation Guide using an analogous process to that of the Da Vinci Project with transparency and with no membership fees. Finally, several commenters raised issues that are out of scope for this rule including concerns specifically with the HIPAA Rules or 42 CFR part 2 which are under the authority of OCR and SAMHSA respectively.

Response. We appreciate the comments received and the insights into real world implementing challenges of consent management. We agree that there is continued work to be done to ballot and field test the C2S platform and the Consent Implementation Guide and also agree with commenters that identified this resource as having significant potential to support consent management for specific use cases such as 42 CFR part 2, behavioral health, and pediatric care. We also note that we had included a series of questions in our Proposed Rule related to the alignment of FHIR releases and we appreciate comments received related to these questions. We direct readers to section VII.B.4.c for further discussion of our adoption in this rule the FHIR Release 4 standard. We note that the Consent Implementation Guide is designed in FHIR Release 3 and that there is significant work to be done in standards development before the IG would be feasible with FHIR Release 4. At this time, FHIR Release 4 version of FHIR consent resource is not normative and can change from version to version and therefore further development, review, balloting, and testing would be required for a FHIR Release 4 based IG to be a viable consensus standard for adoption in the Program. In consideration of comments, and the scope of the additional work required for readiness of an IG that could be adopted in our regulations, we have not finalized the proposed ''consent management for APIs'' certification criterion in § 170.315(g)(11). We maintain, as stated above, that the C2S platform and the Consent Implementation Guide may still serve as a template for implementation of consent management workflows leveraging APIs and that it may be a part of health IT solutions to facilitate health information exchange of sensitive information. We will continue to monitor the development of the Consent Implementation Guide and other FHIR resources to support consent management and may consider including in a future rulemaking.

10. Auditable Events and Tamper-Resistance, Audit Reports, and Auditing Actions on Health Information

Since adopting the Auditable events and tamper-resistance (§ 170.315(d)(2)), Audit Reports (§ 170.315(d)(3)), and Auditing Actions on health information (§ 170.315(d)(10)) criteria in the 2015 Edition, there has been an update to ASTM E2147—1 standard and has been replaced by a newer version. Given the older version has been deprecated and based on comments received, we have updated these criteria with the most up to date standard, ASTM E1247—18 in § 170.210(h). We have also updated the requirements to align with the new numbering sequence of the updated standard. In order to meet the minimum requirements for capturing and auditing electronic health information, we have specified, in § 170.210(e)(1)(i), that the data elements in sections 7.1.1 through 7.1.3 and 7.1.6, through 7.1.9 in ASTM E1247—18 are required. We believe that the updated standard reinforces what we have previously required and maintained with previous certification requirements and note that there is no substantial change to the standard.

We further note that health IT developers must update Health IT Modules to these updated standards referenced in these criteria within 24 months after the publication date of this final rule. We have added as a Maintenance of Certification requirement for the real world testing Condition of Certification requirement, that health IT developers are required to provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the publication date of the final rule. Developers would also need to factor these updates into their next real world testing plan as discussed in section VII.B.5 of this final rule and in § 170.405(b)(7).

C. Unchanged 2015 Edition Criteria—Promoting Interoperability Programs Reference Alignment

In the FY 2019 IPPS/LTCH PPS proposed rule (83 FR 20516), CMS proposed scoring and measurement policies to move beyond the three stages of meaningful use to a new phase of EHR measurement with an increased focus on interoperability and improving patient access to health information. To reflect this focus, CMS changed the name of the Medicare and Medicaid EHR Incentive Programs, to the Medicare and Medicaid Promoting Interoperability (PI) Programs. To align with the renaming of the EHR Incentive Programs, we proposed to remove references to the EHR Incentive Programs and replace them with ''Promoting Interoperability Programs'' in the updated 2015 Edition ''automated numerator recording'' criterion in § 170.315(g)(1) and the ''automated measure calculation'' criterion in § 170.315(g)(2).

Comments. We did not receive any comments on this proposal to remove references to the EHR Incentive Programs and replace them with ''Promoting Interoperability Programs'' in the updated 2015 Edition ''automated numerator recording'' criterion in § 170.315(g)(1) and the ''automated measure calculation'' criterion in § 170.315(g)(2).

Response. We have removed references to the EHR Incentive Programs and replaced them with ''Promoting Interoperability Programs'' in the 2015 Edition ''automated numerator recording'' criterion in § 170.315(g)(1) and the ''automated measure calculation'' criterion in § 170.315(g)(2).

V. Modifications to the ONC Health IT Certification Program

A. Corrections

1. Auditable Events and Tamper Resistance

We proposed to revise § 170.550(h)(3) to require the End-User Device Encryption criterion in § 170.315(d)(7) as appropriate, and exempt Health IT Modules from having to meet § 170.315(d)(7) when the certificate scope does not require § 170.315(d)(7) certification (*see* § 170.315(d)(2)(i)(C)) (84 FR 7454). As noted in the Proposed Rule (84 FR 7454), paragraph 170.315(d)(2)(i)(C) was not applicable to the privacy and security testing and certification of a Health IT Module required by § 170.550(h)(3)(iii), (v), (vii), and (viii), but we intended for it to also be exempted from the aforementioned paragraphs. We, therefore, proposed to revise § 170.550(h)(3)(iii), (v), (vii), and (viii) by removing references to paragraph 170.315(d)(2)(i)(C).

Comments. One commenter expressed support of the proposals under section V (''Modifications of the ONC Health IT Certification Program'') of the Proposed Rule as a whole. However, we received no comments specific to this proposal.

Response. We have finalized the revision as proposed. Certification can proceed for the audit log process without the Health IT Module demonstrating that it can record an encryption status in accordance with § 170.315(d)(2)(i)(C). Paragraph § 170.315(d)(2)(i)(C) is not applicable for the privacy and security testing and certification of a Health IT Module required by § 170.550(h)(3)(iii), (v), (vii), and (viii). We had previously identified this error in guidance,[66] and have now codified the correction to § 170.550(h)(3)(iii), (v), (vii), and (viii) in regulation.

2. Amendments

We proposed to revise § 170.550(h) to remove the ''amendments'' criterion's application to certain non-applicable clinical criteria including: ''Drug-drug, drug-allergy interaction checks for computerized provider order entry (CPOE)'' in § 170.315(a)(4); ''clinical decision support (CDS)'' in § 170.315(a)(9); ''drug-formulary and preferred drug list checks'' in § 170.315(a)(10); and ''patient-specific education resources'' in § 170.315(a)(13) (84 FR 7454). The ''amendments'' certification criterion § 170.315(d)(4) is not necessarily indicated for health IT capabilities that may not have any patient data for which a request for an amendment would be relevant.

Comments. One commenter expressed support of the proposals under section V (''Modifications of the ONC Health IT Certification Program'') of the Proposed Rule as a whole. However, we received no comments specific to this proposal.

Response. We have finalized the proposal with modifications. Health IT Modules presented for certification to these criteria do not have to demonstrate the capabilities required by the revised 2015 Edition ''amendments'' certification criterion (§ 170.315(d)(4)), unless the Health IT Module is presented for certification to another criterion that requires certification to the 2015 Edition ''amendments'' criterion under the privacy and security (P&S) certification framework. We note that, because we have not finalized our proposal to remove the ''drug-formulary and preferred drug list checks'' criterion in § 170.315(a)(10) and the ''patient-specific education'' criterion in § 170.315(a)(13), but to only permit ONC–ACBs to issue certificates for these criteria until January 1, 2022, we have not removed references to these criteria from the exemption in § 170.550(h) at this time. This clarification has already been incorporated into sub-regulatory guidance,[67] and is now codified in regulation.

3. View, Download, and Transmit to 3rd Party

We proposed to remove § 170.315(e)(1)(ii)(B), which includes a cross-reference to § 170.315(d)(2) indicating that a Health IT Module may demonstrate compliance with active history log requirements if it is also certified to § 170.315(d)(2) (84 FR 7454).

Comments. One commenter expressed support of the proposals under section V (''Modifications of the ONC Health IT Certification Program'') of the Proposed Rule as a whole. However, we received no comments specific to this proposal.

Response. We thank commenters for their support and have finalized the proposal to remove § 170.315(e)(1)(ii)(B), which includes a cross-reference to § 170.315(d)(2). As noted in the Proposed Rule (84 FR 7454), this cross-reference indicates that a Health IT Module may demonstrate compliance with activity history log requirements if it is also certified to the 2015 Edition ''auditable events and tamper-resistance'' certification criterion (§ 170.315(d)(2)). However, we no longer require testing of activity history log when certifying for § 170.315(d)(2). Therefore, this cross-reference is no longer applicable to meet certification requirements for the updated 2015 Edition ''view, download, and transmit to 3rd party'' certification criterion (§ 170.315(e)(1)) activity history log requirements. Consequently, we have finalized our proposal to remove § 170.315(e)(1)(ii)(B).

4. Integrating Revised and New Certification Criteria Into the 2015 Edition Privacy and Security Certification Framework

We proposed to require the new certification criteria (§ 170.315(d)(12) and (d)(13)) to apply to all § 170.315 certification criteria (84 FR 7454). Therefore, given these and the other modifications discussed above, we proposed to revise the P&S Certification Framework as shown in Table 1 of the Proposed Rule (84 FR 7455), noting that the P&S Certification Framework when finalized could differ depending on finalization of proposals in section III.B.4 of the Proposed Rule (84 FR 7436 and 7437) to remove certain 2015 Edition certification criteria.

Comments. One commenter expressed support of the proposals under section V (''Modifications of the ONC Health IT Certification Program'') of the Proposed Rule as a whole. However, we received no comments specific to this proposal.

Response. We thank the commenter for their input regarding our proposals under section V (''Modifications of the ONC Health IT Certification Program'') of the Proposed Rule. We have adopted the revisions as proposed with modifications. As noted in section IV.B.8.a, we have also adopted both proposed privacy and security transparency attestation criteria (§ 170.315(d)(12) and (d)(13)) with minor modifications. We have applied § 170.315(d)(12) and (d)(13) to all certification criteria across the P&S Certification Framework. Table 2 shows the final updated P&S Certification Framework, which includes all changes including the removal of certain 2015 Edition certification criteria as finalized in section III.B.4 of this final rule. We updated the P&S Certification Framework to reflect other changes made throughout this final rule. The privacy and security certification criteria applicable to a Health IT Module presented for certification is based on the other capabilities included in the Health IT Module and for which certification is sought (80 FR 62705). In this final rule, we have determined that

[66] *https://www.healthit.gov/test-method/auditable-events-and-tamper-resistance.*

[67] *https://www.healthit.gov/test-method/drug-drug-drug-allergy-interaction-checks-cpoe; https://www.healthit.gov/test-method/clinical-decision-support-cds; https://www.healthit.gov/test-method/drug-formulary-and-preferred-drug-list-checks;* and *https://www.healthit.gov/test-method/patient-specific-education-resources.*

§ 170.315(b)(10) and, consistent with the rationale provided in the 2015 Edition final rule, (g)(1) through (6) are exempt from the P&S Certification Framework due to the capabilities included in these criteria, which do not implicate privacy and security concerns (80 FR 62707).

We have revised § 170.550(h) of this final rule to reflect these clarifications. We also corrected Table 2 to accurately reflect the regulatory text at § 170.315(a)(3), (a)(14), and (a)(15). Sections 170.315(a)(3), (a)(14), and (a)(15), though included in the regulatory text, were erroneously deleted in the Proposed 2015 Edition Privacy and Security Certification Framework table and we corrected it in Table 2.

TABLE 2—2015 EDITION PRIVACY AND SECURITY CERTIFICATION FRAMEWORK

If the Health IT Module includes capabilities for certification listed under:	It will need to be certified to approach 1 or approach 2 for each of the P&S certification criteria listed in the "approach 1" column	
	Approach 1	Approach 2
§ 170.315(a)(1) through (3), (5), (12), (14), and (15).	§ 170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6) (emergency access), (d)(7) (end-user device encryption) (d)(12) (encrypt authentication credentials) (d)(13) (multi-factor authentication).	For each applicable P&S certification criterion not certified using Approach 1, the health IT developer submits system documentation that is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable P&S certification criterion that enable the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion.
§ 170.315(a)(4), (9), (10), and (13)	§ 170.315(d)(1) through (d)(3), (d)(5) through (d)(7), (d)(12), and (d)(13).	
§ 170.315(b)(1) through (3) and (6) through (9).	§ 170.315(d)(1) through (d)(3), (d)(5) through (d)(8) (integrity), (d)(12), and (d)(13).	
§ 170.315(c)	§ 170.315(d)(1) through (d)(3) and (d)(5), (d)(12), and (d)(13)*.	
§ 170.315(e)(1)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(7), (d)(9) (trusted connection), (d)(12), and (d)(13).	
§ 170.315(e)(2) and (3)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(9), (d)(12), and (d)(13)*.	
§ 170.315(f)	§ 170.315(d)(1) through (d)(3), (d)(7), (d)(12), and (d)(13).	
§ 170.315(g)(7) through (g)(10)	§ 170.315(d)(1) and (d)(9); (d)(2) or (d)(10) (auditing actions on health information), (d)(12), and (d)(13).	
§ 170.315(h)	§ 170.315(d)(1) through (d)(3), (d)(12), and (d)(13)*.	

An ONC–ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text "first level paragraph" category of § 170.315 (*e.g.,* § 170.315(a)) identified in Table 2 is certified to either Approach 1 (technically demonstrate) or Approach 2 (system documentation).

In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion identified as part of Approach 1 or Approach 2 so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the certification of a Health IT Module to § 170.315(e)(1) "view, download, and transmit to 3rd party." For this criterion, a Health IT Module must be separately tested to § 170.315(d)(9) because of the specific capabilities for secure electronic transmission included in the criterion.

*§ 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not include end-user device encryption features.

B. Principles of Proper Conduct for ONC–ACBs

1. Records Retention

We proposed to revise the records retention requirement in § 170.523(g) to include the ''life of the edition'' as well as three years after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules (84 FR 7456). We also proposed to clarify that HHS has the ability to access certification records for the ''life of the edition,'' which begins with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of three years from the effective date of the final rule that removes the applicable edition from the Code of Federal Regulations (CFR), not solely during the three-year period after removal from the CFR (84 FR 7456).

Comments. Several commenters expressed support for ONC's proposal to revise the records retention requirement. Another commenter requested that ONC provide a separate posting or notice that lists the dates specific to when the ''life of the edition'' starts and dates specific to when the ''life of the edition'' and the minimum period of three years from the effective date that removes the applicable edition end.

Response. We thank commenters for their input and have finalized this revision as proposed. Because the ''life of the edition'' begins with the codification of an edition of certification criteria in the CFR and ends on the effective date of the final rule that removes the applicable edition from the CFR, the start and end dates for the ''life of the edition'' are published in the **Federal Register** in the rulemaking actions that finalize them. The period of three years beyond the ''life of the edition'' begins on the effective date of the final rule that removes the applicable edition from the CFR, thus the three-year period after removal from the CFR continues through three full calendar years following that date. For example, if the effective date of a hypothetical final rule removing an edition from the CFR were July 1, 2025, then the three year period following the end of the life of this hypothetical edition would be June 30, 2028. We anticipate continuing to work with ONC–ACBs to provide guidance and information resources as necessary or appropriate to promote successful adherence to all Principles of Proper

Conduct (PoPC) applicable to their participation in the Program.

2. Conformance Methods for Certification Criteria

The PoPC in § 170.523(h) specified that ONC–ACBs may only certify health IT that has been tested by ONC–ATLs using tools and test procedures approved by the National Coordinator. We proposed to revise the PoPC in § 170.523(h) in three ways (84 FR 7456).

First, we proposed to revise this PoPC to additionally permit ONC–ACBs to certify Health IT Modules that the ONC–ACB has evaluated for conformance with certification criteria without first passing through an ONC–ATL. However, we proposed that such methods to determine conformity must first be approved by the National Coordinator.

Second, we proposed to revise the PoPC to clarify that certifications can only be issued to Health IT Modules and not Complete EHRs. We proposed to remove the 2014 Edition from the CFR (*see* section III.B.2 of this preamble) and Complete EHR certifications are no longer available for certification to the 2015 Edition (80 FR 62608; 79 FR 54443). We also proposed to remove the provision that permits the use of test results from National Voluntary Laboratory Accreditation Program (NVLAP)-accredited testing laboratories under the Program because the regulatory transition period from NVLAP-accredited testing laboratories to ONC–ATLs has expired (81 FR 72447).

Third, we proposed to remove the provision that permits the certification of health IT previously certified to an edition if the certification criterion or criteria to which the Health IT Module(s) was previously certified have not been revised and no new certification criteria are applicable because the circumstances that this provision seeks to address are no longer feasible with certification to the 2015 Edition.

Comments. One commenter sought clarification on whether the proposal to remove references to § 170.545, which includes the ability to maintain Complete EHR certification, would impact § 170.550(k), which requires ONC–ACBs to accept requests for a newer version of a previously certified Health IT Module(s) to inherit the certified status of the previously certified Health IT Module(s) without requiring the newer version to be recertified. The commenter strongly urged ONC to allow ONC–ACBs to grant inherited certification status to updated versions of certified technology. Another commenter expressed support for ONC's proposal to revise the PoPC to clarify that certifications can only be issued to Health IT Modules and not Complete EHRs. The commenter also expressed support for ONC's proposal to remove the provision that permits the certification of health IT previously certified to an edition if the certification criterion or criteria to which the Health IT Module(s) was previously certified have not been revised and no new certification criteria are applicable because the circumstances that this provision seeks to address are no longer feasible with certification to the 2015 Edition.

Response. We have finalized the proposal to revise the PoPC in § 170.523(h). As noted in the Proposed Rule, the ability to maintain Complete EHR certification is only permitted with health IT certified to the 2014 Edition certification criteria (84 FR 7435). Because this concept was not continued in the 2015 Edition (84 FR 7456), we proposed revisions to clarify that Complete EHR certifications are no longer available. We note that ONC–ACBs have discretion, and processes in place, to evaluate updates made to certified health IT and assess the need for additional testing. These ONC–ACB processes allow for efficient certification of upgraded version releases of previously certified health IT while ensuring its continued conformity with certification criteria and standards to which the prior version release of the same Module(s) had been certified. We have finalized this proposal.

Comments. Multiple commenters expressed support for the use of conformance methods approved by the National Coordinator. One commenter noted that the opportunity would enable alternative testing methods and less costly testing. Another commenter noted that this proposal would reduce burden for EHR developers and for ONC–ATLs by leveraging certification programs and alternative test methods and specifically requested that ONC consider a specific proprietary certification related to e-prescribing functionalities for potential approval. While expressing appreciation for the flexibility offered by the proposed revision, one commenter expressed concern about certifications based on other ONC-approved conformance methods that are not specifically designed to test against the ONC criteria and stressed the importance of assessing conformance to technical standards before being deployed to end users. Another commenter questioned whether the ONC–ACB would be permitted to do all evaluation directly, thus eliminating the need for ONC–ATLs entirely. Two commenters sought clarity from ONC as to what metrics the National Coordinator will use to approve a conformance method. These commenters also sought clarification on ONC's plan to reduce the risk of developers seeking certification through fraudulent means. The commenters cited the example of two developers who are currently operating under corporate integrity agreements with the HHS Office of the Inspector General due to court cases brought against them in relation to conduct including, but not limited to, the process of seeking certification.

Response. We thank commenters for their feedback. We have finalized the proposal to revise the PoPC in § 170.523(h) to permit a certification decision to be based on an evaluation conducted by the ONC–ACB for Health IT Modules' compliance with certification criteria by use of conformity methods approved by the National Coordinator.

We note that all certification criteria will continue to have some method of holding developers responsible for demonstrating conformity whether through ONC–ATL testing, developer self-declaration, or some other method assessed and approved by the National Coordinator. As noted in the Proposed Rule (84 FR 7456), ONC acknowledges that there is a broad spectrum of types of evidence of conformance, from laboratory testing with an ONC–ATL to developer self-declaration. Some of these types of evidence may be more appropriate than others in specific circumstances. Historically, it has been proven that, in some circumstances, the requirement for ONC–ATL testing has presented more administrative burden on health IT developers than benefits for assessing conformity. For example, under § 170.315(a)(5) demographics certification criteria require only documentation or a visual inspection, and do not require testing by an ONC–ATL. We note that industry advancements have presented opportunities for improved efficiency for demonstrating conformity and this flexibility will allow the Program to advance as the state of the art for demonstrating conformance evolves. This flexibility addresses the current Program construct limitation of ONC–ACB certification only being permissible for health IT that has been tested by an ONC–ATL with ONC-approved test procedures. In some instances, such as developer self-declaration, there is no testing required and thus bypassing the ONC–ATL testing step reduces burden and enables a more streamlined and

efficient process. By adopting this flexibility, we may approve conformance methods that rely solely on ONC–ACB evaluation, and not ONC–ATL testing, when appropriate.

We will follow the same process used for alternative test methods (76 FR 1280) for the submission of non-governmental developed conformance methods to the National Coordinator for approval. A person or entity may submit a conformance method to the National Coordinator to be considered for approval for use under the Program. The submission should identify the developer of the conformance method; specify the certification criterion or criteria that is/are addressed by the conformance method; and explain how the conformance method would evaluate a Health IT Module's or, if applicable, other type of health IT's, compliance with the applicable certification criterion or criteria. The submission should also provide information describing the process used to develop the conformance method, including any opportunity for the public to comment on the conformance method and the degree to which public comments were considered. In determining whether to approve a conformance method for purposes of the Program, the National Coordinator will consider whether it is clearly traceable to a certification criterion or criteria adopted by the Secretary; whether it is sufficiently comprehensive (*i.e.,* assesses all required capabilities) for the assessment of Health IT Modules', or other type of health IT's, conformance to the certification criterion or criteria adopted by the Secretary; whether an appropriate public comment process was used during the development of the conformance method; and any other relevant factors. When the National Coordinator has approved a conformance method for purposes of the Program, we will publish a notice of availability in the **Federal Register** and identify the approved conformance method on the ONC website.

3. ONC–ACBs To Accept Test Results From Any ONC–ATL in Good Standing

We proposed to add the PoPC for ONC–ACBs in § 170.523(r) in order to address business relationships between ONC–ACBs and ONC–ATLs (84 FR 7456). To encourage market competition, we proposed to require ONC–ACBs to accept test results from any ONC–ATL that is in good standing under the Program and is compliant with its ISO/IEC 17025 accreditation requirements. However, if an ONC–ACB has concerns about accepting test results from a certain ONC–ATL, the ONC–ACB would have an opportunity to explain the potential issues to ONC and NVLAP, and on a case-by-case basis, ONC could consider the facts and make the final determination.

Comments. Multiple commenters expressed support for the proposed requirement that ONC–ACBs must accept test results from any ONC–ATL in good standing. One commenter expressed an opinion that this proposal has value in ensuring the credibility of the Program. Another commenter agreed that this proposal would encourage market competition and provide more options to developers. One commenter recommended that ONC–ATLs should also be required to provide their results to any ONC–ACB to which the developer has chosen to present its health IT for certification, stating that this consistency across ONC–ACBs and ONC–ATLs would ensure market competition.

Response. We thank commenters for their input. We have finalized the PoPC for ONC–ACBs in § 170.523(r) as proposed. While an ONC–ATL attempting to inappropriately restrict developers' choice of ONC–ACBs to those favored by the ONC–ATL would not support appropriate competition, we do not believe it would be practical to mandate direct transmission of ONC–ATL results to any ONC–ACB designated by the developer, in part because developers often do not initiate engagement with an ONC–ACB until after they have received and had a chance to review their ONC–ATL results. To date, we are not aware of substantial evidence that the standard practice of NVLAP-accredited testing laboratories providing test results to the client who engaged them to test their Health IT Modules is not serving as a sufficient safeguard against anti-competitive behavior on the part of ONC–ATLs in relation to their client developers' selection of ONC–ACBs.

4. Mandatory Disclosures and Certifications

We proposed to revise the PoPC in § 170.523(k) to remove § 170.523(k)(1)(ii)(B) because certifications can only be issued to Health IT Modules and not Complete EHRs (84 FR 7456). We also proposed to revise § 170.523(k)(1)(iii)(A) to broaden the section beyond the Promoting Interoperability (PI) Programs. We proposed to revise the section to include a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities, whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification.

We also proposed to remove the provision in § 170.523(k)(3) that requires a certification issued to a pre-coordinated, integrated bundle of Health IT Modules to be treated the same as a certification issued to a Complete EHR for the purposes of § 170.523(k)(1), except that the certification must also indicate each Health IT Module that is included in the bundle (84 FR 7457).

We proposed to revise § 170.523(k)(4) to clarify that a certification issued to a Health IT Module based solely on the applicable certification criteria adopted by the ONC Health IT Certification Program must be separate and distinct from any other certification(s) based on other criteria or requirements (84 FR 7457).

We also proposed changes related to transparency attestations and disclosures of limitations in section III.B.5 of the Proposed Rule preamble (84 FR 7437 and 7438). Additionally, we proposed other new PoPC for ONC–ACBs as discussed in sections VII.B.5 (84 FR 7501) and VII.D (84 FR 7506 and 7507) of the Proposed Rule preamble.

Comments. Multiple commenters expressed support for ONC's proposal to include a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities—whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification. One commenter endorsed the transparency that this proposal would provide, noting that it would help providers budget for their health IT, but also expressed concern that requiring developers to disclose how much they charge for a particular functionality may be impractical due to variations across contracts and over time, or potentially have unintended consequences on market pricing. Multiple commenters expressed support for our proposal to remove subsection § 170.523(k)(1)(ii)(B). One commenter expressed support for ONC's proposed revisions to § 170.523(k)(4). Another commenter was supportive of the proposal to remove the provision in § 170.523(k)(3).

Response. We thank commenters for their support. We have finalized the proposals, in their entirety, as proposed. To clarify, the finalized revision in § 170.523(k) requires disclosure of a detailed description of all known material information concerning

additional *types* of costs or fees a user may be required to incur or pay to implement or use the Health IT Module's capabilities to achieve any use within the scope of the health IT's certification. We emphasize that (unless required elsewhere in CFR part 170) the requirement is for a description of the *types* of costs or fees, not predicted *amounts* of these costs or fees across the full array of probable implementation circumstances or over time. Among other considerations, we note that costs required to achieve some particular uses within the scope of some certifications may be for third-party services outside the control of the developer required to disclose the detailed description.

C. Principles of Proper Conduct for ONC–ATLs—Records Retention

We proposed to revise the records retention requirement in § 170.524(f) to include the ''life of the edition'' as well as 3 years after the retirement of an edition related to the testing of Health IT Module(s) to an edition of certification criteria (84 FR 7457). The circumstances are the same as in section V.B.1 of the Proposed Rule preamble, as summarized above. Therefore, we proposed the same revisions for ONC–ATLs as we did for ONC–ACBs. We did not receive any comments specific to this proposed revision to the PoPC for ONC–ATLs. In light of the absence of comments, we have finalized the revisions as proposed.

VI. Health IT for the Care Continuum

Health IT should help promote and support patient care when and where it is needed. This means health IT should help support patient populations, specialized care, transitions of care, and practice settings across the care continuum. In the Proposed Rule, we provided a history of the many actions we have taken since the inception of the ONC Health IT Certification Program through the Proposed Rule (84 FR 7457). As stated in the Proposed Rule, section 4001(b)(i) of the Cures Act instructs the National Coordinator to encourage, keep, or recognize, through existing authorities, the voluntary certification of health IT under the Program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. This provision of the Cures Act closely aligns with our ongoing collaborative efforts with both Federal partners and stakeholders within the health care and health IT community to encourage and support the advancement of health IT for a wide range of clinical settings. These initiatives have included projects related to clinical priorities beyond those specifically included in the EHR Incentive Programs (now called the Promoting Interoperability Programs) including efforts in public health, behavioral health, and long-term and post-acute care. We noted in the Proposed Rule that these initiatives often include the development of non-regulatory informational resources to support the specific implementation goal and align with the technical specifications already available in the Program for certification. To advance these efforts, we also explained in the Proposed Rule that we generally consider a range of factors including: Stakeholder input and identification of clinical needs and clinical priorities, the evolution and adoption of health IT across the care continuum, the costs and benefits associated with any policy or implementation strategy related to care settings and sites of service, and potential regulatory burden and compliance timelines. Our goal was then and is now to support the advancement of interoperable health IT and to promote health IT functionality in care and practice settings across the care continuum (see 80 FR 62604). As stated in the Proposed Rule (84 FR 7458), generally, our approach can be summarized in three parts:

- First, we analyze existing certification criteria to identify how such criteria may be applicable for medical specialties and sites of service.
- Second, we focus on the real-time evaluation of existing and emerging standards to determine applicability to medical specialties and sites of service as well as to the broader care continuum, including the evaluation of such standards for inclusion in the ONC Interoperability Standards Advisory (ISA).[68]
- Third, we may work in collaboration with stakeholders to support the development of informational resources for medical specialties and sites of service for which we identify a need to advance the effective implementation of certified health IT.

We continue to believe this approach is economical, flexible, and responsive for both health care providers and the health IT industry. It is also in alignment with the provisions of section 4001(a) in the Cures Act related to burden reduction and promoting interoperability. We are committed to continuing to work with stakeholders to promote the adoption of health IT to support medical specialties and sites of service and to help ensure that providers have the tools they need (such as access to essential health information across care settings) to support patients at the point of care.

A. Health IT for Pediatric Setting

Section 4001(b)(iii) of the Cures Act—''Health information technology for pediatrics'' requires:

- First, that the Secretary, in consultation with relevant stakeholders, shall make recommendations for the voluntary certification of health IT for use by pediatric health providers to support the health care of children, and
- Second, that the Secretary shall adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children.

In the Proposed Rule (84 FR 7458), we described our approach to stakeholder engagement, the analysis used to develop the recommendations, the specific 2015 Edition certification criteria that support each recommendation, and the voluntary certification of health IT for use by pediatric health providers to support the health care of children.

Comments. We received several comments requesting further clarification on whether the pediatric health IT recommendations will be adopted as an independent certification program and/or certification criteria designated specifically for pediatric care. One commenter recommended that pediatric provisions should be formalized over time within what they refer to as the current pediatric program and not as a separate program, and that this future aligns with the 2015 Children's EHR Format. One commenter also sought clarification as whether ONC intends for other government agencies/programs such as CHIP, to develop conditions of participation or financial incentives around the adoption of certification criteria identified in this rulemaking. We also received several comments stating that since current EHRs have pediatric capabilities, there is no need to specify requirements in regulation, and that there is no value in having EHRs certified as ''pediatric-friendly,'' only increased costs. We also received several comments stating that our approach reflects an attempt to retrofit the needs of pediatric patients by using adult requirements.

Response. We thank commenters for their feedback. The comments we received suggests a need for greater clarity on our approach. We therefore reiterate that we did not propose to adopt care- or practice-specific certification tracks, or additional

[68] *https://www.healthit.gov/isa/.*

voluntary program(s), in parallel to the existing voluntary ONC Health IT Certification Program. In the Proposed Rule, we reiterated our statements from the 2015 Edition final rule, which explained that we did not intend to develop and issue separate regulatory certification ''paths'' or ''tracks'' for particular care or practice settings (*e.g.,* a ''long-term and post-acute care (LTPAC) certification'') because it would be difficult to *independently* construct such ''paths'' or ''tracks'' in a manner that would align with other relevant programs and specific stakeholder needs. We further stated that stakeholders had indicated that separate certification pathways could have unintended consequences related to increasing burden on health care providers and health IT developers. We also stated that we would welcome the opportunity to work with HHS agencies, other agencies, and provider associations in identifying the appropriate functionality and certification criteria in the Program to support their stakeholders (80 FR 62704). In response to the comments regarding our approach to implement section 4001(b) of the Cures Act, we clarify that the 2015 Edition certification criteria identified for the voluntary certification of health IT for use by pediatric health providers are agnostic to the age of the patient (with the exception of the pediatric vital signs in the USCDI). Therefore, we believe our approach to fulfilling the Cures Act requirement for pediatric health care providers and settings, which involves identifying existing, new, or revised 2015 Edition criteria—as applicable to an identified clinical or interoperability priority—is appropriate across patient populations. We also note that our authority is limited to implementing the described requirements of the Cures Act related to pediatric settings. We cannot speak for the actions of other Federal agencies, but would note once again that we have taken a limited regulatory approach to implementing the pediatric provisions of the Cures Act.

Comments. We received multiple comments requesting clarification on the intended use and functionality of the Certified Health IT Products List (CHPL) for pediatric certification, such as guidance on navigating the CHPL to identify relevant products based on pediatric care settings.

Response. We thank stakeholders for their comments on the CHPL. We do not intend to have a separate tag functionality on the CHPL that identifies a product specifically for pediatric care. We did not propose, and do not intend, for there to be a separate certification pathway or a new ONC certification designation called pediatric certification. However, we recognize that beyond certification and testing there are certain implementation needs that are important for pediatric care and services. We agree with the overwhelming prior feedback from stakeholders stating that they should not have to purchase separate products that contain universally applicable functionality, such as the ''API functionality'' certification criteria. We are exploring options for non-regulatory informational resources on effective implementation of health IT for use by pediatric health providers to expand the availability of health IT products supporting the care of children.

Comments. We received comments regarding how the approach for voluntary certification of health IT for use by pediatric health providers might be applicable to other medical specialties and use cases. One commenter noted that the pediatric experience is scalable and should be extended to other disciplines. Another commenter sought clarification if this model could be used for broad applicability to multiple medical specialties such as pathologists.

Response. We thank these commenters for identifying the applicability of our approach to pediatrics to other medical specialties. We confirm that our approach for advancing health IT can be used for other use cases and medical specialties, and welcome the opportunity to engage with stakeholders representing a wide range of medical specialties or sites of service to provide insight into this process and to inform stakeholder-led efforts to improve clinically-relevant health IT implementation across specialties and settings of care.

1. Background and Stakeholder Convening

Over the past ten years, a number of initiatives have focused on the availability and use of effective health IT tools and resources for pediatric care. These have included a number of public-private partnerships including efforts between HHS, State agencies, and health systems for innovative projects that range from care coordination enterprise solutions to immunization information systems and to point of care solutions for specialty needs. In order to learn from and build upon these efforts, ONC has engaged with stakeholders in both the public and private sector including other Federal, State and local government partners, health care providers engaged in the care of children, standards developing organizations, charitable foundations engaged in children's health care research, and health IT developers supporting pediatric care settings. For example, significant work has been done by the Agency for Healthcare Research and Quality (AHRQ), CMS, the Health Resources and Services Administration (HRSA), and organizations around the Children's EHR Format (Children's Format), which is critical to any discussion of the pediatric health IT landscape.[69]

The Children's Format was authorized by the 2009 Children's Health Insurance Program Reauthorization Act (CHIPRA)[70] and developed by AHRQ in close collaboration with CMS. It was developed to bridge the gap between the functionality present in most EHRs currently available and the functionality that could optimally support the care of children. Specifically, the Children's Format provides information to EHR system developers and others about critical functionality and other requirements that are helpful to include in an EHR system to address health care needs specific to the care of children. The final version of the Children's Format, released in 2015, consists of 47 high priority functional requirements in 19 topic areas that focus on improvements that would better support the safety and quality of care delivered to children. The Children's Format was intended as a starting point for developers, users, and purchasers for informing an approach for pediatric voluntary certification. We refer to the Voluntary Edition proposed rule for a description of our prior discussion around the Children's Format (79 FR 10930).

In the summer of 2017, the American Academy of Pediatrics (AAP) reviewed the 2015 Children's Format using a robust analytical process and engagement with their members. The result was a prioritized list of eight clinical priorities to support pediatric health care (''Priority List''). In October 2017, we held a technical discussion with stakeholders titled ''Health IT for Pediatrics'' with the specific purpose of obtaining input from an array of stakeholders in an effort to draw correlations between the pediatric providers' clinical priorities identified in the Priority List with the detailed

[69] Agency for Health Care Information and Technology. Health Information Technology. *http://healthit.ahrq.gov/health-it-tools-and-resources/childrens-electronic-health-record-ehr-format.* Accessed September, 2017.

[70] Pub. L. 111–3, section 401 *https://healthit.ahrq.gov/sites/default/files/docs/citation/children-ehr-format-enhancement-final-recommendation-report-abridged.pdf.*

technical requirements outlined in the Children's Format and the capabilities and standards that could be included in certified health IT. Through this collaborative approach, the meeting participants identified a set of priority needs for health IT to support pediatric care based upon those identified by the Priority List and the primary correlation to the Children's Format.

2. Recommendations for the Voluntary Certification of Health IT for Use in Pediatric Care

To support the first part of section 4001(b) of the Cures Act, we considered the historical efforts on the Children's Format, the input from stakeholders, and our own technical analysis and review of health IT capabilities and standards to develop a set of recommendations for voluntary certification of health information technology for use by pediatric health providers to support the health care of children. These include eight recommendations related to the Priority List:

- Recommendation 1: Use biometric-specific norms for growth curves and support growth charts for children
- Recommendation 2: Compute weight-based drug dosage
- Recommendation 3: Ability to document all guardians and caregivers
- Recommendation 4: Segmented access to information
- Recommendation 5: Synchronize immunization histories with registries
- Recommendation 6: Age- and weight- specific single-dose range checking
- Recommendation 7: Transferrable access authority
- Recommendation 8: Associate maternal health information and demographics with newborn

We also developed two additional recommendations beyond the Priority List, which relate to other items within the Children's Format that are considered important to pediatric stakeholders. These additional recommendations, which may be supported by certified health IT, are as follows:

- Recommendation 9: Track incomplete preventative care opportunities
- Recommendation 10: Flag special health care needs

In order to implement the second part of section 4001(b) of the Cures Act for the adoption of certification criteria to support the voluntary certification of health IT for use by pediatric health care providers, we identified both the 2015 Edition certification criteria and the new or revised certification criteria proposed in the Proposed Rule that support the 10 recommendations for the voluntary certification of health IT for use by pediatric health providers to support the health care of children. In the Proposed Rule (84 FR 7459), we directed readers to the appendix of the Proposed Rule for a set of technical worksheets, which include a crosswalk of the various criteria specifically associated with each recommendation. These worksheets outlined the following information:

- The alignment of each recommendation to the primary Children's Format [71] item identified by stakeholders
- The alignment of each recommendation to the 2015 Edition certification criteria and the new or revised criteria described in the Proposed Rule
- Supplemental items from the Children's Format for each recommendation and the related 2015 Edition certification criteria

We also sought comment on the following:

1. Relevant gaps, barriers, safety concerns, and resources (including available best practices, activities, and tools) that may impact or support feasibility of the recommendation in practice.

2. Effective use of health IT itself in support of each recommendation as it relates to provider training, establishing workflows, and other related safety and usability considerations.

3. If any of the 10 recommendations should not be included in ONC's final recommendations for voluntary certification of health IT for use by pediatric health providers to support the health care of children.

4. Any certification criteria from the Program that is identified for the 10 recommendations that should not be included to support the specific recommendation.

Comments. We received many comments asking for detailed guidance and/or implementation specifications post final rulemaking, with one commenter noting that the majority of recommendations require additional capabilities beyond the scope of any aligned existing or proposed certification criteria. We also received many comments providing implementation recommendations specific to the 10 ONC recommendations for the voluntary certification of health IT for use by pediatric health providers such as adding in developmental activity milestones, including what versions of growth charts should be supported, and including listings to clearly identify medical home providers. Several commenters also referenced concerns regarding the feasibility of implementing the content included as part of the pediatric health IT technical worksheet crosswalk analysis included in the Proposed Rule appendix for Recommendation 5 ''Synchronize immunization histories with registries.'' In this regard, several commenters noted that FHIR is not currently consistent with CDC/AIRA standards or practices for immunization data submission or query/response, and that public health is not currently funded to provide this capability from IIS.

Response. We thank commenters for their useful input regarding the technical worksheets in the appendix we included for the Proposed Rule. As we stated in the Proposed Rule, these comments, and the detailed insights received through stakeholder outreach, will inform the future development of a non-binding informational guide or informational resource to provide useful information for health IT developers and pediatric care providers seeking to successfully implement these health IT solutions in a clinical setting. To facilitate adoption of the ten recommendations, we are developing a Pediatric Health IT Developer Informational Resource and a Pediatric Health IT Provider Informational Resource to be available for respective use in 2020. As such, we appreciate the comments we received specific to implementation recommendations and will take them into account in the support of the creation of non-regulatory informational resources for health IT developers and other stakeholders. We plan to continue working with stakeholders as we further develop and consider technical and implementation recommendations we have received through solicited public comments, the Health Information Technology Advisory Committee (HITAC), and other engagements. We also direct readers to our ''pediatrics health IT'' web page (*www.healthIT.gov/pediatrics*) for information on future work pertaining to health IT for pediatric care.

Comments. We received several comments suggesting the use of pediatric-focused clinicians and settings to test EHR systems as part of these provisions, specifically recommending that we should require EHR developers to use pediatric-focused scenarios and mock pediatric patients when testing functionality, as well as requiring the

[71] *http://healthit.ahrq.gov/health-it-tools-and-resources/childrens-electronic-health-record-ehr-format.*

inclusion of pediatric clinicians as part of end-user testing.

Response. We thank commenters for their input. We agree that it would be beneficial for health IT developers to include pediatric-focused testing of their health IT especially with regards to ensuring patient safety. We note that we have established requirements for real world testing that requires health IT developers to real world test their health IT for the types of setting(s) in which it is intended for use (we refer readers to section VII.B.5 for more information on real world testing Condition and Maintenance of Certification requirements).

a. 2015 Edition Certification Criteria

In order to implement the second part of section 4001(b) of the Cures Act to adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children, we identified the following already adopted 2015 Edition certification criteria in the Proposed Rule that support the recommendations. The already adopted 2015 Edition criteria are as follows:

- ''API functionality'' criteria (§ 170.315(g)(7)–(g)(9)) which address many of the challenges currently faced by patients and by caregivers such as parents or guardians accessing child's health information, including the ''multiple portal'' problem, by potentially allowing individuals to aggregate health information from multiple sources in a web or mobile application of their choice.
- ''Care plan'' criterion (§ 170.315(b)(9)) which supports pediatric care by facilitating the documentation of electronic health information in a structured format to improve care coordination (80 FR 62648 and 62649).
- ''Clinical decision support'' (CDS) criterion (§ 170.315(a)(9)) which supports pediatric care by enabling interventions based on the capture of biometric data.
- ''Common Clinical Data Set'' (§ 170.315(b)(4) and § 170.315(b)(5)) which includes *optional* pediatric vital sign data elements including as optional the reference range/growth curve for three pediatric vital signs—BMI percent per LOINC identifiers for age per sex, weight per length/sex, and head occipital-frontal circumference for children less than three years of age.
- ''Data segmentation for privacy'' send criterion and receive criterion (§ 170.315(b)(7) and § 170.315(b)(8)) which provides the ability to: Create a summary record that is tagged at the document level as restricted and subject to re-disclosure; receive a summary record that is document-level tagged as restricted; separate the document-level tagged document from other documents received; and view the restricted document without having to incorporate any of the data from the document.
- ''Demographics'' criterion (§ 170.315(a)(5)) which supports pediatric care through the capture of values and value sets relevant for the pediatric health care setting as well as allowing for improved patient matching which is a key challenge for pediatric care.
- ''Electronic Prescribing'' criterion (§ 170.315(b)(3)) which includes an *optional* Structured and Codified Sig Format, which has the capability to exchange weight-based dosing calculations within the NCPDP SCRIPT 10.6 standard and limits the ability to prescribe all oral, liquid medications in only metric standard units of mL (*i.e.,* not cc) important for enabling safe prescribing practices for children.
- ''Family health history'' criterion (§ 170.315(a)(12)) which supports pediatric care because it leverages concepts or expressions for familial conditions, which are especially clinically relevant when caring for children.
- ''Patient health information capture'' criterion (§ 170.315(e)(3)) which supports providers' ability to accept health information from a patient or authorized representative. This criterion could support pediatric care through documentation of decision-making authority of a patient representative.
- ''Social, psychological, and behavioral data'' criterion (§ 170.315(a)(15)) which supports integration of behavioral health data into a child's record across the care continuum by enabling a user to record, change, and access a patient's social, psychological, and behavioral data based using SNOMED CT® and LOINC® codes.
- ''Transitions of care'' criterion (§ 170.315(b)(1)) which supports structured transition of care summaries and referral summaries that help ensure the coordination and continuity of health care as children transfer between different clinicians at different health care organizations or different levels of care within the same health care organization.
- ''Transmission to immunization registries'' criterion (§ 170.315(f)(1)) which supports the safe and effective provision of child health care through immunizations and registry linkages. This criterion also provides the ability to request, access, and display the evaluated immunization history and forecast from an immunization registry for a patient. Immunization forecasting recommendations allow for providers to access the most complete and up-to-date information on a patient's immunization history to inform discussions about what vaccines a patient may need based on nationally recommended immunization recommendations (80 FR 62662 through 62664).
- ''View, download, and transmit to 3rd party'' (VDT) criterion (§ 170.315(e)(1)) which supports transferrable access authority for the pediatric health care setting and provides the ability for patients (and their authorized representatives) [72] to view, download, and transmit their health information to a 3rd party.

We noted in the Proposed Rule (84 FR 7460) that some of these criteria may be updated based on proposals contained in the Proposed Rule (see further discussion below on new or revised certification criteria); and stated that we continue to believe that prior to any such updates, technology that is currently available and certified to these 2015 Edition criteria can make a significant impact in supporting providers engaged in the health care of children. We invited readers to use the technical worksheets in the appendix of the Proposed Rule to inform their public comment on the recommendations, the inclusion of specific items from the Children's Format, and the identified 2015 Edition certification criteria as they relate specifically to use cases for pediatric care and sites of service.

b. New or Revised Certification Criteria

In order to implement the second part of section 4001(b)(iii) of the Cures Act to adopt certification criteria to support the voluntary certification of health information technology for use by pediatric health providers to support the health care of children, we also identified new or revised 2015 Edition certification criteria (and standards) in the Proposed Rule (84 FR 7460) that support the recommendations. These proposed criteria and standards include:

- New API criterion (§ 170.315(g)(10)) which would serve to implement the Cures Act requirement to permit health information to be accessed, exchanged,

[72] The VDT criterion includes a ''patient-authorized representative'' concept that aligns with the use of the term under the EHR Incentive Program. A ''patient-authorized representative'' is defined as any individual to whom the patient has granted access to their health information (see also 77 FR 13720). However, consent is not needed for minors, for whom existing local, state, or Federal law grants their parents or guardians access (see also 77 FR 13720).

and used from APIs without special effort.

- New ''DS4P'' criteria (two for C–CDA ((§ 170.315(b)(12)) and (§ 170.315(b)(13)) and one for FHIR (§ 170.315(g)(11))) that would support a more granular approach to privacy tagging data for health information exchange supported by either the C–CDA or FHIR-based exchange standards.
- New electronic prescribing certification criterion (§ 170.315(b)(11)), which would support improved patient safety and prescription accuracy, workflow efficiencies, and increased configurability of systems including functionality that could support pediatric medication management.
- USCDI (§ 170.213) and USCDI-based criteria which enables the inclusion of pediatric vital sign data elements, including the reference range/scale or growth curve for BMI percentile per age and sex, weight for age per length and sex, and head occipital-frontal circumference. Each of the new or revised certification criteria and standards are further described in other sections of this final rule, including all final actions related to the criteria (some of which are described below in the response to comments).

Comments. A majority of comments received supported our recommendations for the voluntary certification of health IT for use by pediatric health providers to support the health care of children along with the alignment with the Children's Format and 2015 Edition certification criteria. Several commenters suggested that the 10 recommendations should only be the first step and encouraged future development of additional recommendations using the Children's Format. Commenters were also pleased with the 10 recommendations selected by ONC from the Children's Format stating that they represent a strong, positive step forward for improving EHRs used in the care of children. Many commenters stated that they support the continued alignment with the 2015 Edition recommendations.

Response. We thank commenters for their support and feedback. As such, we have maintained the 10 recommendations for the voluntary certification of health IT for use by pediatric health providers to support the health care of children. We have finalized in this final rule the majority of the aligned proposed new 2015 Edition certification criteria that support the voluntary certification of health IT for use by pediatric health providers, with the exception of the proposed criterion for ''consent management'' in § 170.315(g)(11) since we did not finalize our proposal for the criterion in this final rule. The functionality of the proposed new ''DS4P'' criteria have been incorporated into the already adopted 2015 Edition DS4P criteria DS4P-send (§ 170.315(b)(7)) and DS4P-receive (§ 170.315(b)(8)) now referred to as ''Security tags—Summary of Care-send'' and ''Security tags—Summary of Care—receive,'' respectively. The functionality of the proposed new e-Rx criterion was also incorporated in the already adopted e-Rx criterion (§ 170.315(b)(3)). Last, we have removed the ''Common Clinical Data Set'' (§ 170.315(b)(4) and § 170.315(b)(5)) from the 2015 Edition in this final rule.

We note that we are aware that the NCPDP SCRIPT Standard Version 2017071 Implementation Guide contains a number of requirements intended to improve accurate dosing and pediatric patient safety. One such requirement is the inclusion of the most recent patient height and weight in the Observation Segment on all new and renewal prescriptions sent from the prescriber to the pharmacy, along with the date associated with these measures, for all patients 18 years old and younger. We are also aware of the challenges that such a requirement may pose on specific providers and under certain circumstances where height and/or weight is not required or applicable for dosing of the product. We believe additional work must be done on refining this requirement, and will continue to monitor standards and industry advancements before proposing such a requirement. At this time, we recommend vital signs to be included in all electronic prescriptions for all patient populations when available and where applicable.

The 10 recommendations and the aligned 2015 Edition certification criteria support the health IT needs of pediatric care providers. We believe further support can be provided through non-regulatory informational resources. These resources can help inform technical and implementation specifications for health IT developers and products for use by pediatric health providers to support the health care of children. We also agree with commenters that the 10 recommendations are a first step and welcome input and collaboration from the health IT industry and health care providers to continue efforts to develop and build a health IT infrastructure supporting pediatric care and other specialty care and sites of service across the continuum.

B. Health IT and Opioid Use Disorder Prevention and Treatment—Request for Information

We identified a need to explore ways to advance health IT across the care continuum to support efforts to fight the opioid epidemic. For that purpose, in the Proposed Rule, we included a request for information (RFI) related to health IT and opioid use disorder prevention and treatment (84 FR 7461 through 7465). We received over 100 comments in responses to this RFI, which included recommendations from the HITAC. We appreciate the feedback and recommendations provided by commenters and the HITAC taskforce, respectively. We plan to share this feedback with appropriate Department partners.

VII. Conditions and Maintenance of Certification Requirements for Health IT Developers

Section 4002 of the Cures Act modifies section 3001(c)(5) of the Public Health Service Act (PHSA) to require the Secretary of HHS, through notice and comment rulemaking, to establish Conditions and Maintenance of Certification requirements for the Program. Specifically, health IT developers or entities must adhere to certain Conditions and Maintenance of Certification requirements concerning information blocking; appropriate exchange, access, and use of electronic health information; communications regarding health IT; application programming interfaces (APIs); real world testing; attestations regarding certain Conditions and Maintenance of Certification requirements; and submission of reporting criteria under the EHR Reporting Program under section 3009A(b) of the PHSA.

A. Implementation

To implement section 4002 of the Cures Act, we proposed an approach whereby the Conditions and Maintenance of Certification requirements express initial certification requirements for health IT developers and their certified Health IT Module(s) as well as ongoing maintenance requirements that must be met by both health IT developers and their certified Health IT Module(s) under the ONC Health IT Certification Program (Program). If these requirements are not met, the health IT developer may no longer be able to participate in the Program and/or its certified health IT may have its certification terminated. We proposed to implement each Condition of Certification requirement with further specificity as it applies to

the Program. We also proposed to establish Maintenance of Certification requirements for certain Conditions of Certification requirements as standalone requirements. As we stated in the Proposed Rule, this approach would establish clear baseline technical and behavior Conditions of Certification requirements with evidence that the Conditions of Certification requirements are continually being met through the Maintenance of Certification requirements.

Comments. We received comments expressing general support for the concept of requiring Conditions and Maintenance of Certification requirements. Commenters stated that these requirements are a step forward toward promoting transparency, improving usability, and achieving interoperability of health IT. We also received comments asserting that the Conditions and Maintenance of Certification requirements should only apply to developers of certified health IT.

Response. We thank commenters for their support. We provide further details on each of the Conditions and Maintenance of Certification requirements within their respective subsections in this section of the final rule. However, to clarify our approach to the Conditions and Maintenance of Certification requirements in response to comments, the Conditions and Maintenance of Certification requirements, except for the ''information blocking'' and ''assurances'' Conditions and Maintenance of Certification requirements, apply only to actions and behaviors of health IT developers related to their certified health IT as well as to the certified health IT itself. For the ''information blocking'' and ''assurances'' Conditions and Maintenance of Certification requirements, consistent with the Cures Act provisions and our implementation of section 3022(a) (information blocking) of the PHSA, a health IT developer is also responsible to ensure that all of its health IT and related actions and behaviors do not constitute information blocking or inhibit the appropriate access, exchange, and use of electronic health information (EHI). We refer readers to section VIII of this preamble for further discussion of the information blocking regulations.

B. Provisions

1. Information Blocking

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification requirement under the Program, not take any action that constitutes ''information blocking'' as defined in section 3022(a) of the PHSA (see 3001(c)(5)(D)(i) of the PHSA). We proposed to establish this Information Blocking Condition of Certification in § 170.401. We proposed that the Condition of Certification would prohibit any health IT developer who has at least one health IT product certified under the Program from taking any action that constitutes information blocking as defined by section 3022(a) of the PHSA and proposed in § 171.103. We clarified in the Proposed Rule that this proposed ''information blocking'' Condition of Certification and its requirements would be substantive requirements of the Program and would rely on the definition of ''information blocking'' established by section 3022(a) of the PHSA and proposed in § 171.103 (84 FR 7465).

We received no comments specifically about the Information Blocking Condition of Certification and have adopted the Condition of Certification as proposed. We received many comments regarding the information blocking provision, and have responded to those comments in the information blocking discussion in section VIII of this preamble. We also refer readers to section VII.D of this final rule for additional discussion of ONC's enforcement of this and other Conditions and Maintenance of Certification requirements.

2. Assurances

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification requirement under the Program, provide assurances to the Secretary, unless for legitimate purposes specified by the Secretary, that it will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA, or any other action that may inhibit the appropriate exchange, access, and use of electronic health information (EHI). We proposed to implement this Condition of Certification and accompanying Maintenance of Certification requirements in § 170.402. As a Condition of Certification requirement, a health IT developer must comply with the Condition of Certification as recited here and in the Cures Act. We discussed in section VIII of the Proposed Rule the proposed reasonable and necessary activities specified by the Secretary, which constitute the exceptions to the information blocking definition.

We also proposed to establish more specific Conditions and Maintenance of Certification requirements for a health IT developer to provide assurances that it does not take any action that may inhibit the appropriate exchange, access, and use of EHI. These proposed requirements serve to provide further clarity under the Program as to how health IT developers can provide such broad assurances with more specific actions.

Comments. Most commenters agreed with the central premise of our proposal to adopt the ''assurances'' Condition and Maintenance of Certification requirement, requiring that a health IT developer provide certain assurances to the Secretary, including that, unless done for one of the ''legitimate purposes'' specified by the Secretary, it will not take any actions that constitutes information blocking as defined in section 3022(a) of the PHSA, or any other action that may inhibit the appropriate exchange, access, and use of electronic health information (EHI). Commenters stated that they support ONC's efforts to eliminate barriers that result in information blocking. One commenter stated that it is not clear what constitutes ''satisfactory to the Secretary'' as interpretations may change from Secretary to Secretary, and suggested removing the term ''Secretary.''

Response. We thank commenters for their support. We have finalized our proposal to adopt the ''assurances'' Condition and Maintenance of Certification requirement subject to the clarifications and revisions discussed below. In response to the comment recommending we remove the term ''Secretary'' as Secretaries may change over time, it will not be removed as it is in the authorizing Cures Act statutory language. For clarification, future Secretaries may establish changes to the implementation of the Cures Act ''assurances'' Condition and Maintenance of Certification requirements through notice and comment rulemaking, as has been done with this rulemaking.

a. Full Compliance and Unrestricted Implementation of Certification Criteria Capabilities

We proposed, as a Condition of Certification requirement, that a health IT developer must ensure that its health IT certified under the Program conforms to the full scope of the certification criteria to which its health IT is certified. This has always been an expectation of ONC and users of certified health IT and, importantly, a requirement of the Program. As stated in the Proposed Rule, we believe that by incorporating this expectation as an explicit Condition of Certification requirement under the Program, there

would be assurances, and documentation via the ''Attestations'' Condition and Maintenance of Certification requirements proposed in § 170.406, that all health IT developers fully understand their responsibilities under the Program, including not to take any action with their certified health IT that may inhibit the appropriate exchange, access, and use of EHI. To this point, certification criteria are designed and issued so that certified health IT can support interoperability and the appropriate exchange, access, and use of EHI.

We also proposed that, as a complementary Condition of Certification requirement, health IT developers of certified health IT must provide an assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes. More specifically, developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Such actions may inhibit the appropriate access, exchange, or use of EHI and are therefore contrary to this proposed Condition of Certification requirement. While such actions are already prohibited under the Program (80 FR 62711), making these existing requirements that prohibit developers from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification explicit in this Condition of Certification requirement will ensure that health IT developers are required to attest to them pursuant to the Attestations Condition of Certification requirement in § 170.406, which will in turn provide additional assurances to the Secretary that developers of certified health IT support and do not inhibit appropriate access, exchange, or use of EHI.

As discussed at 84 FR 7466 in our Proposed Rule, actions that would violate this Condition of Certification requirement include failing to fully deploy or enable certified capabilities; imposing limitations (including restrictions) on the use of certified capabilities once deployed; or requiring subsequent developer assistance to enable the use of certified capabilities, contrary to the intended uses and outcomes of those capabilities). The Condition of Certification requirement would also be violated were a developer to refuse to provide documentation, support, or other assistance reasonably necessary to enable the use of certified capabilities for their intended purposes. More generally, any action that would be likely to substantially impair the ability of one or more users (or prospective users) to implement or use certified capabilities for any purpose within the scope of applicable certification criteria would be prohibited by this Condition of Certification requirement. Such actions may include imposing limitations or additional types of costs, especially if these were not disclosed when a customer purchased or licensed the certified health IT.

Comments. We received a comment recommending additional language to allow health IT developers to be able to provide an explanation of how their software conforms to the certification criteria requirements and how they enable the appropriate exchange, access, and use of EHI.

Response. We thank the commenter for their input, but do not accept the recommendation. Health IT must comply with certification criteria as specified in regulation. We also refer readers to the ''Attestations'' Condition of Certification requirement in this section of the preamble for more information regarding how we proposed to provide flexibilities, including a method for health IT developers to indicate their compliance, noncompliance, or the inapplicability of each Condition and Maintenance of Certification requirement as it applies to all of their health IT certified under the Program, as well as the flexibility to specify noncompliance per certified Health IT Module, if necessary. As such, we have finalized the Full Compliance and Unrestricted Implementation of Certification Criteria Capabilities Condition of Certification requirement as proposed that a health IT developer must ensure that its health IT certified under the Program conforms to the full scope of the certification criteria to which its health IT is certified, and that health IT developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. We note that because compliance with the information blocking section of this final rule (Part 171) is not required until six months after the publication date of the final rule, § 170.402(a)(1) also has a six-month delayed compliance date.

Comments. A couple of commenters requested clarification on whether requiring subsequent developer assistance to enable the use of certain certified capabilities would be considered noncompliance with the Condition of Certification requirement, such as managed services, hosting, connecting with exchange networks, or outsourced arrangements under agreement.

Response. We clarify that the purpose of this Condition of Certification requirement is to make certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes. As stated above, the Condition of Certification requirement would be violated were a developer to refuse to provide documentation, support, or other assistance reasonably necessary to enable the use of certified capabilities for their intended purposes (*see* 84 FR 7466). We do not believe that actions by health IT developers to provide their customers with education, implementation, and connection assistance to integrate certified capabilities for their customers would typically constitute actions that interfere with a customer's ability to use certified capabilities for their intended purposes, but in the absence of specific facts, we cannot say that whether there are scenarios that would result in the assistance interfering with a user's ability to access or use certified capabilities for any purpose within the scope of the health IT's certification. As such, education and other assistance may be offered, but care should be taken to do so in a manner that minds the Condition of Certification requirement standards.

Comments. We received a comment asking that health IT developers be required to provide honest communication and expert advice as required by a user.

Response. We appreciate the commenter's suggestion regarding honest communication and expert advice. However, such a requirement would not be consistent with this Condition of Certification requirement, which focuses on assurances that Health IT developers did not take actions that may inhibit the appropriate exchange, access, and use of electronic health information (EHI). We also believe it would be difficult to enforce such a requirement in terms of determining what constitutes an ''honest'' communication and ''expert advice.''

b. Certification to the ''Electronic Health Information Export'' Criterion

We proposed that a health IT developer that produces and electronically manages EHI must certify their health IT to the 2015 Edition ''EHI export'' criterion in § 170.315(b)(10). As

a Maintenance of Certification requirement, we proposed that a health IT developer that produces and electronically manages EHI must provide all of its customers of certified health IT Modules with health IT certified to the functionality included in § 170.315(b)(10) within 24 months of a subsequent final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer. Consistent with these proposals, we also proposed to amend § 170.550 to require that ONC–ACBs certify health IT to the proposed 2015 Edition ''EHI export'' certification criterion when the health IT developer of the health IT Module presented for certification produces and electronically manages EHI. As discussed in section IV.C.1 of the Proposed Rule, the availability of the capabilities in the ''EHI export'' certification criterion promote access, exchange, and use of health information to facilitate electronic access to single patient and patient population health information in cases such as a patient requesting their information, or a health care provider switching health IT systems. As such, health IT developers with health IT products that have health IT Modules certified to the finalized ''EHI export'' certification requirement must make this functionality available to customers and provide assurances that the developer is not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of health information. We discussed the EHI export functionality in section IV.B.4 of the Proposed Rule.

Comments. A couple of commenters expressed their support for the Condition of Certification requirement, noting that certifying health IT to § 170.315(b)(10) would provide greater EHI access to end users. Several commenters requested extending the implementation timeframe to 36 months stating that more time is needed for analysis, product development, and testing, with an additional 12 months for client adoption, testing, and training. A couple of commenters supported the 24-month timeframe, but stated that they did not support ONC dictating the adoption schedule for providers, and that the proposal does not consider the efforts required from providers to plan and execute effective implementation and adoption. One commenter stated that 24 months is not aggressive enough and that the rule should prioritize certain aspects of patient-directed exchange and make these available in 12 months or less. Another commenter suggested that we narrow the type of health IT developer that must certify health IT to § 170.315(b)(10), noting that some Health IT Modules may manage data produced by other Health IT Modules, or received and incorporated from other sources. We did not receive any comments specific to our proposal to amend § 170.550 to require that ONC–ACBs certify health IT to the proposed 2015 Edition ''EHI export'' criterion when the health IT developer of the health IT Module presented for certification produces and electronically manages EHI.

Response. We thank the commenters for their support. In response to comments regarding scope of data export under this criterion, we have modified the proposed ''EHI export'' certification criterion and scope of data export. In doing so, we have also revised our Condition of Certification requirement, which we have finalized in § 170.402(a)(4), that a health IT developer of a certified Health IT Module that is part of a health IT product which electronically stores EHI must certify to the certification criterion in § 170.315(b)(10). Additionally, we clarify that in attesting to § 170.406, a health IT developer must attest accurately in accordance with § 170.402(a)(4) and (b)(2) if the health IT developer certified a Health IT Module(s) that is part of a health IT product which can store EHI. The finalized criterion focuses on the Health IT Module's ability to export EHI for the health IT product's single and patient population, which encompasses the EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. To note, we do not require developers to disclose proprietary information about their products. Also, as clarified above and in § 170.315(b)(10)(iii), we do not require any specific standards for the export format(s) used to support the export functionality.

In regards to when health IT developers must provide all of their users of certified health IT with health IT certified to the functionality included in § 170.315(b)(10), we have removed the proposed language ''within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer.'' Our intention was to provide equity between existing and new health IT developers. However, we have concluded that new health IT developers will not be at a disadvantage to meet the same timeline considering all health IT developers will be aware of requirements necessary for certification when this final rule is published. We also acknowledge the concerns expressed regarding the 24-month timeframe and have extended the compliance timeline to within 36 months of the final rule's publication date, as finalized in § 170.402(b)(2)(i). With the narrowed scope of data export for the criterion, we believe health IT developers should be able to provide all of their customers of Health IT Modules certified to § 170.315(b)(10) with the export functionality included in § 170.315(b)(10) within 36 months. We have also finalized in § 170.402(b)(2)(ii) that on and after 36 months from the publication of this final rule, health IT developers that must comply with the requirements of § 170.402(a)(4) must provide all of their customers of certified health IT with health IT certified to § 170.315(b)(10). From this milestone forward, a health IT developer's participation in the Certification Program obligates them to provide the technical capabilities expressed in § 170.315(b)(10) when they provide such certified health IT to their customers. We will monitor ongoing compliance with this Condition and Maintenance of Certification through a variety of means including, but not limited to, developer attestations pursuant to § 170.406, health IT developers real world testing plans, response to user complaints, and ONC–ACB surveillance activities.

Consistent with the above revisions and in alignment with our proposal to amend § 170.550, we have also amended § 170.550(g)(5) regarding Health IT Module dependent criteria for consistency with the requirements of § 170.402(a)(4) and (b)(2) when a Health IT Module presented for certification is part of a health IT product which can store electronic health information. In addition, we have amended § 170.550(m)(2) to only allow ONC–ACBs to issue certifications to § 170.315(b)(6) until 36 months after the publication date of this final rule. Thus, ONC–ACBs may issue certificates for either § 170.315(b)(6) or (b)(10) up until 36 months after the publication date of this final rule, but on and after 36 months they may only issue certificates for Health IT Modules in accordance with § 170.315(b)(10). We note that ONC–ACBs are required by their ISO/IEC 17065 accreditation to have processes in place to meet the expectations and minimum requirements of the Program. Thus, ONC–ACBs are expected to have processes in place in order to effectively monitor these timeline requirements on and after 36 months after the

publication of this rule, and to additionally ensure that the health IT developer attests accurately to § 170.402(a)(4) and (b)(2). Should a developer fail to comply, the ONC–ACB will follow its processes to institute corrective action and report to ONC in accordance with Program reporting requirements in 45 CFR 170.523(f)(1)(xxii). In the event the developer does not follow through with the corrective action plan established and approved with the ONC–ACB, the ONC–ACB must alert ONC of the health IT developer's failure to comply with the Conditions and Maintenance of Certification requirements.

Comments. A commenter requested ONC add functionality to the CHPL (or in another format) that provides a list of the start and end dates of each previously certified Health IT Module.

Response. We appreciate this suggestion and note that the CHPL already lists certification dates for certified Health IT Modules, including the dates the Health IT Module was last modified, decertified, or made inactive.

c. Records and Information Retention

We proposed that, as a Maintenance of Certification requirement in § 170.402(b)(1), a health IT developer must, for a period of 10 years beginning from the date of certification, retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the Program. In other words, records and information should be retained starting from the date a developer first certifies health IT under the Program and applies separately to each unique Health IT Module (or Complete EHR, as applicable) certified under the Program. This retention of records is necessary to verify health IT developer compliance with Program requirements, including certification criteria and Conditions and Maintenance of Certification requirements. As stated in the Proposed Rule, 10 years is an appropriate period of time given that many users of certified health IT participate in various CMS programs, as well as other programs, that require similar periods of records retention.

In an effort to reduce administrative burden, we also proposed, that in situations where applicable certification criteria are removed from the Code of Federal Regulations before the 10 years have expired, records must only be kept for 3 years from the date of removal for those certification criteria and related Program provisions unless that timeframe would exceed the overall 10-year retention period. This ''3-year from the date of removal'' records retention period also aligns with the records retention requirements for ONC–ACBs and ONC–ATLs under the Program.

We encouraged comment on these proposals and whether the proposed requirements can provide adequate assurances that certified health IT developers are demonstrating initial and ongoing compliance with the requirements of the Program; and thereby ensuring that certified health IT can support interoperability, and appropriate exchange, access, and use of EHI.

Comments. Some commenters requested clarification on what records and information are expected to be maintained and how this is different from the records ONC–ACBs and ONC–ATLs retain. A couple commenters requested clarification on when the records and information retention requirement would take effect. One commenter requested clarification regarding the role of health IT developers that no longer maintain a certified Health IT Module or have their certification suspended. One commenter recommended setting a retention period for record keeping in the event that a health IT developer removes a Health IT Module from market to ensure that potentially short lived Health IT Modules would inadvertently not have their documentation maintained.

Response. We have adopted our proposal in § 170.402(b)(1) without revisions. We continue to believe that 10 years is an appropriate period of time given that many users of certified health IT participate in various CMS programs, as well as other programs, that require similar periods of records retention. We also finalized that in situations where applicable certification criteria are removed from the Code of Federal Regulations, records must only be kept for 3 years from the date of removal for those certification criteria and related Program provisions unless that timeframe would exceed the overall 10-year retention period. We clarify that health IT developers are best situated to determine what records and information in their possession would demonstrate their compliance with all of the relevant Program requirements. We note that it is our understanding that health IT developers are already retaining the majority of their records and information for the purposes of ONC–ACB surveillance and ONC direct review under the Program. We also refer readers to section VII.D of this final rule preamble for additional discussion of records necessary for the enforcement of the Conditions and Maintenance of Certification requirements. In regard to the requested clarification for the role of health IT developers that no longer maintain a certified Health IT Module or have their certification suspended, a health IT developer who does not have any certified Health IT Modules within the Program would no longer have any obligation to retain records and information for the purposes of the Program. However, we note that it may be in the health IT developer's best interest to retain their records and information. For example, records may be useful for health IT developers in any potential investigation or enforcement action taken outside of the ONC Health IT Certification Program such as by the HHS Office of the Inspector General (*e.g.,* information blocking) or the U.S. Department of Justice (*e.g.,* False Claims Act).

d. Trusted Exchange Framework and the Common Agreement—Request for Information

In the Proposed Rule, we included a Request for Information (RFI) as to whether certain health IT developers should be required to participate in the Trusted Exchange Framework and Common Agreement (TEFCA) as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. We received 40 comments on this RFI. We appreciate the input provided by commenters and may consider them to inform a future rulemaking.

3. Communications

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification requirement under the Program, does not prohibit or restrict communication regarding the following subjects:

- The usability of the health information technology;
- The interoperability of the health information technology;
- The security of the health information technology;
- Relevant information regarding users' experiences when using the health information technology;
- The business practices of developers of health information technology related to exchanging electronic health information; and
- The manner in which a user of the health information technology has used such technology.

The Cures Act established the broad communications protections delineated above (referred to hereafter as ''protected communications'') and we proposed in 84 FR 7467 to implement

this general prohibition against developers imposing prohibitions and restrictions on protected communications in § 170.403.

We also recognized that there are circumstances where it is both legitimate and reasonable for developers to limit the sharing of information about their health IT. As such, we proposed to allow developers to impose prohibitions or restrictions on protected communications in certain narrowly defined circumstances. In order for a prohibition or restriction on a protected communication to be permitted, we proposed in 84 FR 7467 that it must pass a two-part test. First, the communication that is being prohibited or restricted must not fall within a class of communications (hereafter referred to as ''communications with unqualified protection'') that is considered to always be legitimate or reasonable—such as communications required by law, made to a government agency, or made to a defined category of safety organizations. Second, to be permitted, a developer's prohibition or restriction on communications must also fall within a category of communications (hereafter referred to as ''permitted prohibitions and restrictions'') for which it is both legitimate and reasonable for a developer to limit the sharing of information about its health IT. This would be because of the nature of the relationship between the developer and the communicator or because of the nature of the information that is, or could be, the subject of the communication. We proposed that a developer's restriction or prohibition that does not satisfy this two-part test would contravene the Communications Condition of Certification requirement. We note that this two-part test strikes a reasonable balance between the need to promote open communication about health IT and related business practices, and the need to protect the legitimate interests of health IT developers and other entities.

Comments. The majority of public comments we received supported the proposed Communications Condition of Certification requirements, with many commenters expressing strong support. Commenters stated that the proposed requirements would enable better communication that would improve health IT and patient care. Some commenters who supported the proposed requirements sought clarification or had specific concerns, including regarding the proposed deadlines for contract modification. These matters are discussed in more detail below. Additionally, a handful of public comments strongly opposed the proposed requirements, primarily based on concerns regarding intellectual property (IP).

Response. We appreciate the overall strong support for the Communications Condition of Certification requirements as proposed and have finalized with modifications in § 170.403. We also recognize the need to provide clarification regarding some aspects of the requirements, including regarding the protections available for IP that are included in the Communications Condition and Maintenance of Certification requirements.

We emphasize that, under section 3001(c)(5) of the PHSA, participation in the ONC Health IT Certification Program (Program) is voluntary. In other words, ONC cannot compel health IT developers to participate in the Program nor can ONC impose consequences (*e.g.,* enforcement actions or penalties) on health IT developers who choose not to participate in the Program. The requirements of the Program are much like requirements for any other voluntary contract or agreement an entity would enter into with the Federal Government. Through the Conditions and Maintenance of Certification requirements, we have essentially offered developers terms for participation in the Program that we believe are appropriate based on: Our statutory instruction and interpretation of the Cures Act; the utility and necessity of using intellectual property, including screenshots, to communicate issues with usability, user experience, interoperability, security, or the way the technology is used (and relatedly, the real and substantial threat to public health and safety resulting from prohibitions and/or restrictions on the communication of screenshots); and the measured approach we have taken throughout the Communications Condition and Maintenance of Certification requirements (which is discussed in detail in this section). Because the Program is voluntary, developers have the option to agree to the terms we have offered or to choose not to participate in the Program. As such, we believe our policies concerning intellectual property, including the use of screenshots, are consistent with other laws and regulations that govern terms for voluntary contracts and agreements with the Federal Government. Further, we believe that the final provisions of this Condition of Certification include appropriate consideration of health IT developers' intellectual property rights.

We further discuss the various aspects of the Communications Condition of Certification requirements, as well as the changes we have made to our proposals, in more detail below.

a. Background and Purpose

The Communications Condition of Certification requirements address industry practices of certified health IT developers that can severely limit the ability and willingness of health IT customers, users, researchers, and other stakeholders to openly discuss and share their experiences and other relevant information about health IT performance, including about the ability of health IT to exchange health information electronically. These practices result in a lack of transparency that can contribute to and exacerbate patient safety risks, system security vulnerabilities, and health IT performance issues.

We explained in the Proposed Rule that the challenges presented by health IT developer actions that prohibit or restrict communications have been examined for some time. The problem was identified in a 2012 report by the Institute of Medicine of the National Academies (IOM) entitled ''Health IT and Patient Safety: Building Safer Systems for Better Care'' [73] (IOM Report). The IOM Report stated that health care providers, researchers, consumer groups, and other health IT users lack information regarding the functionality of health IT.[74] The IOM Report observed, relatedly, that many developers restrict the information that users can communicate about developers' health IT through nondisclosure clauses, confidentiality clauses, IP protections, hold-harmless clauses, and other boilerplate contract language.[75] The report stressed the need for health IT developers to enable the free exchange of information regarding the experience of using their health IT, including the sharing of screenshots relating to patient safety.[76]

Concerns have also been raised by researchers studying health IT,[77] who emphasize that confidentiality and IP provisions in contracts often place broad and unclear limits on authorized uses of information related to health IT,

[73] IOM (Institute of Medicine), Health IT and Patient Safety: Building Safer Systems for Better Care (2012). Available at *http://www.nationalacademies.org/hmd/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx.*

[74] Id. at 37.

[75] Id. at 36, 128.

[76] Id.

[77] See Hardeep Singh, David C. Classen, and Dean F. Sittig, Creating an Oversight Infrastructure for Electronic Health Record-Related Patient Safety Hazards, 7(4) Journal of Patient Safety 169 (2011). Available at *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3677059/.*

which in turn seriously impact the ability of researchers to conduct and publish their research.[78]

The issue of health IT developers prohibiting or restricting communications about health IT has been the subject of a series of hearings by the Senate Committee on Health, Education, Labor and Pensions (HELP Committee), starting in the spring of 2015. Senators on the HELP Committee expressed serious concern regarding the reported efforts of health IT developers to restrict, by contract and other means, communications regarding user experience, including information relevant to safety and interoperability.[79]

Developer actions that prohibit or restrict communications about health IT have also been the subject of investigative reporting.[80] A September 2015 report examined eleven contracts between health systems and major health IT developers and found that, with one exception, all of the contracts protected large amounts of information from being disclosed, including information related to safety and performance issues.[81]

b. Condition of Certification Requirements

i. Protected Communications and Communicators

We proposed in 84 FR 7468 that the protection afforded to communicators under the requirements of the Communications Condition of Certification in § 170.403(a) would apply irrespective of the form or medium in which the communication is made. We proposed in 84 FR 7468 that developers must not prohibit or restrict communications whether written, oral, electronic, or by any other method if they are protected, unless such prohibition or restriction is otherwise permitted by the requirements of this Condition of Certification. Similarly, we proposed that these Condition of Certification requirements do not impose any limit on the identity of the communicators that are able to benefit from the protection afforded, except that employees and contractors of a health IT developer may be treated differently when making communications that are not afforded unqualified protection under § 170.403(a)(2)(i). For example, we proposed that this Condition of Certification's requirements are not limited to communications by health IT customers (*e.g.,* providers) who have contracts with health IT developers.

Comments. Many commenters addressed the scope of protected communications in their comments. Several commenters suggested that the proposed scope of protected communications was too broad. Other commenters stated that the scope should be clarified. One commenter suggested that the scope of private communications that can be shared should be limited and that ONC should require mutual consent for such communications to be made public.

Response. We appreciate these comments. The Cures Act identifies a list of subject areas about which health IT developers cannot prohibit or restrict communications to meet the conditions for certification. The terms we proposed for the protected subject areas are taken from the language in section 4002 of the Cures Act and include:

- The usability of the health information technology;
- The interoperability of the health information technology;
- The security of the health information technology;
- Relevant information regarding users' experiences when using the health information technology;
- The business practices of developers of health information technology related to exchanging electronic health information; and
- The manner in which a user of the health information technology has used such technology.

We continue to interpret the above statutory terms broadly, but within the limiting framework we proposed, which includes a distinction between communications entitled to unqualified protections and those communications not entitled to such protection. We have, however, finalized some provisions with further limiting and clarifying language as well as provided examples to improve understanding of the provisions.

We decline to create a consent requirement as part of the requirements of this Condition of Certification because such a requirement could unnecessarily encumber vital communications protected by the Cures Act. As highlighted above, the Communications Condition of Certification requirements are intended to enable unencumbered communication about usability, interoperability, and other critical issues with health IT, and a consent requirement would chill the ability of users of health IT to engage in that communication as well as be contrary to section 4002 of the Cures Act.

Comments. One commenter stated that the Communications Condition of Certification requirements should apply only to certified health IT, recommending that ONC clarify that the use of ''the health IT'' refers only to the developer's health IT that is certified under the ONC Health IT Certification Program. The commenter stated that the use of ''the health IT'' in the Cures Act can only be reasonably interpreted as referring to the health IT for which a developer is seeking certification, not all of the developer's health IT. Another commenter stated that other health IT, such as billing systems, should be out of scope of this requirement and noted that to do otherwise would create a regulatory imbalance between developers of such health IT who also offer certified health IT and those who do not.

Response. We appreciate these comments regarding restricting the applicability of the Communications Condition of Certification requirements to certified health IT. We clarify that, as with all of the Conditions of Certification requirements, the Communications Condition of Certification requirements apply to developers of health IT certified under the Program and to the conduct of such developers with respect to health IT certified under the Program. By way of example, if a developer had health IT certified under the Program and also had health IT that was not certified under the Program, then only those communications about the certified health IT would be covered by the Communications Condition of Certification requirements.

Comments. We received one comment requesting more specificity on the definition of communicators covered by the Communications Condition of Certification requirements. The commenter expressed concern that the broad scope could impact the ability to maintain confidentiality in traditional business-to-business relationships.

Response. We appreciate this comment and understand the concern noted by the commenter. As stated in the Proposed Rule and finalized in § 170.403, the Communications Condition and Maintenance of Certification requirements generally do not impose any limit on the identity of communicators that are able to benefit from the protection afforded. We also note that there are limited exceptions

[78] Kathy Kenyon, Overcoming Contractual Barriers to EHR Research, Health Affairs Blog (October 14, 2015). Available at *http://healthaffairs.org/blog/2015/10/14/overcoming-contractual-barriers-to-ehr-research/*.

[79] Senate HELP Committee Hearing at 13 and 27 (July 23, 2015), available at *https://www.help.senate.gov/hearings/achieving-the-promise-of-health-information-technology-information-blocking-and-potential-solutions*.

[80] D. Tahir, POLITICO Investigation: EHR gag clauses exist—and, critics say, threaten safety, Politico, August 27, 2015.

[81] Id.

where communications by certain communicators can be restricted. Specifically, as finalized in § 170.403(a)(2)(ii)(A), health IT developers can place limited restrictions on communications by employees and contractors. We believe this will enable traditional business-to-business relationships to continue without undue disruption, including allowing implementation of non-disclosure agreements or other contracts as necessary to maintain confidentiality.

ii. Protected Subject Areas

Comments. We received several comments requesting that we clarify how the Communications Condition of Certification requirements would apply to communications regarding public health reporting, including communications made by public health authorities.

Response. We emphasize that the Cures Act identified a list of subject areas about which we were required to forbid developers from prohibiting or restricting communications. Though public health reporting was not specifically covered by the Cures Act or our proposed regulations, it may be that certain public health communications will fall within the categories established by the statute. We also note that one of the ''communications with unqualified protection'' discussed later in this section is for communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations. Depending on the specific communication in question, a communication about public health reporting or a communication made to public health authorities could be a communication that could not be restricted in any way. We also emphasize that, subject to limited circumstances already discussed above, we do not impose any limit on the identity of the communicators that are able to benefit from protections afforded under the Communications Condition of Certification requirements. Communicators are broadly defined and could include public health agencies and authorities.

Comments. Several commenters had concerns regarding how a developer may address communications that contain false claims or libelous statements. Commenters discussed the need to enable health IT developers to—for example—refute false claims, deal with anonymous claims, and restrict certain communications (such as false statements or communications protected by attorney-client privilege). Some of these comments emphasized that false communications such as libel should not be protected, nor should communications sent by someone who obtained them illegally, such as a hacker. Some of the commenters recommended adding a category of communications that would never be protected under the proposed framework, and such communications would not receive unqualified protection or necessitate permitted restrictions. This would allow a developer to—for example—prohibit or restrict communications that are false or deceptive, would violate a law or court order, or would result in a breach of contract.

Response. We appreciate the concerns expressed by commenters regarding statements that may be false or misleading. However, developers already have legal means and remedies available to them to address such statements, and this rule does not change that. For example, each State has libel laws that address libelous or defamatory statements and provide remedies in situations where the specific facts in a damaging statement can be proven to be untrue. We believe that such statements are best addressed through those laws and that it is neither prudent nor practical for ONC to use the Program and the Communications Condition of Certification requirements to attempt to assess such statements and make determinations as to their veracity.

Further, we note that the Communications Condition of Certification requirements only provide that such protected communications cannot be restricted or prohibited. It is up to the health IT developer whether and how they choose to respond to the protected communication once made. Therefore, we clarify that it is not a violation of the Communications Condition of Certification requirements for developers to respond to false or unlawful comments under applicable law, as they do now, and to pursue litigation or any other available legal remedy in response to any protected communications that are covered by the Communications Condition of Certification. For example, it would not be a violation of the Communications Condition of Certification for a health IT developer who restricts the communication of screenshots as permitted under § 170.403(a)(2)(ii)(D) to pursue litigation for Copyright infringement or violation of contract if a ''protected communication'' disclosed more screenshots than the developer's restriction allowed.

Comments. Several commenters requested that ''safety'' be added as a protected category or that ONC should include in the final rule a specific ban that prohibits any restrictions on communications about health IT-related patient safety. Additionally, several commenters noted that ONC should include specific reporting methods or standards in the final rule to improve safety reporting or add examples to help encourage reporting of safety and security issues. Several commenters also requested that ONC develop protocols for reporting safety issues, and one commenter recommended ONC develop a patient safety reporting system.

Response. In implementing the Cures Act requirement that a health IT developer, as a Condition of Certification requirement under the Program, not restrict communications about health IT, we adhered to the list of protected subject areas identified by Congress in the Cures Act. Those subject areas include communications about ''usability,'' ''relevant information regarding users' experiences when using the health information technology,'' and the ''manner in which a user of the health information technology has used such technology.'' We clarify that patient safety issues related to an interaction with the health IT could be covered in one or more of those categories. Additionally, we agree with commenters that safety-related communications should receive specific protections, and we emphasize that the communication of safety concerns is also addressed as a protected communication receiving ''unqualified protection.'' In the section of this final rule on ''Communications with Unqualified Protection,'' and in § 170.403(a)(2)(i)(B), we state that communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations is a communication about which a developer would be prohibited from imposing any prohibition or restriction.

(A) Usability of Health Information Technology

The term ''usability'' is not defined in the Cures Act, nor in any other relevant statutory provisions. We proposed in 84 FR 7469 that the ''usability'' of health IT be construed broadly to include both an overall judgment on the ''usability'' of a particular certified health IT product by the user, as well as any factor that contributes or may contribute to usability. We proposed that the factors of usability that could be the subject of

protected communications include, but are not limited to, the following: The user interface (*e.g.,* what a user sees on the screen, such as layout, controls, graphics and navigational elements); ease of use (*e.g.,* how many clicks); how the technology supports users' workflows; the organization of information; cognitive burden; cognitive support; error tolerance; clinical decision support; alerts; error handling; customizability; use of templates; mandatory data elements; the use of text fields; and customer support.

Comments. One commenter stated that ''usability'' is too broadly defined and should relate more specifically to judgments on the ease of use of the health IT, rather than factors related to usability.

Response. We do not believe that ''usability'' is inaccurately defined nor too broadly defined. To define usability in the Proposed Rule, we referenced the NIST standard [82] as well as principles recognized by the Healthcare Information and Management Systems Society (HIMSS). We also emphasized that there are a multitude of factors that contribute to any judgment about ''usability,'' including factors contributing to the effectiveness, efficiency, and performance of the health IT. We have finalized the scope of the protected subject area ''usability of its health IT'' in § 170.403(a)(1)(i) as proposed, providing that the ''usability'' of health IT be construed broadly to include both an overall judgment on the ''usability'' of a particular certified health IT product, as well as any of the many factors that could contribute to usability as described in the Proposed Rule. We also note that communications about the usability of health IT may include communications about features that are part of the certified health IT as well as communications about what is not in the certified health IT (*e.g.,* the absence of alerts or features that a user believes would aid in usability or are related to the other subject areas identified by the Cures Act).

(B) Interoperability of Health Information Technology

The Cures Act, as codified in section 3000(9) of the PHSA, provides a definition of ''interoperability'' that describes a type of health IT that demonstrates the necessary capabilities to be interoperable. For the purposes of the Communications Condition of Certification requirements, we proposed that protected communications regarding the ''interoperability of health IT'' would include communications about whether certified health IT and associated developer business practices meet the interoperability definition described in section 3000(9) of the PHSA, including communications about aspects of the technology or developer that fall short of the expectations found in that definition. We stated that this would include communications about the interoperability capabilities of health IT and the practices of a health IT developer that may inhibit the access, exchange, or use of EHI, including information blocking. As previously noted, Congress did not define the terms used in the Communications Conditions of Certification requirements in section 4002(a) of the Cures Act and codified in section 3001(c)(5)(D)(iii) of the PHSA. We believe that ''interoperability'' was appropriately defined in the Proposed Rule by using the interoperability definition that is located elsewhere in section 4003(a)(2) of the Cures Act and codified in section 3000(9) of the PHSA.

We did not receive comments about this aspect of the Proposed Rule, and we have finalized the scope of the protected subject area ''interoperability of its health IT'' in § 170.403(a)(1)(ii) as proposed above.

(C) Security of Health IT

The security of health IT is addressed by the HIPAA Security Rule,[83] which establishes national standards to protect individuals' electronic protected health information (ePHI) that is created, received, maintained, or transmitted by a covered entity or business associate (as defined at 45 CFR 160.103). Covered entities and business associates must ensure the confidentiality, integrity, and availability of all ePHI; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.[84] The HIPAA Security Rule requires health IT developers, to the extent that they are business associates of covered entities, to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.[85] We proposed in 84 FR 7469 that the matters that fall within the topic of health IT security should be broadly construed to include any safeguards, whether or not required by the HIPAA Security Rule, that may be implemented (or not implemented) by a developer to ensure the confidentiality, integrity, and availability of EHI (information that includes ePHI), together with the certified health IT's performance regarding security.

Comments. One commenter noted that it is important that developers are able to remove posts on a website or forum that could compromise the security of health IT and recommended that ONC explicitly allow developers to do so in the final rule.

Response. We recognize the importance of protecting the security of EHI and health IT. We also recognize that our engagement with stakeholders, as well as the language in section 4002 of the Cures Act, emphasize the strong public interest in allowing unencumbered communications regarding the protected subject areas and communications with unqualified protection, which are discussed in more detail below and in § 170.403(a)(2)(i). We emphasize that developers may respond to communications as allowed under applicable law and may pursue any appropriate legal remedy. Taking these factors into consideration, we decline at this time to explicitly allow developers to restrict communications regarding security as suggested by the commenter.

Comments. One commenter requested that ONC consider narrowing the permitted communication of security elements in § 170.403(a)(1)(iii) that might be used to compromise a particular certified health IT's security, for example restricting the sharing of authentication credentials issued to a customer or user to access a system containing sensitive information such as PHI.

Response. We do not believe it is necessary in this final rule to narrow or restrict the information that can be communicated where security elements are included in the communication. As stated above, we believe there is a strong public interest in allowing unencumbered communications regarding the protected subject areas and communications with unqualified protection. Further, assurances that access credentials and PHI communicated under these circumstances will not be shared inappropriately are addressed in the HIPAA Security Rule and relevant State laws, and this rule does not change those protections.

Comments. One comment recommended that the Communications Condition of Certification requirements should protect communication

[82] See *https://www.nist.gov/programs-projects/health-it-usability.*

[83] 45 CFR part 160 and subparts A and C of part 164.

[84] 45 CFR part 160 and subparts A and C of part 164.

[85] Id.

regarding the overall security posture that the health IT developer takes or makes the user take, including communications regarding a system with known and longstanding issues or bugs.

Response. We appreciate this comment and clarify that communications related to the overall security posture taken by a health IT developer would be within the subject area of ''security of its health IT,'' and thus would be protected communications covered by the Communications Condition of Certification requirements. We have finalized the scope of the protected subject area ''security of its health IT'' in § 170.403(a)(1)(iii) as proposed.

(D) User Experiences

The phrases ''relevant information regarding users' experiences when using the health IT'' and ''user experience'' are not defined in the Cures Act nor any other relevant statutory provisions. We proposed in 84 FR 7470 to afford the term ''user experience'' its ordinary meaning. To qualify as a ''user experience,'' we proposed that the experience would have to have been one that is had by a user of health IT. However, beyond this, we did not propose to qualify the types of experiences that would receive protection under the Communications Condition of Certification requirements based on the ''user experience'' subject area. To illustrate the breadth of potential user experiences that would be protected by the proposed Communications Condition of Certification requirements, we proposed that communications about ''relevant information regarding users' experiences when using the health IT'' would encompass, for example, communications and information about a person or organization's experience acquiring, implementing, using, or otherwise interacting with the health IT. We also proposed that this would include experiences associated with the use of the health IT in the delivery of health care, together with administrative functions performed using the health IT. We proposed that user experiences would also include the experiences associated with configuring and using the technology throughout implementation, training, and in practice. Further, we proposed that user experiences would include patients' and consumers' user experiences with consumer apps, patient portals, and other consumer-facing technologies of the health IT developer. We clarified that a ''relevant user experience'' would include any aspect of the health IT user experience that could positively or negatively impact the effectiveness or performance of the health IT.

Comments. One commenter stated that the most relevant aspect of a user's experience of a health IT system is whether that experience resulted in patient safety events and requested that ONC specify patient safety events that arise from the use, misuse, or failure of health IT systems as ''user experiences'' that cannot be covered by gag orders.

Response. As previously noted in our response to patient safety comments above, we reiterate that a user experience resulting in a patient safety event would be covered under the Communications Condition of Certification requirements and that a communication about such an experience would be protected, subject to other applicable laws. Further, communications about ''adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations'' receive unqualified protection as described in § 170.403(a)(2)(i). We noted in the Proposed Rule that the Patient Safety and Quality Improvement Act of 2005 (PSQIA) provides for privilege and confidentiality protections for information that meets the definition of patient safety work product (PSWP). This means that PSWP may only be disclosed as permitted by the PSQIA and its implementing regulations. We clarified that to the extent activities are conducted in accordance with the PSQIA, its implementing regulation, and section 4005(c) of the Cures Act, no such activities shall be construed as constituting restrictions or prohibitions that contravene this Condition of Certification.

We believe that ''user experience'' was appropriately defined in the Proposed Rule and have finalized the scope of the protected subject area ''relevant information regarding users' experiences when using its health IT'' in § 170.403(a)(1)(iv) as proposed, with the clarification provided above regarding patient safety events and to clarify that any communications regarding consumer-facing technologies would need to be about certified consumer-facing technologies per our earlier clarification about the scope of this Condition of Certification being limited to certified health IT.

(E) Manner in Which a User Has Used Health IT

We proposed in 84 FR 7470 that protected communications regarding the ''manner in which a user has used health IT'' would encompass any information related to how the health IT has been used. We also proposed that the terms used to describe the protected subject areas should be construed broadly. We noted in the Proposed Rule that this subject area largely overlaps with the matters covered under the ''user experience'' subject area but may include additional perspectives or details beyond those experienced by a user of health IT. We proposed that the types of information that would fall within this subject area include but are not limited to:

- Information about a work-around implemented to overcome an issue in the health IT;
- customizations built on top of core health IT functionality;
- the specific conditions under which a user used the health IT, such as information about constraints imposed on health IT functionality due to implementation decisions; and
- information about the ways in which health IT could not be used or did not function as was represented by the developer.

We did not receive comments on this specific aspect of the Proposed Rule, and we believe the Proposed Rule appropriately outlined what would fall within the subject matter of the manner in which a user has used health IT. We have finalized the scope of the protected subject area ''manner in which a user of the health IT has used such technology'' in § 170.403(a)(1)(vi) as proposed, with the clarification that ''used'' refers to any uses of the certified health IT by the user and is not limited to uses that involve direct patient care.

(F) Business Practices Related to Exchange

We proposed in 84 FR 7470 that the subject matter of ''business practices of developers of health IT related to exchanging electronic health information'' should be broadly construed to include developer policies and practices that facilitate the exchange of EHI and developer policies and practices that impact the ability of health IT to exchange health information. We further proposed that the exchange of EHI would encompass the appropriate and timely sharing of EHI.

We proposed that protected communications would include, but would not be limited to:

- The costs charged by a developer for products or services that support the exchange of EHI (*e.g.,* interface costs, API licensing fees and royalties, maintenance and subscription fees, transaction or usage-based costs for exchanging information);

• the timeframes and terms on which developers would or would not enable connections and facilitate exchange with other technologies, individuals, or entities, including other health IT developers, exchanges, and networks;
• the developer's approach to participation in health information exchanges and/or networks;
• the developer's licensing practices and terms as it relates to making available APIs and other aspects of its technology that enable the development and deployment of interoperable products and services; and
• the developer's approach to creating interfaces with third-party products or services, including whether connections are treated as ''one off'' customizations, or whether similar types of connections can be implemented at a reduced cost.

Importantly, we further proposed in 84 FR 7470 that information regarding ''business practices of developers of health IT related to exchanging electronic health information'' would include information about switching costs imposed by a developer, as we are aware that the cost of switching health IT is a significant factor impacting health care providers adopting the most exchange-friendly health IT available.

Comments. One commenter stated that our proposed ''business practices'' is too broadly defined and should relate exclusively to interoperability elements of certified health IT, rather than to products and services that support exchange.

Response. As discussed in the Proposed Rule, we believe the term ''business practices of developers of health IT related to exchanging electronic health information'' should be broadly construed consistent with our interpretation of the Cures Act language regarding the Communications Condition of Certification requirements, but limited to those business practices that relate to the certified health IT as clarified previously in this Condition and Maintenance of Certification section. A wide variety of business practices could impact the exchange of EHI, including developer business strategies, pricing, and even fraudulent behavior. As such, we have finalized in § 170.403(a)(1)(v) our proposal that such business practices include developer policies and practices that impact or facilitate the exchange of EHI. They could also include costs charged by a developer not only specifically for interoperability elements of the certified health IT, but also for any products or services that support the exchange of EHI through the certified health IT. We reiterate that business practices related to exchange could include timeframes and terms on which developers facilitate exchange; the developer's approach to participating in health information exchanges and/or networks; the developer's licensing practices and terms as related to APIs and other interoperable services; and the developer's approach to creating interfaces with third-party services. As proposed in 84 FR 7473, this Communications Condition of Certification requirement will also apply to any communication concerning a Program requirement (*e.g.,* a Condition or Maintenance of Certification requirement) related to the exchange of EHI or the information blocking provision.

Comments. Several commenters had concerns regarding communications about prices and costs, with some commenters asserting that such communications should be protected and some others asserting that developers should be able to restrict communications about prices and costs, including switching costs. Additionally, one commenter had concerns about protecting communications regarding timeframes and terms as well as workarounds and customizations. One commenter also recommended that ONC seek guidance from the Antitrust Division of the FTC regarding economic impacts of regulating health IT developer terms, prices, and timeframes.

Response. We continue to interpret costs, information regarding timeframes and terms, and information about health IT workarounds and customizations as protected communications under the ''Business Practices Related to Exchange'' provision of this condition. We believe that this type of information is frequently relied upon and necessary in order to optimize health IT for the exchange of EHI. We emphasize that the costs charged by a developer for certified health IT or related services that support the exchange of EHI are significant factors that can impact the adoption of interoperable certified health IT and should be protected communications. For example, pricing could include prohibitive costs that prevent or discourage customers from using certified health IT to interact with competing technologies. Likewise, information regarding timeframes and terms is the type of information considered and relied upon in the adoption of interoperable certified health IT and is a protected communication. We have also finalized in § 170.403(a)(1)(vi) that information about certified health IT workarounds and customizations relates to important aspects of how a user has used certified health IT, including how the certified health IT can be used to achieve greater interoperability, and is a protected communication.

In response to the comments recommending that we seek guidance from the FTC, we note that we are not regulating health IT developer terms, prices, and timeframes under this Communications Condition of Certification requirements, and therefore do not need to seek further guidance. Rather, the Communications Condition of Certification requirements would protect communications about health IT developer costs, terms, and timeframes as described above and ensure that such information could be shared. We have finalized the scope of the protected subject area ''business practices of developers of health IT related to exchanging electronic health information'' in § 170.403(a)(1)(v) as proposed.

iii. Meaning of ''Prohibit or Restrict''

The terms ''prohibit'' and ''restrict'' are not defined in the Cures Act, nor in any other relevant statutory provisions. We discussed in the Proposed Rule that communications can be prohibited or restricted through contractual terms or agreements (*e.g.,* non-disclosure agreements or non-disparagement clauses) as well as through conduct, including punitive or retaliatory business practices that are designed to create powerful disincentives to engaging in communications about developers or their health IT. Therefore, we proposed in 84 FR 7470 that the Communications Condition of Certification requirements would not be limited to only formal prohibitions or restrictions (such as by means of contracts or agreements) and would encompass any conduct by a developer that would be likely to restrict a communication or class of communications protected by the Communications Condition of Certification requirements. We explained that the conduct in question must have some nexus to the making of a protected communication or an attempted or contemplated protected communication.

(A) Prohibitions or Restrictions Arising by Way of Contract

We explained in the Proposed Rule that the principal way that health IT developers can control the disclosure of information about their health IT is through contractual prohibitions or restrictions. We noted that there are different ways that contractual prohibitions or restrictions arise. In some instances, a contractual prohibition or restriction will be

expressed, and the precise nature and scope of the prohibition or restriction will be explicit in the contract or agreement. However, we also noted that a contract may also impose prohibitions or restrictions in less precise terms. We stated that a contract does not need to expressly prohibit or restrict a protected communication in order to have the effect of prohibiting or restricting that protected communication. The use of broad or vague language that obfuscates the types of communications that can and cannot be made may be treated as a prohibition or restriction if it has the effect of restricting legitimate communications about health IT.

We stated that restrictions and prohibitions found in contracts used by developers to sell or license their health IT can apply to customers directly and can require that the customer ''flow-down'' obligations to the customer's employees, contractors, and other individuals or entities that use or work with the developer's health IT. We proposed that such contract provisions would not comply with the Communications Condition of Certification requirements and would be treated as prohibiting or restricting protected communications. We noted that prohibitions or restrictions on communications can also be found in separate nondisclosure agreements (NDAs) that developers require their customers—and in some instances the users of the health IT or third-party contractors—to enter into in order to receive or access the health IT. We proposed that such agreements are covered by the Communications Condition of Certification requirements.

We did not receive comments on this specific aspect of the Proposed Rule and have finalized our interpretation proposed in FR 7471 regarding prohibitions or restrictions arising by way of contract as stated above.

(B) Prohibitions or Restrictions That Arise by Way of Conduct

We proposed in 84 FR 7471 that conduct that has the effect of prohibiting or restricting a protected communication would be subject to the Communications Condition of Certification requirements. We emphasized that the conduct in question must have some nexus to the making of a protected communication or an attempted or contemplated protected communication. As such, developer conduct that was alleged to be intimidating, or health IT performance that was perceived to be substandard, would not, in and of itself, implicate the Communications Condition of Certification requirements unless there was some nexus between the conduct or performance issue and the making of (or attempting or threatening to make) a protected communication.

We did not receive comments on this specific aspect of the Proposed Rule and have finalized our interpretation proposed in 84 FR 7471 regarding prohibitions or restrictions arising by way of conduct as stated above.

iv. Communications With Unqualified Protection

We proposed in 84 FR 7472 a narrow class of communications—consisting of five specific types of communications—that would receive unqualified protection from developer prohibitions or restrictions. With respect to communications with unqualified protection, a developer would be prohibited from imposing any prohibition or restriction. We proposed that this narrow class of communications warrants unqualified protection because of the strength of the public policy interest being advanced by the class of the communication and/or the sensitivity with which the identified recipient treats, and implements safeguards to protect the confidentiality and security of, the information received. We stated that a developer that imposes a prohibition or restriction on a communication with unqualified protection would fail the first part of the two-part test for allowable prohibitions or restrictions, and as such would contravene the Communications Condition of Certification requirements.

Comments. One commenter recommended adding language specifying the types of entities that can receive communications with unqualified protection, noting that such specificity would help ensure that these communications go to the appropriate entities so that they can be addressed quickly. The commenter recommended that provisions around reporting to government entities should be limited to United States government entities.

Response. We do not believe it is necessary to further specify the types of entities that can receive communications with unqualified protection. We intend for this protection to cover a wide variety of organizations, and further specifying the types of entities that can receive such communications, such as limiting communication to only United States government entities, would unnecessarily limit the scope of this protection and could be counter to the public policy interest to advance the ability of these communications to occur unencumbered. We have finalized in § 170.403(a)(2)(i) our proposal to prohibit developers from imposing any prohibition or restriction on communications that fall into a narrow class of communications—consisting of the five specific types of communications described below—that would receive unqualified protection.

(A) Disclosures Required by Law

We proposed in 84 FR 7472 that where a communication relates to subject areas enumerated in proposed § 170.403(a)(1) and there are Federal, State, or local laws that would require the disclosure of information related to health IT, developers must not prohibit or restrict in any way protected communications made in compliance with those laws. We noted that we expect most health IT contracts would allow for, or not prohibit or restrict, any communication or disclosure that is required by law, such as responding to a court or Congressional subpoena, or a valid warrant presented by law enforcement. We further proposed that if required by law, a potential communicator should not have to delay any protected communication under the Communications Condition of Certification requirements.

We did not receive comments on this aspect of the Proposed Rule and have finalized in § 170.403(a)(2)(i)(A) our approach regarding disclosures required by law as proposed.

(B) Communicating Information About Adverse Events, Hazards, and Other Unsafe Conditions to Government Agencies, Health Care Accreditation Organizations, and Patient Safety Organizations

We proposed in 84 FR 7472 that there is an overwhelming interest in ensuring that all communications about health IT that are necessary to identify patient safety risks, and to make health IT safer, not be encumbered by prohibitions or restrictions imposed by health IT developers that may affect the extent or timeliness of communications. In addition to the public policy interest in promoting uninhibited communications about health IT safety, we proposed that the recognized communication channels for adverse events, hazards, and unsafe conditions provide protections that help ensure that any disclosures made are appropriately handled and kept confidential and secure. We proposed that the class of recipients to which the information can be communicated under this specific category of communications given unqualified protection should provide health IT developers with comfort that there is little risk of such communications prejudicing the developer's IP rights.

We sought comment on whether the unqualified protection afforded to communications made to a patient safety organization about adverse events, hazards, and other unsafe conditions should be limited. Specifically, we sought comment on whether the unqualified protection should be limited by the nature of the patient safety organization to which a communication can be made, or the nature of the communication that can made.

Comments. Several commenters stated that ONC should not place any limits on the unqualified protection afforded to communications made to patient safety organizations about adverse events, hazards, and other unsafe conditions.

Response. We have finalized in § 170.403(a)(2)(i)(B) as proposed regarding the unqualified protection afforded to communications about adverse events, hazards, and other unsafe conditions that are made to government agencies, health care accreditation organizations, and patient safety organizations. Additionally, we placed no limits or qualifiers on such communications, including those communications made to patient safety organizations.

(C) Communicating Information About Cybersecurity Threats and Incidents to Government Agencies

We proposed in 84 FR 7472 that if health IT developers were to impose prohibitions or restrictions on the ability of any person or entity to communicate information about cybersecurity threats and incidents to government agencies, such conduct would not comply with the Communications Condition of Certification requirements.

We sought comment on whether it would be reasonable to permit health IT developers to impose limited restrictions on communications about security issues to safeguard the confidentiality, integrity, and security of EHI. In the Proposed Rule, we asked if, for example, health IT developers should be permitted to require that health IT users notify the developer about the existence of a security vulnerability prior to, or simultaneously with, any communication about the issue to a government agency.

Comments. Some commenters stated that users should never be required to notify the developer when reporting cybersecurity issues, as this would impose a burden on the user and a potential barrier to reporting. Other commenters recommended that developers should be allowed to require users to notify them simultaneously or prior to reporting such incidents, with one comment noting that this would enable developers to better address and respond to security threats prior to the knowledge of a threat becoming widespread. Some commenters recommended that ONC make it a violation for developers to not share cybersecurity vulnerabilities with providers, and that ONC work with DHS to mitigate issues around sharing such vulnerabilities. One commenter recommended changing the wording regarding communicating cybersecurity and security risks to include known vulnerabilities and health IT defects.

Response. We strongly encourage users of health IT to notify developers as soon as possible when reporting security incidents and issues. However, it would not be appropriate to require this practice, which would impose an obligation on users of health IT that is outside the scope of this rule. It would also be outside the scope of this condition to implement additional requirements for developers regarding the sharing of cybersecurity vulnerabilities with health care providers. To be clear, we expect developers with Health IT Modules certified under the Program to share information about cybersecurity vulnerabilities with health care providers and other affected users as soon as feasible, so that these affected users can take appropriate steps to mitigate the impact of these vulnerabilities on the security of EHI and other PII in the users' systems. Thus, we have finalized the Communications Condition of Certification requirements in § 170.403(a)(2)(i)(C) as proposed. Developers must not place restrictions on communications receiving unqualified protections. We also clarify that known vulnerabilities and health IT defects would likely be considered types of ''adverse events, hazards, and other unsafe conditions'' that would receive ''unqualified protection,'' and thus a developer would not be able to restrict a health IT user from communicating about such issues in communications receiving unqualified protections under the Communications Condition of Certification requirements (see § 170.403(a)(2)(i) as finalized). However, we note that in communications not receiving unqualified protection under the Communications Condition of Certification requirements, a security vulnerability that is not already public knowledge would be considered a non-user-facing aspect of health IT, about which developers are permitted to restrict communications (see § 170.403(a)(2)(ii)(B) as finalized). Last, we note that we will continue to work with our Federal partners to mitigate and address cybersecurity threats and incidents.

(D) Communicating Information About Information Blocking and Other Unlawful Practices to a Government Agency

We proposed in 84 FR 7473 that the public benefit associated with the communication of information to government agencies on information blocking, or any other unlawful practice, outweighs any concerns developers might have about the disclosure of information about their health IT. We noted that reporting information blocking, as well as other unlawful practices, to a government agency would not cause an undue threat to a health IT developer's IP.

Comments. We received several comments regarding the lack of whistleblower protections in the Proposed Rule for individuals who report information blocking or other issues regarding certified health IT. These comments discussed the need to provide for whistleblower type protections for individuals who highlight information blocking practices, as well as to identify them to the appropriate authorities so that the individual is not subject to retaliatory action by the actor identified by the whistleblower.

Response. We appreciate these comments and agree that it is extremely important for individuals to be able to report information blocking and violations of other Conditions of Certification without fear of retaliation. We note that the Communications Condition of Certification requirements provide protections against retaliation and intimidation by developers with respect to protected communications. We discussed in the Proposed Rule that the Communications Condition of Certification requirements cover communications that are prohibited or restricted through contractual terms or agreements (*e.g.,* non-disclosure agreements, non-disparagement clauses) between the health IT developer, or offeror of health IT, and the communicator, as well as through conduct, including punitive or retaliatory business practices that are designed to create powerful disincentives to engaging in communications about developers or their health IT. We clarify, however, that merely filing a lawsuit against the communicator regarding the making of

a communication would not be considered intimidating conduct in violation of this Condition. Any such determination would necessarily be fact-specific, and the health IT developer's lawsuit would have to be designed to intimidate a communicator in order to prevent or discourage that communicator from making a protected communication, rather than be designed to pursue a legitimate legal interest. We believe that the proposed broad interpretation of ''prohibit'' and ''restrict'' is appropriate given the intention of the Cures Act, which placed no limitations on the protection of communications about the protected subject areas. We finalized this interpretation of ''prohibit'' and ''restrict'' proposed in 84 FR 7470 and believe that the interpretation would provide significant protections for whistleblowers from retaliatory actions. Thus, retaliatory actions by a developer against a whistleblower would be in violation of this provision. We also emphasize that conduct by a developer that may be perceived as intimidating or punitive would not implicate the Communications Condition of Certification requirements unless that conduct was specifically designed to influence the making of a protected communication. In other words, punitive actions must have a nexus to the making of a protected communication, such as retaliation for reporting of information blocking, in order to violate the Communications Condition of Certification requirements in § 170.403(a)(1). Last, we refer readers to the discussion of ''complaints'' under the information blocking section of this final rule, which details the confidentiality provided to information blocking complaints and complainants.

We have finalized the Communications Condition of Certification requirements in § 170.403(a)(2)(i)(D) as proposed.

(E) Communicating Information About a Health IT Developer's Failure To Comply With a Condition of Certification or Other Program Requirement

We proposed in 84 FR 7473 that the benefits to the public and to users of health IT of communicating information about a health IT developer's failure to comply with a Condition of Certification requirement or other Program requirement (45 CFR part 170) justify prohibiting developers of health IT from placing any restrictions on such protected communications. We explained that information regarding the failure of certified health IT to meet any Condition of Certification requirement or other Program requirement is vital to the effective performance and integrity of the Program. Moreover, the failure of a certified health IT to meet such requirements could impact the performance of the certified health IT with respect to usability, safety, and interoperability. We stated that it is important to enable unencumbered reporting of such information and that such reporting is essential to the transparency that section 4002 of the Cures Act seeks to ensure. While the current procedures for reporting issues with certified health IT encourage providers to contact developers in the first instance to address certification issues, we noted that users of health IT should not hesitate to contact ONC-Authorized Certification Bodies (ONC–ACBs), or ONC itself, if the developer does not provide an appropriate response, or the matter is of a nature that should be immediately reported to an ONC–ACB or to ONC.

We did not receive any comments on this aspect of the Proposed Rule. In consideration of the above, we have finalized this provision in § 170.403(a)(2)(i)(E) as proposed.

v. Permitted Prohibitions and Restrictions

We proposed in 84 FR 7473 that, except for communications with unqualified protection (§ 170.403(a)(2)(i)), health IT developers would be permitted to impose certain narrow prohibitions and restrictions on communications. Specifically, we proposed that, with the exception of communications with unqualified protection, developers would be permitted to prohibit or restrict the following communications, subject to certain conditions:

- Communications of their own employees;
- Disclosure of non-user-facing aspects of the software;
- Certain communications that would infringe the developer's or another person's IP rights;
- Publication of screenshots in narrow circumstances; and
- Communications of information that a person or entity knows only because of their participation in developer-led health IT development and testing.

The proposed Communications Condition of Certification requirements delineated the circumstances under which these types of prohibitions and restrictions would be permitted, including certain associated conditions that developers would be required to meet. We emphasized that any prohibition or restriction not expressly permitted would violate the Communications Condition of Certification requirements. Additionally, we proposed that it would be the developer's burden to demonstrate to the satisfaction of ONC that the developer met all associated requirements. Further, as an additional safeguard, we proposed that where a developer sought to avail itself of one of the permitted types of prohibitions or restrictions, the developer must ensure that potential communicators are clearly and explicitly notified about the information and material that can be communicated, and that which cannot. We proposed this would mean that the language of health IT contracts must be precise and specific. We stressed that contractual provisions or public statements that support a permitted prohibition or restriction on communication should be specific about the rights and obligations of the potential communicator. We explained that contract terms that are vague and cannot be readily understood by a reasonable health IT customer would not benefit from the qualifications to this Condition of Certification requirement as outlined in the Proposed Rule and below.

(A) Developer Employees and Contractors

We recognized in the Proposed Rule in 84 FR 7473 that health IT developer employees, together with the entities and individuals who are contracted by health IT developers to deliver products and/or services (such as consultants), may be exposed to highly sensitive, proprietary, and valuable information in the course of performing their duties. We also stated that we recognize that an employer should have the ability to determine how and when the organization communicates information to the public, and that employees owe confidentiality obligations to their employers. We noted that this would similarly apply to contractors of a developer. We proposed in 84 FR 7473 that on this basis, developers would be permitted to impose prohibitions or restrictions on the communications of employees and contractors to the extent that those communications fall outside of the class of communications with unqualified protection as discussed above.

Comments. One commenter stated that this provision should be clarified and expanded to cover other third parties with whom the health IT developer shares its confidential information, including subcontractors, agents, auditors, suppliers, partners, co-sellers, and re-sellers, as well as

potential relationships for which a contract has not yet been signed in case information is shared during a pre-contract evaluation stage.

Response. We reiterate that ''developer employees and contractors'' include health IT developer employees, together with the entities and individuals who are contracted by health IT developers to deliver health IT and/or services who may be exposed to highly sensitive, proprietary, and valuable information in the course of performing their duties. This functional description of employees and contractors could include subcontractors, agents, auditors, suppliers, partners, co-sellers, and re-sellers, depending on the specific relationship and circumstances. We have finalized the proposed approach to describing employees and contractors in § 170.403(a)(2)(ii)(A). We note that we did not expand this description to include ''potential relationships'' because such an addition would make the description overly broad, and it is unlikely that individuals who are not yet under contract would be exposed to highly sensitive, proprietary, and valuable information.

Comments. We received one comment that self-developers should not be permitted to place restrictions on the communications of their employees who are using their certified health IT.

Response. We agree that self-developers should not be allowed to restrict the communications of users of their certified health IT who are also employees or contractors. We have revised § 170.403(a)(2)(ii)(A) to clarify that the limited prohibitions developers may place on their employees or contractors under the Communications Condition of Certification requirements cannot be placed on users of a self-developer's certified health IT who are also employees or contractors of the self-developer. For example, a large health system with a self-developed EHR cannot restrict a health care provider, who is employed by that health system and using that EHR to provide services, from communicating about the EHR as a user based on the fact that the health care provider is also an employee of the health system. We note that the concept of ''self-developed'' refers to a Complete EHR or Health IT Module designed, created, or modified by an entity that assumed the total costs for testing and certification and that will be the primary user of the health IT (76 FR 1300).

(B) Non-User-Facing Aspects of Health IT

We proposed in 84 FR 7474 that the Communications Condition of Certification requirements would permit health IT developers to impose prohibitions and restrictions on communications to the extent necessary to ensure that communications do not disclose ''non-user-facing aspects of health IT.'' We noted that, like all permitted prohibitions, such prohibitions and restrictions could only be put in place by developers if there is not an unqualified protection that applies. We proposed in 84 FR 7474 that a ''non-user-facing aspect of health IT,'' for the purpose of this Condition of Certification, was an aspect of health IT that is not a ''user-facing aspect of health IT.'' We stated that ''user-facing aspects of health IT'' would include the design concepts and functionality that is readily ascertainable from the health IT's user interface and screen display. We stated that they did not include those parts of the health IT that are not exposed to persons running, using, or observing the operation of the health IT and that are not readily ascertainable from the health IT's user interface and screen display, all of which would be considered ''non-user-facing'' concepts. We proposed in 84 FR 7474 that ''non-user-facing aspects of health IT'' would include source and object code, software documentation, design specifications, flowcharts, and file and data formats. We welcomed comments on whether these and other aspects of health IT should or should not be treated as user-facing.

In the Proposed Rule, we noted that the terminology of ''non-user-facing aspects of health IT'' is not intended to afford only health IT users with specific protections against developer prohibitions or restrictions on communications and is agnostic as to the identity of the communicator.

Comments. Some commenters expressed concern regarding the broad scope of ''user-facing'' and, by extension, the scope of ''non-user-facing.'' One commenter asked for clarification regarding the definition of ''software documentation'' with regards to non-user-facing aspects of health IT and suggested that it applies to documentation that is for back-end components, not documents for normal-end use. Additionally, a couple of comments stated that administrative functions should not be considered user-facing, including one comment that the relevant users for the purpose of the Communications Condition of Certification requirements are ''end'' users, thus the non-user-facing provision should apply only to ''non-end-user-facing'' aspects of health IT. Some commenters emphasized that administrative portions of health IT contain more insight into health IT systems and that administrative functions affect a limited number of users and are not the types of communications or subject matters contemplated by the Cures Act. One commenter stated that algorithms should be considered non-user-facing. Another commenter stated that ONC should clarify the status of diagrams and flowcharts.

Response. We do not see a necessary or appreciable distinction between ''users'' and ''end users,'' as we have focused on the aspects of the health IT that are and are not subject to protected communications under this Condition of Certification. We also believe that there could be unintended consequences with the term ''end user,'' such as limiting certain users not specified under the ''*permitted prohibitions and restrictions*'' (*e.g.,* developer employees and contractors) from making protected communications. Therefore, we believe ''non-user-facing'' best reflects the scope of the communications about health IT we seek to capture with these terms.

We reiterate that ''non-user-facing aspects of health IT'' comprise those aspects of the health IT that are not readily apparent to someone interacting with the health IT as a user of the health IT, including source and object code, certain software documentation, design specifications, flowcharts, and file and data formats. We clarify that ''non-user-facing aspects of health IT'' would also include underlying software that is utilized by the health IT in the background and not directly by a user of the health IT. For example, the programming instructions for proprietary APIs would be considered non-user-facing because they are not readily apparent to the individual users of the health IT. In addition, underlying database software that connects to health IT and is used to store data would be considered a non-user-facing aspect of health IT because it serves data to the health IT, not directly to a user.

We further clarify that algorithms would be considered ''non-user-facing aspects of health IT'' as they are not readily apparent to persons using health IT for the purpose for which it was purchased or obtained. Thus, communications regarding algorithms (*e.g.,* mathematical methods and logic) could be restricted or prohibited, while communications regarding the output of the algorithm and how it is displayed in

a health IT system could not be restricted as ''non-user-facing aspects of health IT.'' Similarly, we also clarify that certain ''software documentation'' that would be considered to be a non-user-facing aspect of health IT would include documentation for back-end components, again because it is not readily apparent to persons using health IT.

Whether or not a communication would be considered a ''non-user-facing aspects of health IT'' would be based on whether the communication involved aspects of health IT that would be evident to anyone running, using, or observing the operation of the health IT for the purpose for which it was purchased or obtained. With respect to administrative functions, where the communication at issue relates to aspects of the health IT that are not observable by users of the health IT, it would be considered ''non-user-facing'' for the purpose of this Condition of Certification requirement. For example, a communication regarding an input process delay experienced by an administrator of health IT that was caused by the underlying database software could be restricted if the communication discussed the underlying database software, which would be considered a non-user-facing aspect of the health IT. However, if the communication discussed the user screens and the delay experienced by the administrator, which would be considered user-facing aspects of health IT, it could not be restricted. Similarly, as long as diagrams or flowcharts do not include aspects of the health IT that are observable by users of the health IT, as described above, they would be considered communications about non-user-facing aspects of health IT.

We have finalized in § 170.403(a)(2)(ii)(B) our proposed approach to the scope of ''non-user-facing aspects of health IT'' with the clarification provided above regarding scope.

(C) Intellectual Property

We proposed in 84 FR 7474 that the Communications Condition of Certification requirements are not intended to operate as a de facto license for health IT users and others to act in a way that might infringe the legitimate IP rights of health IT developers or other persons. Indeed, we proposed in 84 FR 7474 that health IT developers are permitted to prohibit or restrict certain communications that would infringe their IP rights so long as the communication in question is not a communication with unqualified protection. We proposed in 84 FR 7474 that any prohibition or restriction imposed by a developer must be no broader than legally permissible and reasonably necessary to protect the developer's legitimate IP interests. We also proposed in 84 FR 7474 that health IT developers are not permitted to prohibit or restrict, or purport to prohibit or restrict, communications that would be a ''fair use'' of any copyright work comprised in the developer's health IT.[86] ''Fair use'' is a legal doctrine that allows for the unlicensed use of copyright material in certain circumstances, which could include circumstances involving criticism, commentary, news reporting, and research.[87]

Comments. One commenter stated that fair use should not override other IP protections and stressed that relying on fair use could lead to uncertainty because it is determined on a case-by-case basis. Another commenter stated that because the fair use doctrine can be difficult to implement and can lead to uncertain results, ONC should expand the list of communications that would be explicitly protected as fair use to include news reporting, criticism, parody, and communications for educational purposes.

Response. We disagree with commenters and believe that relying on the ''fair use'' doctrine for determining when a screenshot or other communication cannot be restricted should be allowed under the Communications Condition of Certification requirements. This doctrine presents a framework of analysis that is well-developed in case law and thus can be interpreted and applied consistently, even when materials are not formally copyrighted. Accordingly, we are retaining the concept of ''fair use'' in the final provision in § 170.403(a)(2)(ii)(C). Developers and ONC will apply a fair use test to copyrighted materials and, by analogy, to materials that could be copyrighted, to determine whether developers may prohibit a communication that would infringe on IP rights.

The Communication Condition of Certification requirements relate only to protected communications, thus developers can place restrictions on communications about subject matters outside of the protected communications categories without implicating the Communications Condition of Certification requirements. Also, as discussed earlier regarding developer employees and contractors in § 170.403(a)(2)(ii)(A), developers may restrict communications by their employees, contractors, and consultants without implicating the Communications Condition of Certification requirements, provided they do not restrict communications with unqualified protections. Further, as described earlier regarding non-user-facing aspects of certified health IT in § 170.403(a)(2)(ii)(B), developers may restrict communications that disclose non-user-facing aspects of the developer's certified health IT, provided they do not restrict communications with unqualified protections. We clarified in that section that screenshots or videos depicting source code would be considered communications of non-user-facing aspects of health IT and could be restricted under the Communications Condition of Certification requirements as long as they did not receive unqualified protection. We also clarify that this Condition does not prohibit health IT developers from enforcing their IP rights and that a lawsuit filed by a health IT developer in response to a protected communication regarding infringement of IP rights would not automatically be considered intimidation or retaliation in violation of this Condition.

As discussed later in the pre-market testing and development section in § 170.403(a)(2)(ii)(E), developers can place restrictions on communications related to pre-market health IT development and testing activities, which could include IP protections, provided they do not restrict communications with unqualified protections. Combined, these avenues allow for protecting IP in ways that would not implicate the Communications Condition of Certification requirements, thereby allowing developers to take a number of actions to protect and safeguard IP in their certified health IT.

Comments. Several commenters requested clarity regarding how the proposed protections for IP would work. One commenter stated that the rule must allow developers to protect legitimate IP interests and asked for clarity on how ONC would determine whether a developer's restriction on the communication of a screenshot was an allowable protection of trade secrets or an impermissible restriction of protected communications. Several other commenters, who generally supported the Communications Condition of Certification requirements, requested clarification regarding how a

[86] See 17 U.S.C. 107 (setting forth the four factors required to evaluate a question of fair use under the statutory framework).

[87] See *https://www.copyright.gov/fair-use/more-info.html* for more information on fair use.

prohibition on communications that is designed to protect IP can be applied. Some commenters requested examples of the types of communications that can be restricted on the basis of IP and clarification of the standard ONC will use to determine what prohibitions are permissible.

Response. We have finalized an approach in § 170.403(a)(2)(ii)(C) that allows developers to prohibit or restrict communications that involve the use or disclosure of intellectual property existing in the developer's health IT (including third-party intellectual property), provided that any prohibition or restriction imposed by a developer must be no broader than necessary to protect the developer's legitimate intellectual property interests and consistent with all other requirements under the ''permitted prohibitions and restrictions'' (§ 170.403(a)(2)(ii)) of this section. As discussed above, a restriction or prohibition would be deemed broader than necessary and inconsistent with the ''permitted prohibitions and restrictions'' (§ 170.403(a)(2)(ii)) if it would restrict or preclude a public display of a portion of a work subject to copyright protection (without regard to whether the copyright is registered) that would reasonably constitute a ''fair use'' of that work.

Examples of the types of communications that could be restricted under the Communications Condition of Certification requirements might include a blog post describing a customization of a developer's health IT that includes the source code of the developer's health IT or a written review of an analytical feature of the developer's health IT that reveals the algorithms used. However, as mentioned above, the restriction must be no broader than necessary to protect the developer's legitimate IP interests, thus only the infringing portions of the communications could be restricted.

Comments. One commenter recommended that a health IT developer must demonstrate that a communication was specifically designed to copy or steal a developer's IP in order for the developer to be allowed to prohibit the communication as an infringement on their IP rights.

Response. We appreciate this comment, but decline to require that a developer demonstrate that a communication was designed to copy or steal IP in order for the developer to restrict the communication as one that would infringe on IP rights. We believe that the revised approach discussed above provides appropriate balance between protecting IP rights and enabling protected communications and do not believe that an ''intent'' element would be necessary. We have finalized the proposals regarding IP in § 170.403(a)(2)(ii)(C), as amended above.

(D) Faithful Reproductions of Health IT Screenshots

We proposed in 84 FR 7475 that health IT developers generally would not be permitted to prohibit or restrict communications that disclose screenshots of the developer's health IT. We proposed that the reproduction of screenshots in connection with the making of a communication protected by this Condition of Certification would ordinarily represent a ''fair use'' of any copyright subsisting in the screen display, and developers should not impose prohibitions or restrictions that would limit that fair use. Notwithstanding this, we proposed that health IT developers would be allowed to place certain restrictions of the disclosure of screenshots as specified in proposed § 170.403(a)(2)(ii)(D).

With respect to the limited allowable restrictions on screenshots, we proposed in 84 FR 7475 that developers would be permitted to prevent communicators from altering screenshots, other than to annotate the screenshot or to resize it for the purpose of publication. We also proposed that health IT developers could impose restrictions on the disclosure of a screenshot on the basis that it would infringe third-party IP rights (on their behalf or as required by license). However, to take advantage of this exception, we proposed in 84 FR 7475 that the developer would need to first put all potential communicators on sufficient written notice of those parts of the screen display that contain IP and cannot be communicated, and would still need to allow communicators to communicate redacted versions of screenshots that do not reproduce those parts. Finally, we proposed in 84 FR 7475 that it would be reasonable for developers to impose restrictions on the communication of screenshots that contain PHI, provided that developers permit the communication of screenshots that have been redacted to conceal PHI, or where the relevant individual's consent or authorization had been obtained.

We welcomed comments on whether an appropriate balance had been struck between protecting legitimate IP rights of developers and ensuring that health IT customers, users, researchers, and other stakeholders who use and work with health IT can openly discuss and share their experiences and other relevant information about the performance of health IT.

Comments. A large number of commenters, particularly health care providers, supported our proposals regarding the communication of screenshots, with several stressing how helpful screenshots are when communicating usability and safety issues with health IT. One commenter noted that communication of screenshots can help different health care systems understand whether a proposed implementation of an EHR has introduced safety-related challenges at other locations, or help identify solutions to common problems, such as usability challenges. One other commenter stated that there is nothing novel displayed in health IT screenshots that would need to be protected.

Response. We appreciate the many positive comments on our proposals regarding screenshots.

Comments. Commenters stated that the scope of protected communications as proposed should exclude disclosure of the health IT itself, such as through screenshots. The commenter stressed that the Cures Act required that health IT developers not restrict communications about the certified health IT with respect to specific topic areas, while the Proposed Rule expands that restriction to include communication of the health IT itself. One commenter noted that the Cures Act does not mention screenshots and they should not be included in the Communications Condition of Certification requirements.

Response. The Cures Act amended title XXX of the PHSA to establish this condition of certification, which applies to ''health information technology.'' Title XXX of the PHSA was previously added by the HITECH Act, which included the definition of ''health information technology.'' Section 3000(5) of the PHSA defines health information technology to mean hardware, software, integrated technologies or related licenses, IP, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. We emphasize both that this definition includes IP associated with the health information technology and that it applies to this condition of certification as this condition references communications regarding health information technology. We have also adopted this definition in § 170.102.

We disagree with the commenters' interpretation of the statutory provision. The statutory provision focuses on ''communications'' regarding

enumerated aspects of the health IT. Communications are not defined nor limited in the Cures Act, and we proposed to broadly define them. Verbal, written, and visual, as well other types of communications, are all covered under the Cures Act. A screenshot is a copy/picture of the user interface of the health IT, or a ''visual communication'' that is protected under this condition of certification. We have specifically defined ''communication'' for this section in § 170.403(c) to mean any communication, irrespective of the form or medium. The term includes visual communications, such as screenshots and video.

As we emphasized in the Proposed Rule in 84 FR 7475, the sharing of screenshots (with accompanying annotation and/or explanatory prose) is often a critical form of communication of issues with health IT related to—for example—usability, user experience, interoperability, security, or the way the technology is used. We believe screenshots are uniquely helpful as a form of visual communication that can non-verbally illustrate the ''user's experiences when using the health information technology'' and the ''manner in which a user of the health information technology has used such technology'' as they relate intrinsically to both subject areas and capture those user experiences immediately and directly. Further, enabling screenshot sharing can allow for clearer, more immediate, and more precise communication on these pertinent issues, potentially helping a health system avoid costly, or even deadly, complications when implementing health IT. It is also our understanding that screenshots are often the only recourse a user in a network enterprise system has for capturing, documenting, and explaining their concerns. We clarify, however, that the sharing of a screenshot alone would not be considered a protected communication as it would need to be accompanied by an explanation of the issues or aspects of the health IT that the screenshot is meant to communicate or illustrate.

Considering the value of communicating significant issues regarding health IT through screenshots, we have finalized our proposal to include screenshots as a protected communications under the Cures Act. However, as discussed in responses to other comments below, we have revised our final policy in multiple ways.

Comments. One commenter recommended that screenshots should be defined broadly to include video and other media that can be helpful in demonstrating challenges with EHRs.

Response. We agree with the recommendation that protections afforded to screenshots should extend to video. We clarify that, like screenshots, video is considered a form of visual communication. A video of a computer screen while a software program is in operation would capture the user experience of interacting with that program and essentially would show a number of screenshots from that program in rapid succession. We emphasize that video, similarly to individual screenshots, is a critical form of communication of issues with the health IT, including issues related to usability, user experience, interoperability, security, or the way the technology is used.

As with screenshots, video is particularly useful in communicating a user's experience with health IT and the manner in which the user has used health IT. This is especially the case when issues of a temporal nature are involved. For example, video would be essential for illustrating a latency issue experienced during drug ordering that could not be communicated through screenshots or other forms of communication. Video also could be critical to demonstrating an issue with a clinical decision support alert that is designed to appropriately and timely notify the provider of a patient matter but fails to do so.

Comments. Several commenters expressed concern regarding how a developer's IP may be impacted by the proposed Communications Condition of Certification requirements. Several commenters stated that the Proposed Rule goes beyond protecting communications for the purposes of patient safety and system improvement and would enable or require inappropriate sharing and disclosure of IP, potentially creating security risks, increased IP theft, and harming innovation and the marketplace for health IT. Several commenters stated that trade secrets, patent protections, and protections for confidential and proprietary information were not addressed or considered appropriately in the Proposed Rule, and that as a result it would be possible for bad actors to create pirated health IT based on the disclosure of screenshots and similar communications. Commenters stated that developers of health IT have successfully used licensing and nondisclosure agreements that apply to user-facing aspects of the technology to maintain the trade secret status of their health IT and that the Proposed Rule would impact their ability to do so and remain competitive in the market.

Response. We appreciate the comments regarding how a developer's IP may be impacted by the Communications Condition of Certification requirements. As discussed earlier in this section, participation in the Program is voluntary; and developers have the option to agree to the terms we have offered or to choose not to participate in the Program. However, we recognize the need to properly balance the protection of a developer's IP with the need to advance visual communications (*e.g.,* screenshot and video communications) under the Communications Condition and Maintenance of Certification requirements, which we believe is critical to addressing—among other things—the usability, interoperability, and security of health IT. As discussed throughout this section and in section (C) above, we believe that we have properly considered and addressed health IT developers' IP rights in this final rule in § 170.403(a)(2)(ii)(C) by amending the proposed regulation as described above.

We emphasize that the communication of screenshots is essential to protect public health and safety and that our final policies take a measured approach to responding to and addressing a real and substantial threat to public health and safety. The communication of screenshots enables providers, researchers, and others to identify safety concerns, share their experiences with the health IT, learn from the problems, and then repair dangers that could otherwise cause serious harm to patients. Our position is informed both by years of experience regulating health IT and overwhelming research and academia, which is discussed below.

For instance, a study published in 2018 was performed to better characterize accessibility to EHRs among informatics professionals in various roles, settings, and organizations across the United States and internationally.[88] To quantify the limitations on EHR access and publication rights, the researchers conducted a survey of informatics professionals from a broad spectrum of roles including practicing clinicians, researchers, administrators, and members of industry. The results were analyzed and levels of EHR access were stratified by role, organizational affiliation, geographic region, EHR type, and restrictions with regard to

[88] Khairat, S, et al. 2018 Assessing the Status Quo of EHR Accessibility, Usability, and Knowledge Dissemination. eGEMs (Generating Evidence & Methods to improve patient outcomes), pp. 1–11, *https://doi.org/10.5334/egems.228.*

publishing results of usability testing, including screenshots. Among faculty members and researchers, 72 percent could access the EHR for usability and/or research purposes, but, of those, fewer than 1 in 3 could freely publish screenshots with results of usability testing and half could not publish such data at all. Across users from all roles, only 21 percent reported the ability to publish screenshots freely without restrictions.[89]

The study explained that the patient safety implications of EHR publication censorship and restricted EHR access are multiple. First, limiting institutions from sharing usability research findings can prevent the correction of known problems. Second, without public dissemination, poor design practices will propagate to future iterations of existing vendor systems. Finally, research efforts are directed away from real-world usability problems at a time when EHR systems have become widely deployed and when an urgency exists to accelerate usability testing. The study referenced the 2011 Institute of Medicine report (as discussed in the Proposed Rule and in additional detail below), which identified contractual restrictions as a barrier to knowledge regarding patient safety risks related to health IT.[90]

The study emphasized that the result of this level of censorship is that a vast majority of scientists researching EHR usability are either prevented from publishing screenshots altogether or must first obtain vendor permission, thus impeding the free dialogue necessary in communities of investigation.[91] The study argued that: (1) Lack of EHR access makes many critical EHR usability research activities impossible to conduct, and (2) publication censorship, especially regarding screenshots, means that even those usability studies which can be conducted may not have the impact they otherwise would. As a consequence, innovation can be stifled. As such, one of the recommendations made by the researchers was that there should be a mandate that screenshots and images from EHR systems be freely publishable without restrictions from copyright or trade secret constraints.[92]

In the report by the Institute of Medicine that was noted above, entitled Health IT and Patient Safety: Building Safer Systems for Better Care,[93] the Committee on Patient Safety and Health Information Technology (Committee) explained that a significant impediment to gathering safety data is contractual barriers (*e.g.,* nondisclosure, confidentiality clauses) that can prevent users from sharing information about health IT–related adverse events. They further explained that such barriers limit users' abilities to share knowledge of risk-prone user interfaces, for instance through screenshots and descriptions of potentially unsafe processes. In addition, some vendors include language in their sales contracts and escape responsibility for errors or defects in their software (*i.e.,* ''hold-harmless clauses''). The Committee concluded that these types of contractual restrictions limit transparency, which significantly contributes to the gaps in knowledge of health IT–related patient safety risks. Further, these barriers to generating evidence pose unacceptable risks to safety.[94] Based on these findings, the committee recommended that the Secretary of HHS should ensure insofar as possible that health IT vendors support the free exchange of information about health IT experiences and issues and not prohibit sharing of such information, including details (*e.g.,* screenshots) relating to patient safety.[95]

Recently, the U.S. Food and Drug Administration (FDA) funded Brigham and Women's Hospital Center for Patient Safety Research and Practice to conduct an exploration of computerized prescriber order entry (CPOE)-related potential for errors in prescribing, particularly as these relate to drug name displays, and ordering and workflow design issues. The project investigated ways to better identify, understand, and prevent electronic ordering errors in the future.[96] However, the researchers noted that one large vendor would not grant permissions to share requested screenshots necessary for the study. This refusal ran counter to both the FDA's task order initial precondition as well as multiple high-level panels' health IT safety recommendations. The FDA emphasized that it is hard to justify from a safety viewpoint why such permission was withheld, despite the vendors' proprietary concerns. FDA explained that identifying, preventing, and learning from errors and improving prescribing safety should be a priority and should take precedence over commercial considerations (and to the extent correctable problems can be identified, likely would result in an improved commercial CPOE product). In cases where the FDA sought to illustrate problems in the system, they drew generic screenshots to illustrate the issue in question.[97]

Among their recommendations, the FDA recommended that vendors be required to share screenshots and error reports. The FDA emphasized that vendors should be required to permit the sharing of screenshots and information with the FDA and other institutions regarding other CPOE system issues of concern or that pose risk for errors. They stressed that the practice of prohibiting such sharing via copyright must be eliminated. Further, the FDA recommended that vendors should be required to disclose errors reported to them or errors identified in their products, analogous to the requirement that drug manufacturers report significant adverse drug effects.[98]

One of the co-authors of the FDA study recently wrote a law review article that discussed the significance of screenshots.[99] The author noted that the results of the FDA study were remarkable and remarkably distressing, as they identified and took screenshots of over fifty different dangers in the health IT. He expressed frustration that it took up to two years of additional discussions with the vendors to get permission to share the screenshots publicly, and that even after these extended discussions, one vendor—''with more than a lion's share of the market''—prevented the study from displaying the screenshots, some of which were clearly dangerous or deadly. He explained that they had worked around that limitation by substituting the one vendor's screens with parallel screens taken from Harvard's homegrown, but by then superannuated, EHR. The author emphasized that those images and screenshots illustrated over fifty EHR risks caused by dangerous and confusing EHR interfaces. The author also emphasized that the study could have been even more helpful in identifying these risks if the FDA had been able to present the findings when first available, rather than haggle for a year or two, and if the study was able

[89] Id. at 1.

[90] Id. at 2.

[91] Id. at 7.

[92] Id. at 8.

[93] Institute of Medicine 2012. Health IT and Patient Safety: Building Safer Systems for Better Care. Washington, DC: The National Academies Press, *https://doi.org/10.17226/13269.*

[94] Id. at 3.

[95] Id. at 7.

[96] U.S. Food & Drug Admin., UCM477419, Computerized Prescriber Order Entry Medication Safety: Uncovering and Learning from Issues and Errors, *https://www.fda.gov/downloads/Drugs/DrugSafety/MedicationErrors/UCM477419.pdf.*

[97] Id. at 44.

[98] Id. at 52.

[99] Ross Koppel, Uses of the Legal System That Attenuate Patient Safety, 68 DePaul L. Rev. (2019) Available at: *https://via.library.depaul.edu/law-review/vol68/iss2/6.*

to include all of the full images from each system they studied.[100]

Comments. A commenter recommended that ONC draw a distinction around purpose of use in relation to the fair use of screenshots and require that the discloser of a screenshot be responsible for ensuring the appropriateness of that purpose.

Response. As discussed under section (C) above we have retained the concept of ''fair use'' as it applies to all health IT developer intellectual property covered under ''permitted prohibitions and restrictions'' (§ 170.403(a)(2)(ii)). As discussed throughout this section, we have placed certain restrictions on the sharing of screenshots responsive to the commenter.

Comments. One commenter urged ONC to revise the proposed approach to screenshots by adopting a process that would allow developers to review and approve screenshots for publication for specific purposes, such as communications about safety and usability.

Response. A pre-approval process could create potential or perceived barriers to communications and thus could discourage or delay the making of protected communications that are vital to patient safety or other important issues regarding certified health IT. For example, a user might be less willing to go through the process, the time the process takes could undermine the conveyance of the communications, and the objections raised during the process may not be valid or amenable to all parties.

Comments. Several commenters had concerns regarding the volume of screenshots that could be shared under our proposal and potential harms that could occur. One commenter emphasized that sharing of screenshots could disclose information about how health IT works, including algorithms and workflows, and enable creation of duplicate software and theft of valuable IP. One commenter suggested that if a user of health IT published hundreds of screenshots of the health IT, a bad actor could theoretically deduce trade secrets based on the screenshots. Several additional commenters were also concerned that the Proposed Rule could allow communication of an unlimited number of screenshots of certified health IT, and one commenter suggested revising the proposed approach to include limiting sharing of screenshots to a reasonable number, such as seven.

Response. We appreciate those comments expressing concerns regarding the volume of screenshots that could be shared and the potential negative consequences of allowing screenshots to be shared. In the Proposed Rule in 84 FR 7475, we proposed to allow developers to place limited restrictions on the sharing of screenshots. We stressed in the Proposed Rule that our goal with our proposals concerning screenshots was to enable communications that will address matters such as patient safety, system security vulnerabilities, health IT performance, and usability. Our intent was not to prevent developers from restricting the communication of screenshots for purposes outside the scope of the protected communications detailed in the Cures Act. Additionally, we believe that modern software design best practices uncouple screen design from underlying algorithms, and that limited use of screenshots for safety would not allow reverse engineering of large parts of the underlying code. However, we further emphasize that it was never our intention that screenshots (or other visual communications such as video) depicting source or object codes would be protected communications (*see* the non-user-facing aspects provision of this Condition of Certification), so long as such communications are not communications with unqualified protection.

We reviewed comments that suggested establishing a set numerical limit for the sharing of screenshots. However, we have not finalized a requirement in § 170.403(a)(2)(ii)(D) with a fixed numerical limit because there is no non-arbitrary way to determine what the ''right'' or ''appropriate'' number is in a one-size-fits-all way. That is because the number of screenshots or amount of video that would be needed to communicate about the health IT could vary, from one situation to the next, based on the specific issue and circumstances. For instance, an issue with health IT functionality regarding a particular process that involves the user viewing and making selections on several different screens may necessitate images of all of the screens involved in order to communicate the issue. However, an issue regarding how one value is being displayed in a particular context (*e.g.,* a medication name being truncated) may only necessitate one screenshot in order to communicate the issue. Thus, we believe the best approach is to adopt a qualitative standard that is designed to be sufficiently flexible for the wide range of health IT issues that may arise and the varying visual communications that need to be communicated to demonstrate or display the issue.

We have finalized provisions in § 170.403(a)(2)(ii)(D)(*2*) and (*3*) that allow health IT developers to require persons who communicate screenshots to limit the sharing of screenshots to only the relevant number of screenshots and amount of video that are needed to communicate about the health IT regarding one or more of the six subject areas identified in the Cures Act and detailed in § 170.403(a)(1). Allowing developers to limit the sharing of screenshots to only the relevant number needed to communicate about the health IT—regarding one or more of those six subject areas—places a limitation on the number of screenshots allowed to be shared under the Communications Condition of Certification requirements and requires that the screenshots are related to, and thus necessary in illustrating, the protected communication being made. In practice, this would mean that if a particular safety issue in the health IT could be communicated using three screenshots, the communicator should not share additional screenshots that are irrelevant or only potentially relevant to communicate the safety issue with the health IT. If the communication included additional screenshots that were not necessary to visually communicate about the particular safety issue with the health IT that falls within the usability category, the health IT developer would have grounds to seek redress.

As with screenshots, we wish to be sensitive to concerns regarding protecting IP in health IT and allow developers to appropriately limit video communication in order to protect against harms that could occur due to unlimited sharing. Similar to screenshots, the amount of video that may be necessary to make a protected communication about health IT could vary, depending on the nature of the issue or aspect of the health IT being addressed. For example, a video meant to communicate a delay in order entry would need to be long enough to communicate the significance of the delay, but would not need to include video of the log-in process or other unrelated functionality of the health IT. We have finalized a provision in § 170.403(a)(2)(ii)(D)(*3*) that allows health IT developers to place certain limitations on the communication of video. Under this provision, a health IT developer may require persons who communicate video to limit the sharing of video to: (1) The relevant amount of video needed to communicate about the health IT regarding one or more of the

[100] Id. at 280–81.

subject areas identified in the Cures Act and detailed in § 170.403(a)(1); and (2) only videos that address temporal matters that the user reasonably believes cannot be communicated through screenshots or other forms of communications.

In sum, any disclosure must be limited to the relevant number of screenshots or amount of video that is necessary to convey the matter that falls within one of the six subject areas, with video only being used to convey temporal matters that cannot be communicated through screenshots or other forms of communication. We believe these additional limitations on the communication of screenshots and video will further bolster protections for developer IP, while still allowing necessary and effective communication about health IT issues within the six subject areas.

Comments. Several commenters stated that there should be a way to protect against doctored screenshots.

Response. As proposed, communicators of screenshots must not alter the screenshots (or video), except to annotate the screenshots or resize the screenshots (§ 170.403(a)(2)(ii)(D)(*1*)). These restrictions similarly apply to video as well (§ 170.403(a)(2)(ii)(D)(*1*)). We further note that, despite a lack of comments, on further reflection, we have elected to not finalize proposed limitations to allow developers to impose restrictions on the communication of screenshots that contain PHI. We have made this determination because we believe that most of the individuals or entities communicating the screenshots would be bound by other laws, including the HIPAA Rules and State privacy laws, which would be applicable to the PHI at issue. Therefore, we do not believe it is necessary to provide for developers policing the release of such data in the form of screenshots in this Condition of Certification.

Comments. A number of commenters discussed the infeasibility of the proposed requirements regarding restricting communication of screenshots, and in particular, the requirement that health IT developers put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because it would infringe IP rights. Some commenters stated that the proposed language should be amended to require a list of third-party content that might appear in a screen or that the developer sublicenses, or to require a notice on the developer's website. Other commenters stated that the proposal should be removed. One commenter recommended ONC consider not making developers accountable for actions by health IT users regarding the disclosure of screenshots with third-party information. One commenter requested additional guidance from ONC for dealing with third-party, non-health IT content in health IT.

Response. Where a health IT developer is prohibited by this rule from restricting the communication of a screenshot and allows a screenshot containing third-party content to be communicated, the health IT developer is acting as required by this final rule and enabling important communication regarding critical health IT issues to occur. Thus, we believe developers acting in accordance with this final rule should not be responsible for third-party content in screenshots that are communicated as required by the Communications Condition of Certification requirements. As such, in § 170.403(a)(2)(ii)(D) we have removed from the requirements related to third-party IP rights proposed in 84 FR 7475.

(E) Testing and Development

We discussed in the Proposed Rule in 84 FR 7475 that some health IT developers expose aspects of their health IT to health care providers and others for the purpose of testing and development prior to a product's ''general availability'' release. We stated that such disclosures may relate to beta releases that are shared with certain customers for testing prior to the software being made generally available to the market, or may be made as part of a joint-venture or cooperative development process. In these circumstances, we proposed in 84 FR 7475 that a health IT developer would be justified in keeping information about its health IT confidential. We explained that this permitted prohibition or restriction would allow developers to seek appropriate IP protection and discuss novel, ''unreleased'' product features with their customer base, which has significant public policy benefits for research and innovation in the health IT industry.

We proposed in 84 FR 7475 that this permitted restriction would be limited and would not apply to communications that are subject to unqualified protection as specified in proposed § 170.403(a)(2)(i). We proposed that this permitted restriction would also not apply to communications about the released version of the health IT once the health IT has been released.

We requested comment on whether we should limit the time this protection would apply for testing purposes. We also requested comment on whether we should set specific parameters for covered testing.

Comments. A couple of commenters stated that there should be no limit on how long testing and development could last for the purpose of the restrictions that developers would be allowed to place on communications regarding products in development. These commenters stressed that any limit would be arbitrary and that until certified health IT is in live commercial use, health IT developers should be permitted to restrict communications about it.

Response. We agree with the commenters and did not propose to add a time limit on testing and development phases for the purpose of this Condition of Certification requirement.

Comments. A couple of commenters requested clarification that providers testing products in real-world environments would not be considered ''contractors'' of developers for the purpose of the Communications Condition of Certification requirements because such treatment could result in developers being allowed to place additional communication restrictions on employees and contractors under the Communication Condition of Certification requirements. One comment also stated that restrictions on communications by employees and contractors should not extend to their communications regarding product features and functionality that the employees and contractors were not involved in developing or testing.

Response. The applicability of this allowable restriction to providers testing products would be determined by the particular facts at issue and whether or not the provider was an actual contractor, employee, or consultant for the developer. We also clarify that this final rule does not limit the restrictions a developer may place on an employee, contractor, or consultant with regard to protected communications, except to the extent that the communication is one with unqualified protection, in which case no such restrictions would be allowed.

Comments. One commenter recommended that a health IT user must have used health IT in a real-world context before a communication by the user about the health IT can be protected.

Response. We have finalized our proposal in § 170.403(a)(2)(ii)(E) that a health IT developer would be justified in keeping information about its health

IT confidential prior to a product's ''general availability'' release. We note that a health IT developer would also be justified in keeping information about a product update confidential because the update is not yet generally available. We do not place any limits on who the communicator has to be in order to be covered by the Communications Condition of Certification requirements, particularly since the protections in the Communications Condition of Certification requirements extend beyond users of certified health IT to cover researchers and other stakeholders who may experience certified health IT in a variety of settings and scenarios. As such, we have decided not to limit the communication protection to only those communications that are made by users of certified health IT in the real-world context.

c. Maintenance of Certification Requirements

We proposed in 84 FR 7476 that to maintain compliance with the Communications Condition of Certification requirements, a health IT developer must not establish or enforce any contract or agreement provision that contravenes the Communications Condition of Certification requirements. We also proposed in 84 FR 7476 that a health IT developer must notify all entities or individuals with which it has a contract/agreement related to certified health IT that any communication or contract/agreement provision that contravenes the Communications Condition of Certification requirements will not be enforced by the health IT developer. We proposed in 84 FR 7476 that such notification must occur within six months of the effective date of the final rule. Further, we proposed in 84 FR 7476 that this notice would need to be provided annually up to and until the health IT developer amends the contract or agreement to remove or make void any contractual provision that contravenes the Communications Condition of Certification requirements. We further proposed as a Maintenance of Certification requirement in proposed § 170.403(b)(2) that health IT developers must amend their contracts/agreements to remove or make void any provisions that contravene the Communications Condition of Certification requirements within a reasonable period of time, but not later than two years from the effective date of a final rule.

In the event that a health IT developer cannot, despite all reasonable efforts, locate an entity or individual that previously entered into an agreement with the developer that prohibits or restricts communications protected by the Communications Condition of Certification requirements, we proposed in 84 FR 7476 that the developer would not be in contravention of the Communications Condition of Certification requirements so long as it takes no step to enforce the prohibition or restriction. We did not propose that health IT developers be required to furnish to ONC or their ONC–ACB copies of notices made to customers, or copies of contracts or agreements revised, in satisfaction of this Maintenance of Certification requirement, although we noted that those communications could be requested by ONC or an ONC–ACB in the usual course of business or to demonstrate compliance.

Comments. A number of commenters expressed concerns regarding the proposed deadlines for complying with the requirements. Several commenters stated that the requirement to notify customers and others with whom the developer has contracts or agreements within six months was too long and recommended that the deadline be shortened. Regarding the deadline for amending contracts/agreements that contravene the Communications Condition of Certification requirements, most commenters stated that the deadline was too short, with several requesting that it be extended to five years. Some other commenters recommended that modification of any contracts/agreements to comply with the Communications Condition of Certification requirements should occur whenever such contracts/agreements are renewed, or at the earliest available time, without the need for a specific deadline. A couple of commenters recommended that a health IT developer not be held responsible for amending contracts within two years of the effective date of the final rule if it has made reasonable efforts to do so. Several comments recommended that ONC should allow alternative means of completing this requirement, such as posting relevant language on the developer's website. One commenter stated that it would be helpful to have a ''standard exception clause'' that developers could use in their contracts and agreements.

Response. We appreciate the comments we received on this provision. We clarify in § 170.403(b)(2)(i) that a developer may not include provisions that contravene the Communications Condition of Certification requirements in any new contract as of the effective date of the final rule. In consideration of comments, we have decided to modify the timeframe requirement proposed in 84 FR 7476 for amending contracts/agreements to be in compliance with this condition. While we considered extending the deadline to five years to allow developers to have additional time for compliance, we determined that a more flexible solution is appropriate. As such, we have modified the requirement in § 170.405(b)(2)(ii) to state that any contracts/agreements in place as of the effective date of the final rule and containing language in contravention of the Communications Condition of Certification requirements must be revised to remove or void the contractual provision that contravenes the Communications Condition of Certification requirements whenever the contract is next modified for any reason. We clarify that where a contract automatically renews, the developer would still be prohibited under the Program from enforcing any agreement or contract provisions that contravene the Communications Condition of Certification requirements in § 170.403(a) and the developer would also be responsible for sending an annual notice as described above until such provisions have been modified. To note, we decline to absolve a developer of the requirement to modify the contract solely because the developer has made a reasonable effort to do so.

We finalized the notification requirements proposed in 84 FR 7476. A health IT developer must notify all entities and individuals with which it has a contract/agreement related to certified health IT that any communication or contract/agreement provision that contravenes the Communications Condition of Certification requirements will not be enforced by the health IT developer. However, we no longer require that such notification must occur within six months of the effective date of the final rule and annually thereafter until contravening provisions are amended. Instead, notification must only occur annually, beginning in calendar year 2020, and continue until all contravening provisions are amended. Given the timing of the publication of the final rule, health IT developers could have potentially been required to provide both initial notification and an annual notification in the same calendar year. We believe the removal of the six months notification deadline and retention of an annual requirement only, beginning with notification in calendar year 2020, will simplify compliance for health IT developers while still providing adequate notice and ensuring that initial notification is provided in a reasonable amount of time. Therefore

we have finalized the deadline for the notice requirement in § 170.403(b)(1) to be annually, beginning in calendar year 2020.

Comments. Several commenters requested clarification that once the final rule goes into effect, contravening provisions in developer contracts prohibiting communications cannot be enforced. One of these commenters stated that developers would often include language in their contracts prohibiting communication on the part of end users and entities, thus preventing communication about issues with EHRs. Several commenters requested that ONC explicitly state that any permitted communication made following the effective date of the final rule be inadmissible as a violation of a contract/agreement regardless of whether the customer has been notified. One commenter requested that ONC clarify that, with respect to protecting communications regarding developer business practices, where the disclosure of certain information is prohibited by contract, the developer would not be liable for its inability to communicate such information.

Response. We emphasize that as of the effective date of the final rule, contravening provisions in contracts or agreements cannot be enforced without the risk of losing certification for the developer's health IT or a certification ban for the developer under the Program, regardless of whether the customer was notified as required by the Communications Condition of Certification requirements. We clarify that provisions of contracts requiring that the health IT customer ''flow-down'' obligations onto the customer's employees, contractors, and other users of the health IT that would restrict protected communications would be in contravention of this Condition of Certification. Such provisions could not be enforced after the effective date of the final rule without risking loss of certification as noted above for the developer under the Program.

We appreciate commenters' concern regarding disclosing information that may be otherwise prohibited by contract. However, we clarify that the purpose of the Communications Condition of Certification requirements is to prevent developers from improperly restricting protected communications, including communications about a developer's practices and policies related to facilitating the exchange of health information. As discussed earlier in this section, costs, timeframes, licensing practices and terms, as well as the developer's approach to working with third-party services, could all be considered protected communications to the extent they relate to facilitating the exchange of health information. Thus, we reiterate that where a contract entered into by the developer would restrict a communication protected by the Communications Condition of Certification requirements, the developer may not enforce such a contract and may not restrict a protected communication in violation of the Communications Condition of Certification requirements after the effective date of the final rule without risking loss of certification. It is also important to note that not all contractual provisions related to communications would create a risk of de-certification. As noted above, the Communications Condition of Certification requirements in § 170.403(a)(2)(ii) do allow for developers to place restrictions on certain communications as discussed above. Therefore, contractual provisions that appropriately address those allowances would not create a risk of de-certification under the Program.

Comments. One commenter suggested that ''renew'' should be added to the maintenance requirement to not establish or enforce any contract or agreement that contravenes the Communications Condition of Certification requirements in § 170.403(a).

Response. We appreciate this comment and amended the proposed regulatory text in § 170.403(b)(2)(i) to include ''renew.'' We clarify that where a contract auto-renews, the developer would still be prohibited under the Program from enforcing any agreement or contract provisions that contravene the Communications Condition of Certification requirements without risking loss of certification and would also be responsible for sending an annual notice as described above until such provisions have been modified.

Comments. A couple of commenters expressed concern about developer efforts to re-negotiate other terms of a contract that are unrelated to protected communications as part of the contract modification process.

Response. We stress that the contract modifications required as part of the Communications Condition of Certification requirements are strictly limited to removing any provisions of the relevant contract/agreement that would restrict protected communications in contravention of the Communications Condition of Certification requirements and are not required to be done until the contract/agreement is modified for other purposes.

4. Application Programming Interfaces

The API Condition of Certification requirement in Section 4002 of the Cures Act requires health IT developers to publish APIs that allow ''health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.'' The requirement also states that a developer must, through an API, ''provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.'' Additionally, the API Condition of Certification requirement of the Cures Act includes several key phrases and requirements for health IT developers that go beyond the technical functionality of the Health IT Modules they present for certification. In this section of the preamble, we outline the proposals we have adopted to implement the API Condition of Certification requirement of the Cures Act to provide compliance clarity for health IT developers.

We have adopted new standards, new implementation specifications, a new certification criterion, Condition and Maintenance of Certification requirements, and modified the Base EHR definition. Health IT developers should consider these final requirements in the context of information blocking provisions described in section VIII of this preamble.

a. Statutory Interpretation and API Policy Principles

Section 4002 of the Cures Act requires health IT developers certified to the Program to publish APIs that allow ''health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law.'' To implement the Cures Act API requirements, we proposed a new 2015 Edition Cures Update ''API'' certification criterion at 84 FR 7476 that included requirements for an API to have ''read'' capabilities that support two types of services: (1) Services for which a single patient's data is the focus; and (2) services for which multiple patients' data are the focus.

We conveyed in the Proposed Rule our belief that ''without special effort'' requires APIs and the health care ecosystem in which they are deployed to be standardized, transparent, and pro-

competitive. Therefore, we noted that any Health IT Module certified to the new 2015 Edition Cures Update API criterion and a health IT developer's business practices would have to have these attributes.

b. API Standards and Implementation Specifications

i. Base Standard

We proposed in § 170.215(a)(1) at 84 FR 7477 to adopt HL7® FHIR® Draft Standard for Trial Use (DSTU) 2 for reference in the criterion proposed in § 170.315(g)(10). Additionally, we requested comment in 84 FR 7478 and 7479 on four options to determine the best version of HL7 FHIR to reference for use in § 170.315(g)(10): Option 1: FHIR DSTU 2, Option 2: FHIR DSTU 2 and FHIR Release 3, Option 3: FHIR DSTU 2 and FHIR Release 4, and Option 4: FHIR Release 4 only. We requested commenters review the proposed certification criterion in § 170.315(g)(10) and the accompanying Condition of Certification requirements attributed to the API certification criteria. Notably, we stated in the Proposed Rule at 84 FR 7479 that if we adopted another FHIR Release in a final rule as an alternative to FHIR Release 2 for the proposed API criterion in § 170.315(g)(10), then we would also adopt the applicable implementation specifications associated with the FHIR Release.

Comments. We received overwhelming support for Option 4: Adopt solely FHIR Release 4 in the final rule for reference in § 170.315(g)(10). We received support for the adoption of FHIR Release 4 across a broad array of stakeholders, including health IT developers, medical trade associations, software application developers, and payers. Commenters noted that FHIR Release 4 is the first FHIR release with normative FHIR resources and support for enhanced capabilities. Most commenters emphasized that Option 4 will allow the industry to unify and focus on a single baseline standard, rather than accommodating multiple releases proposed in Options 2 and 3. A minority of commenters suggested alternative or multiple versions, noting this would allow for flexibility, but the vast majority of commenters supported the adoption of FHIR Release 4 only.

Response. We appreciate the feedback and agree with commenters that adoption of a single standard is the best option to align industry and enable widespread interoperability. We have adopted the latest version of the standard at the time of this final rule publication (FHIR Release 4.0.1) in § 170.215(a)(1) and finalized its use in § 170.315(g)(10).

ii. United States Core Data for Interoperability

We proposed in § 170.215(a)(2) at 84 FR 7479 to adopt the API Resource Collection in Health (ARCH) Version 1 implementation specification, which listed a set of base HL7® FHIR® resources that Health IT Modules certified to the proposed criterion in § 170.315(g)(10) would need to support.

Comments. Most commenters were opposed to the adoption of the ARCH in the final rule. Commenters argued for the use of American National Standards Institute accredited standards, and suggested ONC work with standards developing organizations for standards development and maintenance.

Several commenters noted that the ARCH has not gone through a formal balloting process, did not support ONC's proposal to rely upon the National Technology Transfer and Advancement Act's exception to adopt the ARCH in the final rule, and encouraged the use of technical standards developed or adopted by voluntary consensus standards bodies. Several commenters noted that requiring the ARCH in addition to the other adopted standards could create confusion. Commenters further emphasized the importance of maintaining ongoing consistency between the ARCH and the other adopted standards, and noted this would be challenging to achieve.

Additional comments against the ARCH expressed concern with the proposed updates through the Standards Version Advancement Process, and with ONC over-regulating API functionality. Commenters also noted that ONC could encourage API access to specific data elements without creating a new implementation specification.

Some commenters in favor of the ARCH implementation specification asked for data element revisions. Commenters also asked for clarity that EHRs will not need to provide the full set of data to modular applications, and asked for specificity on how much of this data would need to be mapped by the API Technology Supplier. Additionally, commenters asked for guidance on lab results, including application creation implementation guides that would ensure accuracy and compliance when incorporating lab data.

Response. In response to commenters, we did not adopt the ARCH as an implementation specification in the final rule. Upon consideration of public comments and in an effort to consistently approach how we reference the United States Core Data for Interoperability (USCDI) with various content standards (*e.g.,* C–CDA), we determined that having an implementation specification to map USCDI to HL7 FHIR could create more restrictions than we intended. We appreciate the concerns raised by stakeholders, and as we evaluated the ARCH in context of our other proposals, we determined that we could achieve our desired policy outcome to link the USCDI Data Elements to FHIR Resources without the ARCH. We refer commenters to the sections that follow for further clarity regarding the implementation of Data Elements included in the USCDI implementation specification (IV.B.1).

iii. US Core IG and Bulk IG

We proposed in 84 FR 7480 in § 170.215(a)(3) to adopt the Argonaut Data Query Implementation Guide version 1 (Argonaut IG) implementation specification, which specifies constraints for 13 of the HL7® FHIR® resources proposed in § 170.215(a)(2). Additionally, we proposed in § 170.215(a)(4) to adopt the Argonaut Data Query Implementation Guide Server implementation specification.

Comments. Several commenters advocated for the adoption of the FHIR US Core Implementation Guide STU 3 Release 3.0.0 implementation specification instead of the Argonaut Implementation Guides. Commenters noted that the US Core Implementation Guide was built from the Argonaut Implementation Guides and has been balloted by the standards community.

Response. We thank commenters for their feedback. We note that in the Proposed Rule at 84 FR 7479 we stated that if we were to adopt another FHIR Release in the final rule as an alternative to FHIR Release 2, then we would also adopt the applicable implementation specifications and FHIR profiles associated with the FHIR Release. Considering this and commenters' recommendations, we have adopted the HL7 FHIR US Core Implementation Guide STU 3.1.0 (US Core IG) implementation specification in § 170.215(a)(2). We note that we adopted the latest version of the US Core IG at the time of the final rule publication. The US Core IG defines the minimum conformance requirements for accessing patient data using FHIR Release 4 (adopted in § 170.215(a)(1)), including profiled resources, operations, and search parameters for the Data Elements required in the USCDI implementation specification (adopted in § 170.213).

We note that in the Proposed Rule at 84 FR 7479 we proposed to require that the ''Patient.address'' and ''Patient.telecom'' elements of the ''Patient'' resource must be supported. We note these requirements have since been subsumed by the US Core IG, given that ''Patient.address'' and ''Patient.telecom'' elements are both flagged ''must support'' for the ''Patient'' profile in the US Core IG. We also proposed to require that the ''Device.udi'' element follow the human readable representation of the unique device identifier found in the recommendation, guidance, and conformance requirements section of the ''HL7 Version 3 Cross Paradigm Implementation Guide: Medical Devices and Unique Device Identification Pattern, Release 1.'' These requirements have also been subsumed by the US Core IG. Additional information can be found in the ''Device'' profile of the US Core IG adopted in § 170.215(a)(2).

We note that in the Proposed Rule we proposed in 84 FR 7480 that the clinical note text included in the ''DocumentReference'' resource would need to be represented in its ''raw'' text form, and further proposed in 84 FR 7480 that it would be unacceptable for the note text to be converted to another file or format (*e.g.,* .docx, PDF) when it is provided as part of an API response. We clarify that the clinical note text included in any of the notes described in the ''Clinical Notes Guidance'' section of the US Core IG adopted in § 170.215(a)(2) must be represented in a ''plain text'' form, and would be unacceptable for the note text to be converted to another file or format (*e.g.,* .docx, PDF) when it is provided as part of an API response.

We note that in the Proposed Rule we proposed in 84 FR 7480 to require that the ''Provenance.recorded'' and ''Provenance.agent.actor'' elements of the ''Provenance'' resource must be supported. We note these requirements have been subsumed by the US Core IG, given that ''Provenance.recorded'' and ''Provenance.agent.who'' elements are both flagged ''must support'' for the ''Provenance'' profile in the US Core IG.

As addressed under the header ''Standardized API for Patient and Population Services'' in the section V.B.4.c, we have finalized the adoption of the HL7 FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1) implementation specification (Bulk IG), including mandatory support for the ''group-export'' ''OperationDefinition'' in § 170.215(a)(4).

iv. HL7 SMART IG and Backend Services Authorization

We proposed in 84 FR 7481 in § 170.215(a)(5) to adopt the HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 implementation specification, a profile of the OAuth 2.0 specification.

Comments. Most commenters expressed support for the HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0 (SMART IG) implementation specification. Multiple commenters suggested that in addition to requiring support for ''refresh tokens,'' ''Standalone Launch,'' and ''EHR Launch'' capabilities from the SMART IG, ONC also require support for ''sso-openid-connect,'' ''launch-standalone,'' ''launch-ehr,'' ''client-public,'' ''client-confidentialsymmetric,'' ''context-ehr-patient,'' ''context-standalone-patient,'' ''permission-patient,'' ''permission-user,'' and ''permission-offline'' capabilities.

Response. We thank stakeholders for their comments. The ten optional capabilities commenters suggested are included in the ''SMART on FHIR Core Capabilities'' section of the SMART IG. The ''SMART on FHIR Core Capabilities'' suggested by commenters include ''sso-openid-connect,'' which allows for support of the OpenID Connect profile in the SMART IG; ''client-public'' and ''client-confidential-symmetric,'' which allow for client authentication; ''context-ehr-patient'' and ''context-standalone-patient,'' which provide context to apps at launch time; and ''permission-patient,'' ''permission-user,'' and ''permission-offline,'' which allow support for patient-level scopes, user-level scopes, and refresh tokens, respectively. Other ''SMART on FHIR Core Capabilities'' that were not suggested by commenters include ''context-banner'' and ''context-style,'' which provide basic context to apps at launch time, and ''context-ehr-encounter'' and ''context-standalone-encounter,'' which provide encounter-level granularity to apps at launch time. Given the importance of these ''SMART on FHIR Core Capabilities,'' and in consideration of public comments and our own research, we have adopted the SMART IG, including mandatory support for the ''SMART on FHIR Core Capabilities'' in § 170.215(a)(3). We explicitly require mandatory support of the ''SMART on FHIR Core Capabilities'' in § 170.215(a)(3) because these capabilities are indicated as optional in the implementation specification. We further clarify these ''SMART on FHIR Core Capabilities'' are in scope for Program testing and certification. Additionally, we clarify that by requiring the ''permission-patient'' ''SMART on FHIR Core Capability'' in § 170.215(a)(3), Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on FHIR resource-level scopes. Specifically, this means patients would need to have the ability to authorize access to their EHI at the individual FHIR resource level, from one specific FHIR resource (*e.g.,* ''Immunization'') up to all FHIR resources necessary to implement the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2). This capability will give patients increased control over how much EHI they authorize applications of their choice to receive. For example, if a patient downloaded a medication management application, they would be able to use these authorization scopes to limit the EHI accessible by the application to only information contained in FHIR ''MedicationRequest'' and ''Medication'' profile.

Comments. Some commenters noted concerns for privacy and security of APIs. Specifically, one commenter explained the threat of cross-site request forgery (CSRF), and suggested we take action to mitigate that risk, including by requiring the use of both OAuth 2.0 and OpenID Connect Core 1.0.

Response. We appreciate the concerns expressed by commenters regarding the privacy and security of APIs. The OAuth 2.0 standard defined at Request For Comment (RFC) 6749 [101] describes that ''[The OAuth 2.0 authorization] framework was designed with the clear expectation that future work will define prescriptive profiles and extensions necessary to achieve full web-scale interoperability.'' The SMART IG serves as a ''prescriptive profile'' as described in RFC 6749. Thus, consistent with commenters' recommendations, we have adopted a profile of the OAuth 2.0 standard (SMART IG) in § 170.215(a)(3). Additionally, we have adopted OpenID Connect Core 1.0 incorporating errata set 1 in § 170.215(b), and require conformance with the relevant parts of this standard as part of testing and certification. CSRF is a well-documented security threat in OAuth 2.0, which can be prevented with adequate security practices. We encourage implementers to adhere to industry best practices to mitigate CSRF and other known security threats. Relatedly, we note that the HL7 community has developed an

[101] *https://tools.ietf.org/html/rfc6749.*

''Implementer's Safety Check List,'' [102] a guide of security best practices for implementing FHIR-based APIs. We encourage stakeholders to consult this guide during development and implementation of § 170.315(g)(10)-certified Health IT Modules to minimize security risks.

For backend services authorization, as addressed under the header ''Standardized API for Patient and Population Services'' in the section V.B.4.c, we have finalized the adoption of the HL7 FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1) implementation specification (Bulk IG), which includes the ''Backend Services Authorization Guide'' in § 170.215(a)(4).

v. OpenID Connect

We proposed in 84 FR 7480 through 7481 in § 170.215(b) to adopt OpenID Connect Core 1.0 including errata set 1.

Comments. We received few comments regarding the adoption of OpenID Connect Core 1.0 including errata set 1, however, commenters generally supported the adoption of this standard.

Response. We thank commenters for their feedback. Given their support, we have finalized the adoption of OpenID Connect Core 1.0 including errata set 1 as proposed in § 170.215(b). We clarify that only the relevant parts of the OpenID Connect Core 1.0 including errata set 1 adopted in § 170.215(b) that are also included in the implementation specification adopted in § 170.215(a)(3) will be in-scope for testing and certification.

c. Standardized API for Patient and Population Services

We proposed in 84 FR 7481 to adopt a new certification criterion, § 170.315(g)(10), to replace § 170.315(g)(8), and we proposed in 84 FR 7495 to update the 2015 Edition Base EHR definition, as referenced in § 170.102. The proposed certification criterion would require Health IT Modules to support API-enabled ''read'' services for single and multiple patients. ''Read'' services include those that allow authenticated and authorized third-party applications to view EHI through a secure API. These services specifically exclude ''write'' capabilities, where authenticated and authorized third-party applications would be able to create or modify EHI through a secure API.

Comments. Commenters supported the proposed adoption of a new certification criterion, § 170.315(g)(10), to replace § 170.315(g)(8).

Response. We appreciate the support from commenters. As a result, we have adopted a new certification criterion in § 170.315(g)(10), to replace § 170.315(g)(8) and made several revisions to address public comment as discussed further below. Although the certification criteria finalized at § 170.315(g)(10) will replace § 170.315(g)(8), we note that § 170.315(g)(8) is not removed from regulation. We maintain § 170.315(g)(8) and have finalized in § 170.550(m) that ONC–ACBs can issue certificates for § 170.315(g)(8) during the transition period to § 170.315(g)(10) for 24 months after the publication date of the final rule.

Comments. Commenters suggested dividing the § 170.315(g)(10) criterion into two separate criteria for single and multiple patients.

Response. We appreciate the feedback. We decline to split the certification criterion into two criteria. In consideration of comments and for clarity, we have improved the organization of the final certification requirements for API-enabled ''read'' services for single and multiple patients by separating the criterion into distinct sections in the regulation text.

Comments. Several commenters supported referencing a standard for API-enabled ''read'' services for multiple patients, including the HL7® FHIR® Bulk Data Access Implementation Guide Release 1.0.0. Commenters felt that omitting a standard in the criterion would undermine interoperability for API-enabled ''read'' services for multiple patients.

Response. We thank commenters for their feedback. To enable consistent health IT implementation of API-enabled ''read'' services for multiple patients, we have finalized the adoption of the Bulk IG, including mandatory support for the ''group-export'' ''OperationDefinition'' in § 170.215(a)(4). As part of the Program, we require Health IT Modules presented for testing and certification to conform to the Bulk IG implementation specification finalized in § 170.215(a)(4). The adoption of an implementation specification for API-enabled ''read'' services for multiple patients in § 170.215(a)(4) is responsive to stakeholder concerns and further supports our intent to prevent ''special effort'' for the use of APIs as mandated in section 4002 of the Cures Act. Furthermore, based on our analysis, we believe the ''group-export'' ''OperationDefinition,'' as defined in the Bulk IG implementation specification is essential to fulfill the use cases envisioned for API-enabled ''read'' services for multiple patients. The ''group-export'' ''OperationDefinition'' will allow application developers interacting with § 170.315(g)(10)-certified Health IT Modules to export the complete set of FHIR resources as constrained by the US Core IG adopted in § 170.215(a)(2) and USCDI adopted in § 170.213 for a pre-defined cohort of patients. We appreciate commenters' recommendations, and agree that coalescing around a common implementation specification will advance interoperability of API-enabled ''read'' services for multiple patients. We provide further discussion of the supported search operations, data response, and authentication and authorization requirements for API-enabled ''read'' services for multiple patients in the sections below.

Comments. Commenters requested clarification that API-enabled ''read'' services for multiple patients are not intended for patient end users and that health IT developers and health care providers are therefore not expected to supply a patient-facing mechanism for these requests.

Response. We appreciate the feedback from commenters. API-enabled ''read'' services for multiple patients are not intended for patient end users because API-enabled ''read'' services for multiple patients allow for the disclosure of multiple patients' records, and individual patients only have the right to access their own records or records of patients to whom they are the personal representative (45 CFR 164.502(f)(1)). Health IT Modules are not required to support patient-facing API-enabled ''read'' services for multiple patients for the purposes of this certification criterion.

Comments. One commenter suggested we modify the language that defines the purpose of this section to provide more clarity, specifically the term ''services.'' The commenter also requested we include the scope of cohorts we intended to address in ''population services.''

Response. We appreciate the feedback from commenters. The term ''services'' includes all § 170.315(g)(10)-related technical capabilities included in a Health IT Module presented for testing and certification. The API-enabled ''read'' services for single patients is intended to support EHI requests and responses for individual patient records and the API-enabled ''read'' services for multiple patients is intended to support EHI requests and responses for multiple patients' records. The scope of patient cohorts for ''population services'' can include various groups defined at the

[102] *https://www.hl7.org/FHIR/safety.html.*

discretion of the user of the API-enabled ''read'' services for multiple patients, including, for example, a group of patients that meet certain disease criteria or fall under a certain insurance plan. We have adopted the Bulk IG in § 170.215(a)(4) to support this function as discussed further below. The technical capabilities expected of API-related Health IT Modules presented for testing and certification are included in § 170.315(g)(10).

Comments. Commenters requested clarification for information blocking policies and health care provider obligations for API-enabled ''read'' services for multiple patients.

Response. We appreciate the request for clarification from commenters. We clarify that the criteria finalized in § 170.315(g)(10) includes the technical capabilities that must be met by API-related Health IT Modules presented for testing and certification. The information blocking policies in this rule do not compel health care providers to implement Health IT Modules certified to requirements in 170.315(g)(10). We note that other programs, like CMS value-based programs, may require the use of this technology. We refer commenters to the information blocking section (VIII) for additional clarification.

Comments. Commenters asked us to clarify the relationship between the API-enabled ''read'' services for single and multiple patients in § 170.315(g)(10) and the ''EHI export'' criterion in § 170.315(b)(10).

Response. We thank commenters for this request. The API criterion in § 170.315(g)(10) is separate from the ''EHI export'' criterion in § 170.315(b)(10). While both criteria aim to advance health IT in alignment with the Cures Act's goal of ''complete access, exchange, and use of all electronically accessible health information'' for both single and multiple patients, the criteria specifications and Condition and Maintenance of Certification requirements are distinct.

The ''EHI export'' criterion focuses on a Health IT Module's ability to electronically export EHI, as defined in § 171.102, that can be stored at the time of certification by the product, of which the Health IT Module is a part. In contrast, the finalized API criterion in § 170.315(g)(10) focuses on ''read'' services for single and multiple patients for the USCDI (adopted in § 170.213) Data Elements and US Core IG (adopted in § 170.215(a)(2)) FHIR profiles. Additionally, the ''EHI export'' criterion finalized in § 170.315(b)(10) does not mandate conformance to standards or implementation specifications, whereas the criterion finalized in § 170.315(g)(10) requires conformance to several standards and implementation specifications, as described further below. We refer to the finalized ''EHI export'' criterion in § 170.315(b)(10) for additional information.

Comments. Several commenters supported requiring Health IT Modules to support API-enabled ''write'' services for single patients, either in this rule or in a future rulemaking. One commenter suggested including a subset of data classes for ''write'' services for single patients, including ''patient goals,'' ''patient-generated health data'' (including patient-reported outcomes, patient generated device data, and questionnaires), and ''care plans.'' Another commenter suggested adding a list of required operations (''read'' and ''write'') to USCDI elements, limited to ''read'' for this rulemaking.

Response. We appreciate the feedback from commenters. While we support the interest in API-enabled ''write'' services, we have not adopted such requirements. We do not believe API-enabled ''write'' services have reached a level of a maturity to warrant the addition of regulatory conformance requirements within the Program. We encourage industry to consider all the implications and implementation requirements for API-enabled ''write'' services, and perform additional API-enabled ''write'' pilot implementations to demonstrate the readiness for API-enabled ''write'' services in the testing and certification of Health IT Modules. Additionally, we encourage industry to expand existing profiles like the US Core IG to support ''write'' services.

Comments. Commenters recommended including a requirement for event logging for ''read'' services for single and multiple patients.

Response. We appreciate the recommendation from commenters. The 2015 Edition Privacy and Security Certification Framework requires that if a Health IT Module includes capabilities for certification under § 170.315(g)(10) it needs to be certified to several privacy and security certification criteria including auditable events in § 170.315(d)(2) or auditing actions on health information in § 170.315(d)(10).

Comments. Commenters noted that references to APIs focus exclusively on RESTful query and ignore ''push'' elements of the FHIR API, such as ''POST,'' ''PUT,'' and FHIR messaging.

Response. We appreciate the feedback from commenters. While we support the interest in the ''push'' operations of the FHIR standard, including ''POST,'' ''PUT,'' and FHIR messaging, we have not adopted such requirements for the Program. We encourage industry stakeholders to further consider all the requirements and implications for the ''push'' operations of the FHIR standard, develop use cases, perform additional API-enabled ''push'' pilot implementations, create or expand implementation profiles to support ''push'' services, and demonstrate the utility of the ''push'' operations of the FHIR standard for future potential inclusion in the Program.

i. Data Response

We proposed in 84 FR 7482 in § 170.315(g)(10)(i) that Health IT Modules presented for testing and certification must be capable of responding to requests for data on single and multiple patients in accordance with proposed standards and implementation specifications adopted in § 170.215(a)(1) (HL7® FHIR® DSTU 2 (v1.0.2–7202)), specified in the proposed § 170.215(a)(2) (API Resource Collection in Health (ARCH) Version 1), and consistent with the proposed specifications in § 170.215(a)(3) (Argonaut Data Query Implementation Guide Version 1.0.0). We clarified that all data elements indicated as ''mandatory'' and ''must support'' by the proposed standards and implementation specifications must be supported and would be in scope for testing.

Comments. Commenters expressed concern with fully enforcing ''mandatory'' and ''must'' support requirements of the referenced specifications and implementation guides, explaining that developers may be required to support requirements that are not applicable to the stated intended use of the Health IT Module(s).

Response. We appreciate the concerns expressed by commenters. We clarify that the standards and implementation specifications adopted and required for this certification criterion were created by standards developing organizations to support a wide range of health care use cases.

We have finalized in § 170.315(g)(10)(i)(A) that Health IT Modules presented for testing and certification must be capable of responding to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted in § 170.215(a)(2), including the mandatory capabilities described in ''US Core Server CapabilityStatement,'' for each of the Data Elements included in the standard adopted in § 170.213. This requirement will enable Health IT Modules to support US Core IG

operations for each of the Data Elements included in the USCDI.

Additionally, we have finalized in § 170.315(g)(10)(i)(B) that Health IT Modules presented for testing and certification must be capable of responding to requests for data on multiple patients as a group according to the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a)(2) and § 170.215(a)(4), for each of the Data Elements included in the standard adopted in § 170.213. Finally, we clarify that the use of the ''SMART Backend Services: Authorization Guide'' section of the implementation specification adopted in § 170.215(a)(4) is required for API ''read'' services for multiple patients as finalized in § 170.315(g)(10)(i)(B) and described above.

For requests for data on multiple patients, we note that the implementation specification adopted in § 170.215(a)(4) has optional parameters which can be used to filter results to a period of time, or one or several specified FHIR resources. While these parameters are not required for testing and certification, we encourage health IT developers to adopt these parameters and other ''OperationDefinitions'' to enhance the utility of requests for data on multiple patients.

ii. Search Support

We proposed in 84 FR 7482 in § 170.315(g)(10)(ii) that Health IT Modules presented for testing and certification must be capable of responding to all of the ''supported searches'' specified in the proposed implementation specification in § 170.215(a)(4) (Argonaut Data Query Implementation Guide Server). We reiterated that Health IT Modules presented for testing and certification and as implemented must support all search capabilities for single and multiple patients in accordance with the proposed implementation specification in § 170.215(a)(4). We also requested comments on the minimum ''search'' parameters that would need to be supported for the ''DocumentReference'' and ''Provenance'' HL7® FHIR® resources.

Comments. Most commenters supported this proposal. One commenter recommended only requiring the ''target'' query parameter for the ''Provenance'' FHIR resource, and ''patient'' and ''date'' query parameters for the ''DocumentReference'' FHIR resource. One commenter suggested deferring this certification requirement until a standard is published by HL7.

Response. We appreciate the feedback from commenters. Since we have not finalized the adoption of the ARCH as proposed in § 170.215(a)(2), and instead rely on the search parameters specified in the US Core IG finalized in § 170.215(a)(2) and Bulk IG finalized in § 170.215(a)(4), the comments related to the specific ''Provenance'' and ''DocumentReference'' FHIR resources are no longer applicable. We have finalized in § 170.315(g)(10)(ii)(A) that Health IT Modules presented for testing and certification must support all search capabilities for single patients according to the implementation specification adopted in § 170.215(a)(2), including support for all mandatory capabilities included in the ''US Core Server CapabilityStatement.'' Additionally, we have finalized in § 170.315(g)(10)(ii)(B) that Health IT Modules presented for testing and certification must respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4). We clarify that the scope of data available in the data responses defined in § 170.315(g)(10)(i) must be supported for single and multiple patient searches via the supported search operations finalized in § 170.315(g)(10)(ii). Additionally, we clarify for the requirements finalized in § 170.315(g)(10)(i) and (ii) that all data elements indicated as ''mandatory,'' ''must support,'' by the standards and implementation specifications must be supported and are in scope for testing.

iii. Application Registration

We proposed in 84 FR 7483 in § 170.315(g)(10)(iii) that Health IT Modules presented for testing and certification must be capable of enabling apps to register with an ''authorization server.'' As proposed, this would have required an API Technology Supplier to demonstrate its registration process, but would not have required conformance to a standard. We requested comment at 84 FR 7483 on whether to require the OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591) [103] standard as the sole method to support registration for the proposed certification criterion in § 170.315(g)(10), and requested comment on whether we should require its support as part of the final rule's certification criterion. Additionally, we requested comment at 84 FR 7483 on whether to include application registration in the testing and certification of apps executed within an API Data Provider's clinical environment.

Comments. Commenters generally supported that Health IT Modules presented for testing and certification must enable apps to register with an authorization server. Some commenters supported excluding application registration from the testing and certification of apps executed within an API Data Provider's clinical environment.

Response. We appreciate the feedback from commenters. Given the overwhelming support, we have finalized in § 170.315(g)(10)(iii) that Health IT Modules presented for testing and certification must enable apps to register with an authorization server. We clarify that Health IT Modules presented for testing and certification must support application registration regardless of the scope of patient search utilized by the application (*e.g.,* single or multiple). This certification criterion requires a health IT developer, as finalized in the Condition of Certification requirements section below, to demonstrate its registration process, but does not require conformance to a standard. Additionally, we expect that apps executed within an implementer's clinical environment will be registered with an authorization server, but we do not require a health IT developer to demonstrate its registration process for these ''provider-facing'' apps. We reiterate that we believe implementers of § 170.315(g)(10)-certified Health IT Modules should have the discretion to innovate and execute various methods for application registration within a clinical environment.

Comments. Commenters provided a mix of support and opposition for requiring the OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591) standard as the sole method of application registration. Some commenters felt that the Program should require dynamic client registration in the context of patient-access scenarios only, and others felt the standard is not ready for mandated adoption in the Program. Commenters opposed to requiring the OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591) felt that not specifying a standard would allow flexibility for different innovative registration approaches to be used and developed. Other commenters suggested there should be an option for data holders to support dynamic client application registration if the data holder prefers that approach, including support for dynamic application registration via trusted networks.

[103] *https://tools.ietf.org/html/rfc7591.*

Response. We appreciate the feedback from commenters. We have not adopted a requirement for Health IT Modules presented for testing and certification to support the OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591) standard. We agree with commenters and believe that requiring registration without a mandated standard will allow registration models to develop further. We encourage health IT developers to coalesce around the development and implementation of a common standard for application registration with an API's authorization server.

Comments. Commenters suggested permitting implementers of § 170.315(g)(10)-certified Health IT Modules to undertake a review of third-party applications prior to permitting them to connect to the implementers' deployed APIs.

Response. We appreciate the suggestion from commenters. The requirement that health IT developers must enable an application to register with the § 170.315(g)(10)-certified Health IT Module's authorization server only applies for the purposes of demonstrating technical conformance to the finalized certification criterion and Condition and Maintenance of Certification requirements. The practices by all parties (including implementers of Health IT Modules) other than developers of certified Health IT Modules are not in scope for this certification criterion nor the associated Condition and Maintenance of Certification requirements. All other practices associated with third-party application review or ''vetting'' by implementers must not violate the information blocking provision described in section VIII of this preamble and applicable laws and regulations. In general, an implementer of § 170.315(g)(10)-certified Health IT Modules (*e.g.,* health care providers) would be allowed to review third-party applications the implementer intends to use for its own business use (*e.g.,* a third-party decision-support application used by the health care provider in the course of furnishing care) prior to permitting the third-party applications to connect to the implementer's deployed APIs within its enterprise and clinical users' workflow. However, implementers of § 170.315(g)(10)-certified Health IT Modules (*e.g.,* health care providers) are not permitted to review or ''vet'' third-party applications intended for patient access and use (see section VII.C.6 of this preamble). We clarify that the third-party application registration process that a health IT developer must meet under this criterion is not a form of review or ''vetting'' for purposes of this criterion.

Comments. Commenters requested clarity on whether the ''EHR Launch'' scenario was out of scope for testing during registration with an authorization server.

Response. Commenters referred to the ''EHR Launch'' scenario, which is the ''launch-ehr'' ''SMART on FHIR Core Capability'' included in the implementation specification adopted in § 170.215(a)(3). Health IT Modules presented for testing and certification must enable all apps that utilize the SMART IG ''launch-standalone'' ''SMART on FHIR Core Capability'' to register with an authorization server. We reiterate that the application registration requirement finalized in § 170.315(g)(10)(iii) does not require conformance to a standard or implementation specification. We envision that apps using only the SMART IG ''launch-ehr'' ''SMART on FHIR Core Capability'' will be tightly integrated with § 170.315(g)(10)-certified Health IT Modules deployed by implementers, and will be able to accommodate registration processes that best suit the needs of those implementers. Additionally, while we do not require conformance to a standard or implementation specification for application registration, we clarify that Health IT Modules presented for testing and certification are required to support application registration functions to enable authentication and authorization as finalized in § 170.315(g)(10)(v).

iv. Secure Connection

We proposed in 84 FR 7483 in § 170.315(g)(10)(iv) that Health IT Modules presented for testing and certification must be capable of establishing a secure and trusted connection with an application requesting patient data in accordance with the proposed § 170.215(a)(5) (HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0), including mandatory support for ''Standalone Launch'' and ''EHR Launch'' modes.

Comments. Commenters asked for clarification around where ''Standalone Launch'' and ''EHR Launch'' capabilities are required, suggesting that ''Standalone Launch'' support be used exclusively for patient access and ''EHR Launch'' support be used exclusively for provider/clinician access. They also noted that testing and certification of ''Standalone Launch'' would not be a valid use case and should be excluded from the certification criterion.

Response. We appreciate the feedback from commenters. The SMART IG ''Standalone Launch'' and ''EHR Launch'' modes can be used by both provider- and patient-facing applications. We refer to the adopted implementation specification in § 170.215(a)(3) for clarification of certification requirements for the SMART IG. We have finalized in § 170.315(g)(10)(iv)(A) that Health IT Modules presented for testing and certification must demonstrate the ability to establish a secure and trusted connection with an application requesting data for a single patient in accordance with the implementation specifications adopted in § 170.215(a)(2) and (a)(3). We amended this text from the Proposed Rule by adding the US Core IG implementation specification adopted in § 170.215(a)(2) because the US Core IG specifically requires Transport Layer Security 1.2 (RFC 5246) [104] or higher for all transmissions not taking place over a secure network connection. Pursuant to this adopted implementation specification, we will test Health IT Modules for support for all ''SMART on FHIR Core Capabilities'' including both ''launch-ehr'' and ''launch-standalone.''

Additionally, we have finalized in § 170.315(g)(10)(iv)(B) that Health IT Modules presented for testing and certification must demonstrate the ability to establish a secure and trusted connection with an application requesting data for multiple patients in accordance with the implementation specification adopted in § 170.215(a)(4). The implementation specification adopted in § 170.215(a)(4) has several sections, but for testing and certification to this criterion, we specifically require conformance to, but not limited to, the ''SMART Backend Services: Authorization Guide.''

v. Authentication and Authorization

We proposed in 84 FR 7483 in § 170.315(g)(10)(v) that Health IT Modules presented for testing and certification must demonstrate the ability to perform user authentication, user authorization, and issue a refresh token valid for a period of at least 3 months during its initial connection with an application to access data for a single patient in accordance with the proposed standard in § 170.215(b) (OpenID Connect Core 1.0 incorporating errata set 1) and the proposed implementation specification in § 170.215(a)(5) (HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0).

[104] *https://tools.ietf.org/html/rfc5246.*

Additionally, we proposed in § 170.315(g)(10)(vi) that Health IT Modules presented for testing and certification must demonstrate the ability of an application to access data for a single patient and multiple patients during subsequent connections of applications capable of storing a client secret, in accordance with the proposed implementation specification in § 170.215(a)(5) (HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0), without requiring the user to re-authorize and re-authenticate when a valid refresh token is supplied. Additionally, we proposed in 84 FR 7483 that Health IT Modules presented for testing and certification must demonstrate it can issue a new refresh token to an application, valid for a period of at least 3 months.

Comments. A majority of commenters supported that Health IT Modules presented for testing and certification must demonstrate the ability to perform user authentication, user authorization, and issue a refresh token valid for a period of at least 3 months. Some commenters noted that the OAuth 2.0 implementation guide does not recommend servers provide refresh tokens to public/non-confidential applications.

Response. We thank commenters for their feedback. Given the general support and in response to these comments, we have consolidated the proposed requirements in § 170.315(g)(10)(v) and § 170.315(g)(10)(vi) as a revised set of requirements finalized in § 170.315(g)(10)(v). Specifically, we have finalized requirements for authentication and authorization for patient and user scopes in § 170.315(g)(10)(v)(A) and requirements for authentication and authorization for system scopes in § 170.315(g)(10)(v)(B). We have focused the revised requirements around authentication and authorization scopes to remove any confusion associated with requirements for single and multiple patients. We have finalized authentication and authorization requirements for first time connections for patient and user scopes in § 170.315(g)(10)(v)(A)(*1*). This include the requirement finalized in § 170.315(g)(10)(v)(A)(*1*)(*i*) that Health IT Modules presented for testing and certification must demonstrate that authentication and authorization occurs during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b). It also includes the requirement finalized in § 170.315(g)(10)(v)(A)(*1*)(*ii*) that an application capable of storing a client secret must be issued a refresh token valid for a period of no less than three months. Additionally, we have finalized authentication and authorization requirements for subsequent connections for patient and user scopes in § 170.315(g)(10)(v)(A)(*2*). This includes the requirements finalized in § 170.315(g)(10)(v)(A)(*2*)(*i*) that Health IT Modules presented for testing and certification must demonstrate that access is granted to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application. It also includes the requirements finalized in § 170.315(g)(10)(v)(A)(*2*)(*ii*) that an application capable of storing a client secret must be issued a new refresh token valid for a new period of no less than three months.

Additionally, we have finalized requirements for authentication and authorization for system scopes in § 170.315(g)(10)(v)(B), which require that Health IT Modules presented for testing and certification must demonstrate that authentication and authorization occurs during the process of granting an application access to patient data in accordance with the ''SMART Backend Services: Authorization Guide'' section of the implementation specification adopted in § 170.215(a)(4) and the application must be issued a valid access token. We note that for system scopes, applications will likely be authorized via a prior authorization negotiation and agreement between applications and Health IT Modules.

For clarity, we use the term ''an application capable of storing a client secret'' to refer to ''confidential clients.'' In the definition at RFC 6749, ''confidential'' clients are ''clients capable of maintaining the confidentiality of their credentials (*e.g.,* client implemented on a secure server with restricted access to the client credentials), or capable of secure client authentication using other means.'' RFC 6749 also defines ''public'' clients as ''clients incapable of maintaining the confidentiality of their credentials (*e.g.,* clients executing on the device used by the resource owner, such as an installed native application or a web browser-based application), and incapable of secure client authentication via any other means.'' We clarify that the term ''an application capable of storing a client secret'' specifically excludes ''public'' clients.

Additionally, we clarify that Health IT Modules will be explicitly tested for US Core IG operations using authentication and authorization tokens acquired via the process described in the implementation specification adopted in § 170.215(a)(3), and Health IT Modules will be explicitly tested for Bulk IG operations using authentication and authorization tokens acquired via the process described in the implementation specification adopted in § 170.215(a)(4).

Comments. One commenter recommended that ONC introduce a Condition of Certification requirement to ensure that implementers of § 170.315(g)(10)-certified Health IT Modules can obtain automated system-level access to all API calls from the API servers offered by the Certified Health IT Developers (*e.g.,* via the SMART Backend Services authorization guide), with ''system/*.*'' scopes.

Response. We decline to accept the recommendation to require ''system/*.*'' scopes as a certification requirement in § 170.315(g)(10). Insofar as the commenter requested that Health IT Modules make available automated system-level scopes for the purposes of an ''all information export,'' we have finalized a similar requirement in § 170.315(b)(10), and refer the commenter to that section for additional detail. Additionally, we have finalized in § 170.315(g)(10)(v)(B) that Health IT Modules must perform authentication and authorization during the process of granting an application access to patient data using system scopes in accordance with the ''SMART Backend Services: Authorization Guide'' section of the implementation specification adopted in § 170.215(a)(4). We recognize that the capabilities supported by ''SMART Backend Services: Authorization Guide'' could be used for many other use cases that are currently not required by the criterion. We clarify that implementers of Health IT Modules are not prohibited from configuring Health IT Modules to support the backend ''system'' scope described in the ''SMART Backend Services: Authorization Guide'' section of the Bulk IG adopted in § 170.215(a)(4) for API-enabled ''read'' services defined in the US Core IG. Indeed, we strongly encourage health IT developers to support these use cases as they develop in order to make full use of the certified functions of Health IT Modules and advance the state of the industry.

Comments. Commenters suggested specifying that refresh tokens apply exclusively to patient access scenarios, noting that there are too many security risks to allow persistent tokens for provider-facing applications.

Additionally, commenters suggested permitting Health IT Modules to support the revocation of refresh tokens in appropriate scenarios to address legitimate security concerns.

Response. We appreciate the feedback from commenters. We do not agree that there are too many security risks to allow refresh tokens to be used for provider-facing applications. Refresh tokens are commonly used in health care and other industries to provide seamless integration of systems with other applications while reducing the need for the burdensome process of re-authentication and re-authorization. We expect implementers of § 170.315(g)(10)-certified Health IT Modules to have the capability of revoking refresh tokens where appropriate. Additionally, we clarify that implementers of § 170.315(g)(10)-certified Health IT Modules are not prohibited from changing the length of refresh tokens for users of the API including patients and providers to align with their institutional policies. However, implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of information blocking provisions applicable to them and that requiring patients to re-authenticate and re-authorize at a high frequency could inhibit patient access and implicate information blocking.

Comments. Commenters suggested amending the time from three months to 12 months. One commenter agreed that the patient token should be valid for three months, but suggested the provider token be limited to 24 hours. One commenter suggested requiring re-authentication every time information is sought via APIs.

Response. We appreciate the feedback from commenters. We believe a refresh token valid for a period of three months is sufficient to balance persistent access and security concerns. Moreover, for subsequent connections of applications capable of storing a client secret, Health IT Modules are required to issue a new refresh token valid for a new period of no shorter than three months per the API certification criterion requirement finalized in § 170.315(g)(10)(v)(A)(*2*)(*ii*). Given this requirement, we anticipate that the user's application will renew its refresh token (valid for a new period of three months) every time the user actively engages with the application. We believe this justifies a refresh token length for a moderate period of no shorter than three months rather than a long period of 12 months suggested by commenters. Additionally, as stated above, implementers of § 170.315(g)(10)-certified Health IT Modules are not prohibited from changing the length of refresh tokens for users of the API, including patients and providers, to align with their institutional policies. Further, implementers of § 170.315(g)(10)-certified Health IT Modules are not prohibited from implementing their § 170.315(g)(10)-certified Health IT Modules in accordance with their organizational security policies and posture, including by instituting policies for re-authentication and re-authorization (*e.g.,* providers and/or patients could always be required to re-authenticate and re-authorize after a set number of refresh tokens have been issued). We also note that we have finalized a requirement in § 170.315(g)(10)(vi) that a Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction. This required capability will enable patients to definitively revoke an application's authorization to receive their EHI until reauthorized, if ever, by the patient.

Comments. Commenters suggested creating a more robust assessment process for identity management, including adding additional criteria for identity proofing, authentication, and authorization, and ensuring software developers do not act in a way that could inhibit patient control of their data.

Response. We appreciate the feedback and suggestions. Although we agree that identity proofing is an important practice, we did not include requirements for identity proofing in the Proposed Rule, and have not finalized requirements for identity proofing in response to this comment. We note that the certification criterion finalized in § 170.315(g)(10) only applies to health IT developers. Given the scope of the Program, we believe that mandating identity proofing, which are generally business practices performed by organizations and other entities, is not something appropriate to require of health IT developers. We note that per the requirements of the 2015 Edition Privacy and Security Certification Framework, health IT developers with Health IT Modules certified to § 170.315(g)(7) through (g)(10) are required to certify to § 170.315(d)(1), which includes requirements for authentication, access control, and authorization. Additionally, authentication and authorization for use of § 170.315(g)(10)-certified Health IT Modules are included in the requirements finalized in § 170.315(g)(10)(v). We appreciate the sentiment expressed by commenters, and have created thorough and rigorous requirements to ensure adequate privacy and security capabilities are present in § 170.315(g)(10)-certified Health IT Modules. Regarding the request for certification requirements to ensure that software developers do not act in a way that could inhibit patient control of their data, we refer to the requirement finalized in § 170.315(g)(10)(A), which requires that patients have the ability to grant applications authorization to access their EHI using granular FHIR Resources of their choice to comply with the adopted implementation specification in § 170.215(a)(3), and requirement in § 170.315(g)(10)(vi), which requires that a Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction.

Comments. Several commenters suggested that patients be able to specify refresh token length, if desired, and revoke a third-party application's access at any time. Commenters suggested that clear information be provided to patients whether authorized access is one-time or ongoing.

Response. We appreciate the feedback from commenters. Refresh tokens are an OAuth 2.0 concept, and are largely opaque to the end user. However, we clarify that patients are not prohibited from changing the length of refresh tokens to the degree this option is available to them. Additionally, pursuant to these comments, and to ensure patients have the ability to revoke an application's access to their EHI at any time, we have finalized an additional certification requirement in § 170.315(g)(10)(vi) which requires that a Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction. We have finalized this as a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop. Additionally, per the requirement finalized in § 170.315(g)(10)(v)(A), Health IT Modules must perform authorization conformant with the implementation specification adopted in § 170.215(a)(3), including all ''SMART on FHIR Core Capabilities.'' The ''permission-offline'' ''SMART on FHIR Core Capability'' includes support for the ''offline_access'' scope. Importantly, the implementation specification adopted in § 170.215(a)(3) requires that patients have the ability to explicitly enable the ''offline_access'' scope during authorization. If the ''offline_access'' scope is not enabled by patients, patients will be required to re-

authenticate and re-authorize an application's access to their EHI after the application's access token expires.

Comments. Commenters suggested providing the ability for implementers of § 170.315(g)(10)-certified Health IT Modules to perform token introspection using services enabled by health IT developers to ensure that additional resource servers can work with the same access tokens and authorization policies as the resource servers provided by API Technology Suppliers.

Response. We appreciate the feedback from commenters. Based on feedback, we have finalized in § 170.315(g)(10)(vii) that Health IT Modules presented for testing and certification must demonstrate the ability to receive and validate a token issued by its authorization server, but we did not specify a standard for this requirement. Token introspection will allow implementers of § 170.315(g)(10)-certified Health IT Modules to use API authorization servers and authorization tokens with various resource servers. This functionality has the potential to reduce complexity for implementers of § 170.315(g)(10)-certified Health IT Modules authorizing access to several resource servers and reduces the overall effort and subsequent use of § 170.315(g)(10)-certified Health IT Modules consistent with the goals of section 4002 of the Cures Act to enable the use of APIs without ''special effort.'' Although we do not specify a standard for token introspection, we encourage industry to coalesce around using a common standard, like OAuth 2.0 Token Introspection (RFC 7662).[105]

Comments. One commenter expressed concerns with the privacy and security of APIs, and nefarious actors posing as legitimate health facilities.

Response. Regarding the privacy and security of APIs, the Standardized API for Patient and Population Services certification criterion finalized in § 170.315(g)(10) requires Health IT Modules presented for testing and certification to implement the implementation specification adopted in § 170.215(a)(3), which is based on the OAuth 2.0 security standard that is widely used in industry. The implementation of OpenID Connect paired with OAuth 2.0 allows health care providers to securely deploy and manage APIs consistent with their organizational practices. Health care providers retain control over how their workforce and patients authenticate when interacting with the API. For example, a patient may be required to use the same credentials (*e.g.,* username and password) they created and use to access their EHI through a patient portal as they do when authorizing an application to access their data. Since patients complete the authentication process directly with their health care provider, no application will have access to their credentials. There is little protection software can provide to protect against nefarious actors posing as legitimate health facilities, however, we believe that implementing the security controls and safeguards described above, along with the privacy and security requirements required under the 2015 Edition Privacy and Security Certification Framework, will help to protect Health IT Modules against nefarious actors. Additionally, the protections required for ePHI in Health IT Modules offered by health IT developers acting as business associates of health care providers remain unchanged.

vi. Technical Documentation

We proposed in 84 FR 7484 in § 170.315(g)(10)(vii) that an API Technology Supplier needed to provide complete documentation via a publicly accessible hyperlink, without additional access requirements, for all aspects of its § 170.315(g)(10)-certified API, especially for any unique technical requirements and configurations, including API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns, the software components and configurations necessary for an application to successfully interact with the API and process its response(s), and all applicable technical requirements and attributes necessary for an application to be registered with an authorization server. Additionally, we proposed in 84 FR 7484 to remove the ''terms of use'' documentation provisions in the API certification criteria adopted in § 170.315(g)(7) through (g)(9) in order to reflect the Condition of Certification requirements and not be duplicative of the terms and conditions transparency Condition of Certification requirements proposed in 84 FR 7485.

Comments. Commenters generally supported the requirements for this criterion as proposed. Some commenters suggested technical documentation should be limited to descriptions of how the API differs from the utilized standards and implementation specifications, like HL7® FHIR® and the SMART IG.

Response. We appreciate the feedback from commenters. We did not make substantive changes to the requirements proposed in § 170.315(g)(10)(vii). We have finalized these requirements § 170.315(g)(10)(viii). We recognize that our formal adoption of the HL7 FHIR standard and the associated implementation specifications referenced in § 170.315(g)(10) would be consistent across all Health IT Modules presented for certification. As a result, there may be minimal additional documentation needed for these capabilities beyond what is already documented in adopted standards and implementation specifications. We expect health IT developers to disclose any additional data their § 170.315(g)(10)-certified Health IT Module supports in the context of the adopted standards and implementation specifications. The content of technical documentation required to meet this certification criteria are described in requirements finalized in § 170.315(g)(10)(viii)(A). We expect these and any additional documentation relevant to the use of a health IT developer's § 170.315(g)(10)-certified Health IT Module to be made available via a publicly accessible hyperlink without preconditions or additional steps to meet the requirement as finalized in § 170.315(g)(10)(viii)(B).

d. API Condition of Certification Requirements

i. Key Terms

We proposed in 84 FR 7477 to adopt new definitions for ''API Technology Supplier,'' ''API Data Provider,'' and ''API User'' in § 170.102 to describe the stakeholders relevant to our proposals.

Comments. The majority of commenters recommended updating definitions and providing examples for the key terms, including API User. Most commenters recommended dividing ''API User'' into two categories: ''First-Order Users,'' to include patients, health care providers, and payers that use apps/services that connect to API technology, and ''Third-Party Users,'' to include third-party software developers, and developers of software applications used by API Data Providers.

Response. We thank commenters for their feedback. We note that in this section we use the terms proposed in § 170.102 that we finalized in § 170.404(c) with added quotation marks for emphasis and clarity. We considered separating the term ''API User'' into distinct terms for developers of software applications and other users, such as patients and health care providers. However, we determined that this distinction was unnecessary from a regulatory perspective. Narrowing our

[105] *https://tools.ietf.org/html/rfc7662.*

definitions to distinct subgroups could exclude unforeseen stakeholders that emerge in a future API ecosystem. The term ''API User'' was intended to describe stakeholders that interact with the certified API technology either directly (*e.g.,* to develop third-party apps/services) or indirectly (*e.g.,* as a user of a third-party app/service).

Based on suggestions to revise the proposed key terms, we have renamed the term ''API Data Provider'' to ''API Information Source'' finalized in § 170.404(c) to make clear which party is the source and responsible for the EHI (as in ''the source of the information is the health care provider''), and ''API Technology Supplier'' to ''Certified API Developer'' finalized in § 170.404(c) to more clearly refer to health IT developers with Health IT Modules certified to any of the API criteria under the Program. Rather than keeping ''API technology'' an undefined term, we renamed it to ''certified API technology'' and finalized a definition in § 170.404(c). Additionally, we amended the definition of ''API User'' for clarity in § 170.404(c) to ''API User means a person or entity that creates or uses software applications that interact with the 'certified API technology' developed by a 'Certified API Developer' and deployed by an 'API Information Source.''' Additionally, we did not include the non-exhaustive list of examples of ''API User'' in the definition finalized in § 170.404(c). Instead, we rely on preamble to provide guidance for examples of ''API Users'' rather than appearing to limit the regulatory definition to these examples. We interpret that ''API Users'' can include, but are not limited to, software developers, patients, health care providers, and payers. We simplified the definition of ''API Information Source'' in § 170.404(c) to ''API Information Source means an organization that deploys 'certified API technology' created by a 'Certified API Developer.''' We revised the definition of ''Certified API Developer'' in § 170.404(c) to ''Certified API Developer means a health IT developer that creates the 'certified API technology' that is certified to any of the certification criteria adopted in § 170.315(g)(7) through (10).'' We added the definition of ''certified API technology'' in § 170.404(c) as ''certified API technology means the capabilities of Health IT Modules that are certified to any of the API-focused certification criteria adopted in § 170.315(g)(7) through (10).'' For ease of reference and to clarify that these terms only apply to the Condition and Maintenance of Certification requirements, we have finalized these revised definitions in § 170.404(c). In this and other sections of the rule, we use the original proposed terms in the proposal and comment summaries, and the finalized terms in our responses.

Comments. Some commenters suggested ONC allow flexibility for instances where stakeholders may meet the definition of more than one key term, and others recommended restricting stakeholders from meeting the definition of more than one key term. Commenters expressed concern with the complexity of key terms in the Proposed Rule, and confusion with the interaction of these terms with other criteria within the rule.

Response. We thank commenters for expressing their concern about stakeholders being able to serve more than one role under the definitions proposed in § 170.102 that we have finalized in § 170.404(c). We do not believe it is practical to restrict persons or entities to just one definition. We anticipate situations where a person or entity can serve more than one role. For example, a large health care system could purchase and deploy ''certified API technology'' as an ''API Information Source'' and have ''API Users'' on staff that create or use software applications that interact with the ''certified API technology.'' Additionally, a health IT developer could serve as a ''Certified API Developer'' that creates ''certified API technology'' for testing and certification and as an ''API User'' when it creates software applications that connect to ''certified API technology.'' We clarify that a stakeholder will meet a role defined in § 170.404(c) based on the context in which they are acting. For example, only health IT developers (when acting in the context of a ''Certified API Developer'') are required to comply with these API Condition and Maintenance of Certification requirements.

Comments. Commenters expressed concern that ONC exceeded its regulatory authority by implicating physicians in the definition of ''API Data Providers.''

Response. We remind commenters that these definitions were created to describe relationships between key API stakeholders and to help describe the Condition and Maintenance of Certification requirements. We clarify that health care providers are not covered by the Condition and Maintenance of Certification requirements to which the definitions apply in § 170.404(c) unless they are serving the role of a ''Certified API Developer.

ii. Scope and Compliance

We proposed in 84 FR 7485 that the Condition and Maintenance of Certification requirements proposed in § 170.404 apply to API Technology Suppliers with Health IT Modules certified to any API-focused certification criteria adopted in the proposed § 170.315(g)(7) through (11).

Comments. Commenters agreed that the proposed applicability for the Condition of Certification requirements proposed in § 170.404 should be limited to health IT developers certified to any API-focused criteria adopted in the proposed § 170.315(g)(7) through (11). One commenter requested clarification whether non-certified internally developed laboratory systems would be subject to this requirement.

Response. We thank stakeholders for their comments. We have generally finalized the scope and compliance for the Condition and Maintenance of Certification requirements as proposed in § 170.404 with one modification. Given that we have not adopted the certification criterion proposed for adoption in § 170.315(g)(11), the scope of the Condition and Maintenance of Certification requirements apply only to health IT developers with Health IT Modules certified to any of the API-focused criteria finalized in § 170.315(g)(7) through (10). The Condition and Maintenance of Certification requirements finalized in § 170.404 do not apply to health IT developers not seeking certification, nor do they apply to health IT developers certified to solely non-API-focused criteria. Additionally, we clarify that the Condition and Maintenance of Certification requirements only apply to practices of Certified API Developers with respect to the capabilities included in § 170.315(g)(7) through (10). In other words, the Condition and Maintenance of Certification requirements would not apply to practices of Certified API Developers with respect to non-certified capabilities or practices associated with, for example, the immunization reporting certification criterion in § 170.315(f)(1), because that criterion is not one of the API-focused criteria finalized in § 170.315(g)(7) through (10). However, health IT developers should understand that other requirements in this final rule, especially those related to information blocking, could still apply to its business practices associated with non-API-focused certification criteria.

iii. General

We proposed in 84 FR 7485 in § 170.404(a)(1) to adopt the Cures Act's

API Condition of Certification requirement stating that an API Technology Supplier must, through an API, ''provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.'' We then subsequently proposed in 84 FR 7485 to interpret ''all data of a patient's electronic health record'' for the purposes of the scope of this API Condition of Certification requirement to include the proposed ARCH standard, its associated implementation specifications, and the policy expressed around the data elements that must be supported by § 170.315(g)(10)-certified APIs.

Comments. Commenters supported our adoption of the Cures Act's API Condition of Certification requirement. For the purposes of the scope of data covered under this API Condition of Certification requirement, most commenters recommended defining ''all data elements'' as the Data Elements referenced by the USCDI and the FHIR resources in the FHIR US Core Implementation Guide STU 3 (US Core IG) for FHIR Release 4. We received comments recommending additional data elements to be included that we discuss in our comment summary for the ARCH in the ''API Standards, Implementation Specifications, and Certification Criterion'' section of this final rule.

Response. We appreciate stakeholder feedback. The § 170.315(g)(10) certification criterion requirement and associated standards and implementation specifications will enable secure, standards-based API access to a specific set of information. We have finalized that a Certified API Developer must publish APIs, and must allow EHI from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws, in § 170.404(a)(1). Additionally, for the purposes of meeting this portion of the Cures Act's API Condition of Certification requirement, we clarify the data required and that must be supported to demonstrate conformance to the final § 170.315(g)(10) certification criterion (including all of its associated standards and implementation specifications) constitutes ''all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.'' Regarding the recommendation by commenters that the scope of ''all data elements'' include the Data Elements of the standard adopted in § 170.213 and FHIR resources referenced by the implementation specification adopted in § 170.215(a)(2), we note that both the standard and implementation specification are included in the interpretation of ''all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws'' above. We note that this specific interpretation does not extend beyond the API Condition and Maintenance of Certification requirements finalized in § 170.404 and cannot be inferred to reduce the scope or applicability of other Cures Act Conditions of Certification or the information blocking policies, which include a larger scope of data.

iv. Transparency Conditions

We proposed in 85 FR 7485 and 7486 in § 170.404(a)(2)(i) to require API Technology Suppliers make available complete business and technical documentation via a publicly accessible hyperlink, including all terms and conditions for use of its API technology. Additionally, we proposed that API Technology Suppliers must make clear to the public the timing information applicable to their disclosures in order to prevent discrepancies between an API Technology Supplier's public documentation and its direct communication to customers. Additionally, we requested comment at 84 FR 7486 on whether the expectation for API Technology Suppliers to make necessary changes to transparency documentation should be finalized in regulation text, or whether this would be standard practice as part of making this documentation available.

Comments. We received overall support from commenters for the need to make complete business and technical documentation available via a publicly accessible hyperlink. We did not receive public comment on whether we should formally include public disclosure requirements for regular updates to business and technical documentation in regulatory text.

Response. We thank commenters for their support to make complete business and technical documentation available via a publicly accessible hyperlink. We have finalized in § 170.404(a)(2)(i) that a Certified API Developer must publish complete business and technical documentation, including the documentation described in § 170.404(a)(2)(ii), via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. We made small adjustments to § 170.404(a)(2)(i) to reflect the changes in API definitions finalized in § 170.404(c).

Given that we did not receive public comment on whether we should formally include public disclosure requirements for regular updates to business and technical documentation in regulatory text, so we have finalized in 170.404(a)(4)(iii)(B) that a Certified API Developer must provide notice and a reasonable opportunity for API Information Sources and API Users to update their applications to preserve compatibility with certified API technology and to comply with applicable terms and conditions. We note that notice could include a public notice made available on a website, but also encourage Certified API Developers to contact API Information Source customers and registered API Users (application developers) directly prior to updating business and technical documentation.

(A) Terms and Conditions

We proposed in 84 FR 7485 in § 170.404(a)(2)(ii)(A) that API Technology Suppliers must publish all terms and conditions for its API technology, including any restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to: Develop software applications to interact with the API technology; distribute, deploy, and enable the use of software applications in production environments that use the API technology; use software applications, including to access, exchange, and use EHI by means of the API technology; use any EHI obtained by means of the API technology; and register software applications. Additionally, we proposed in § 170.404(a)(2)(ii)(B) that any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language, including the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

Comments. We received support from stakeholders regarding the transparency of ''all terms and conditions'' associated with the use of API technology.

Response. We thank commenters for their support. We believe this terms and conditions transparency requirement would ensure that API Information Sources and API Users do not experience ''special effort'' in the form

of unnecessary costs or delays in obtaining the terms and conditions for certified API technology. Furthermore, we believe full transparency is necessary to ensure that API Users have a thorough understanding in advance of any terms or conditions that might apply to them once they have committed to developing software that interacts with certified API technology. We have finalized in § 170.404(a)(2)(ii)(A) that Certified API Developers must publish all terms and conditions for its certified API technology, including any fees, restrictions, limitations, obligations, registration process requirements or other similar requirements as enumerated in § 170.404(a)(2)(ii)(A)(*1*) through (*6*). We made small adjustments to § 170.404(a)(2)(ii)(A) to reflect the changes in API definitions finalized in § 170.404(c). Additionally, we moved ''App developer verification'' from its proposed location in § 170.404(a)(2)(ii)(C) and finalized it in § 170.404(b)(1) to improve organization. We added the phrase ''Used to verify the authenticity of API Users'' to the regulation text finalized in § 170.404(a)(2)(ii)(A)(*5*) for consistency with our proposed policy. We also moved the phrase ''Register software applications'' from its proposed location in § 170.404(a)(2)(ii)(A)(*5*) to the finalized location in § 170.404(a)(2)(ii)(A)(*6*) and revised the phrase for consistency. Additionally, we made small changes to the regulation text finalized in § 170.404(a)(2)(ii)(A)(*1*) through § 170.404(a)(2)(ii)(A)(*6*) for clarity.

Comments. We received both support and disagreement for the requirement to publish transparency documentation on API fees. Some commenters felt transparency documentation of API fees should be limited to value-added services, because those are the only permitted fees applicable to API Users, and the other permitted fees applicable to API Data Providers (usage-based fees and fees to recover costs for development, deployment, and upgrades) would be included in contractual documentation with their customers.

Response. We recognize that some commenters had concern with making documentation on permitted fees publicly available. We believe that transparent documentation of all permitted fees is necessary to maintain a competitive marketplace and ensure that fees are reasonably related to the development, deployment, upgrade, and use of certified API technology. Fee transparency will also enable API Information Sources and API Users to shop for certified API technology and related services that meet their needs. We have finalized in § 170.404(a)(2)(ii)(B) that any and all fees charged by a Certified API Developer for the use of its certified API technology must be described in detailed, plain language, including all material information described in § 170.404(a)(2)(ii)(B)(*1*) through (*3*). Additionally, we made small adjustments to § 170.404(a)(2)(ii)(B) to reflect the changes in API definitions finalized in § 170.404(c).

Comments. Multiple stakeholders expressed the need to include consumer protections in the terms and conditions documentation with an explanation about how EHI will be used.

Response. This provision of the Condition of Certification requirements does not prohibit additional content or limit the type of content a Certified API Developer may include in its terms and conditions. A Certified API Developer would be permitted to include consumer protections in their terms and conditions documentation. Additionally, we clarify these API Conditions of Certification requirements only apply to Certified API Developers. As such, API Information Sources and API Users are not required by the API Condition of Certification requirements to publish any terms and conditions, including those that apply to consumer protections.

v. Fees Conditions

(A) General Fees Prohibition

We proposed in § 170.404(a)(3)(i)(A) that API Technology Suppliers would be prohibited from imposing fees associated with API technology as a Condition of Certification requirement. In establishing this general prohibition, ONC was mindful of the need for API Technology Suppliers to recover their costs and to earn a reasonable return on their investments in providing API technology that has been certified under the Program. Accordingly, we identified categories of ''permitted fees'' in 84 FR 7487 that API Technology Suppliers would be permitted to charge and still be compliant with the Condition of Certification and Program requirements. These include the proposed § 170.404(a)(3)(ii) (permitted fee for developing, deploying, and upgrading API technology), proposed § 170.404(a)(3)(iii) (permitted fee to recover costs of supporting API usage for purposes other than patient access), and proposed § 170.404(a)(3)(iv) (permitted fee for value-added services). We also proposed in 84 FR 7487 that API Technology Suppliers would not be permitted to impose fees on any person in connection with an API Technology Supplier's work to support the use of API technology to facilitate a patient's ability to access, exchange, or use their EHI. We also clarified that while the proposed permitted fees set the boundaries for the fees API Technology Suppliers would be permitted to charge and to whom those permitted fees could be charged, the proposed regulations did not specify who could pay the API Technology Supplier's permitted fee. Rather, we proposed general conditions that an API Technology Supplier's permitted fees must satisfy in § 170.404(a)(3)(i)(B)(*1*) through (*4*), and requested comment in 84 FR 7488 on these conditions and whether they sufficiently restrict fees from being used to prevent access, exchange, and use of EHI through APIs without special effort. We include detailed discussions of permitted fees and related conditions below.

Comments. Some commenters supported the clear prohibition on API fees outside those fees permitted in § 170.404(a)(3)(ii) through (iv), expressing that the language in the rule would prevent confusion regarding allowable and restricted fees. Some commenters noted that prohibiting fees would enable patients to exercise their HIPAA right of access without experiencing cost barriers, and remove cost barriers to hospitals and health care facilities using APIs for interoperability. Commenters noted that the proposals addressed many of the access and pricing practices that API Technology Suppliers engaged in to limit data exchange and gain a competitive advantage. Commenters noted that API Technology Supplier pricing practices often create barriers to entry and competition for apps that health care providers seek to use. Some commenters supported the proposal that prohibits API Technology Suppliers from charging fees to API Users.

Response. We thank stakeholders for their support of and feedback on our proposal. We have finalized in § 170.404(a)(3)(i)(A) that all fees related to certified API technology not otherwise permitted by § 170.404(a)(3) are prohibited from being imposed by a Certified API Developer. Additionally, we have modified and reorganized these Condition of Certification requirements for clarity. We have renamed the title for the section from the Proposed Rule to ''Fees conditions'' because the requirements include both permitted and prohibited fees. We have updated the terminology used in this section to reflect changes made to the terminology used throughout the API Condition of

Certification requirements and finalized in § 170.404(c). We finalized a requirement in § 170.404(a)(3)(i)(A) that permitted fees in paragraphs § 170.404(a)(3)(ii) and § 170.404(a)(3)(iv) may include fees that result in a reasonable profit margin in accordance with the information blocking Costs Exception provision finalized in § 170.302. We clarify that any fee that is not covered by those exceptions would be suspect under the information blocking provision, and would equally not be permitted by this API Condition of Certification requirement.

This general prohibition on fees as finalized in § 170.404(a)(3)(i)(A) is meant to ensure that Certified API Developers do not engage in pricing practices that create barriers to entry and competition for apps and API-based services that health care providers seek to use. Such activities are inconsistent with the goal of enabling API-based access, exchange, and use of EHI by patients and other stakeholders without special effort. As finalized, this general prohibition allows for three categories of permitted fees (§ 170.404(a)(3)(ii) through (iv)) to allow Certified API Developers to recover their costs and to earn a reasonable return on their investments in providing certified API technology while being compliant with the Condition of Certification and Program requirements.

Comments. Some commenters were critical of our proposals, expressing concerns that the proposed policies may stifle relationships between API Technology Suppliers and application developers. Others expressed concern that the proposed fee structure would place undue burden on API Data Providers, and that ONC should instead consider regulations that allow fee sharing across stakeholders. Some commenters stated that ONC should remove all prohibitions, and allow for market pricing and revenue sharing.

Several commenters, many of whom were providers and provider organizations, requested additional clarity and guidance regarding the API fees that can be charged under the Condition of Certification requirements. Some commenters requested clarification regarding whether an API Data Provider can transfer costs to API Users. Other commenters requested clarification regarding when it is (and is not) appropriate for an API User to be charged a fee in connection with use of API technology. A few commenters requested that ONC provide a chart that lists all actors, all types of costs, and who can charge whom.

Response. We appreciate this feedback from commenters. These ''general conditions,'' as finalized in § 170.404(a)(3)(i) and discussed above, will facilitate API-based access, exchange, and use of EHI by patients and other stakeholders without special effort. We disagree with commenters that the permitted fee policies will stifle relationships between Certified API Developers and API Users. Cumulatively, these final policies create guardrails to protect against anti-competitive practices and reinforce the independence that we believe API Information Sources should have to establish relationships with API Users. Furthermore, we believe these fee policies are necessary in light of the potential for Certified API Developers to use their market position and control over certified API technology to engage in discriminatory practices that create special effort and barriers to the use of certified API technology. We continue to receive evidence that some Certified API Developers are engaging in practices that create special effort for the use of certified API technology. These practices include fees that create barriers to entry or competition as well as rent-seeking and other opportunistic behaviors. For example, we have received feedback that some Certified API Developers are conditioning access to technical documentation on revenue sharing or royalty agreements that bear no plausible relation to the costs incurred by the Certified API Developer to provide or enable the use of certified API technology. We are also aware of discriminatory pricing policies that have the purpose or effect of excluding competitors from the use of APIs and other interoperability elements despite the fact that the API Information Source would like to partner with and use these competitive, best-of-breed services. These practices from Certified API Developers close off the market to innovative applications and services that could empower patients and enable providers to deliver greater value and choice to health care consumers and other service providers.

We note that Certified API Developers and API Users have the ability to collaborate and form relationships, so long as these relationships do not conflict with any of the provisions of this final rule or other applicable Federal and State laws and regulations. Further, we clarify that while the permitted fees set the boundaries for the fees Certified API Developers are permitted to charge and to whom those permitted fees can be charged, they do not prohibit who may pay the Certified API Developer's permitted fee. In other words, these conditions limit the party from which a Certified API Developer may require payment, but they do not speak to who may pay the fee. For example, a permitted practice under these conditions could include a relationship or agreement where an API User or other party offered to pay the fee owed by the API Information Source to a Certified API Developer. This is an acceptable practice because the fee is first agreed upon between the Certified API Developer and API Information Source and subsequently paid by the API Information Source directly or by a third party on behalf of the API Information Source. We note that fees charged for ''value-added services'' can arise between an API Information Source and Certified API Developer or API User. As a general matter, we note that stakeholders should be mindful of other Federal and State laws and regulations that could prohibit or limit certain types of relationships involving remuneration.

We provide additional clarity and guidance regarding the API fees that can be charged under the Condition of Certification requirements in the sections that follow. Additionally, we appreciate commenters' requests for clarification, including a chart of actors and costs. We will take this comment into consideration as we develop educational materials to help explain the permitted fees conditions finalized in § 170.404(a)(3).

Comments. Commenters suggested that one way to clarify the limits on API fees would be to require API Technology Suppliers provide fee information to ONC and for ONC to make this information publicly available, including information on individual pricing transactions.

Response. We appreciate the recommendation from commenters to require Certified API Developers to provide fee information to ONC. We view fee transparency as a responsibility that a Certified API Developer can fulfill without having to send a listing of its API fees to ONC. We have finalized the provision in § 170.404(a)(2)(ii) that a Certified API Developer must publish all terms and conditions for its certified API technology, including any fees. Specifically, we have finalized in § 170.404(a)(2)(ii)(B) that any and all fees charged by a Certified API Developer for the use of its certified API technology must be described in detailed plain language, including the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variable(s) and

methodology(ies) that will be used to calculate the fee.

(B) Certified API Developer Permitted Fees Conditions

We proposed general conditions in § 170.404(a)(3)(i)(B)(*1*) through (*4*) that an API Technology Supplier's permitted fees must satisfy in order for such fees to be expressly permitted.

Comments. We received support for the general conditions for permitted fees from commenters. Some commenters expressed appreciation for the guardrails and transparency of the permitted fees. Under the first condition, commenters sought clarity on the nature and extent of some of the permissible fees an API Technology Supplier can charge and how to model such fees, specifically regarding the ''objective and verifiable'' criteria. Another commenter supported the second condition that fees must be reasonably related to API Technology Supplier's costs of supplying and, if applicable, supporting the API technology to the API Data Provider, especially in situations where physicians may also develop APIs or support apps.

However, some commenters expressed concern with the third condition to reasonably allocate fees across all customers of the API. Commenters explained that fees could not be reasonably allocated across all customers of the API, because the number of customers will change over time. We received no comments on the fourth condition that API Technology Suppliers must ensure that fees are not based on whether the requestor or other person is a competitor who will be using the API technology in a way that facilitates competition. In addition to the general permitted fees proposed, some commenters recommended clear fee exemption for any health information provided or reported by a practice for the purpose of meeting reporting requirements.

Response. We appreciate feedback from commenters. We have finalized these general conditions for permitted fees in § 170.404(a)(3)(i)(B) with some modifications as described further below. We have finalized that for all permitted fees, a Certified API Developer must: (1) Ensure that such fees are based on objective and verifiable criteria that are uniformly applied to all similarly situated API Information Sources and API Users; (2) Ensure that such fees imposed on API Information Sources are reasonably related to the Certified API Developer's costs of supplying certified API technology to, and if applicable, support certified API technology for, API Information Sources; (3) Ensure that such fees for supplying, and if applicable, supporting certified API technology are reasonably allocated among all similarly situated API Information Sources; and (4) Ensure that such fees are not based on whether API Information Sources or API Users are competitors, potential competitors, or will be using the certified API technology in a way that facilitates competition with the Certified API Developer. We have revised the term ''substantially similar'' to ''similarly situated'' in § 170.404(a)(3)(i)(B)(*1*) for clarity and to align with changes made in § 171.302. Additionally, in response to comments and to align with changes made in § 171.302 and § 170.404(a)(3)(i)(B)(*1*), we have revised the term ''substantially similar'' to ''similarly situated'' in § 170.404(a)(3)(i)(B)(*3*). We emphasize that this provision is meant to prevent one customer or a specific group of customers to whom the certified API technology is supplied or for whom it is supported from bearing an unreasonably high cost compared to other customers, which could lead to ''special effort'' for accessing and using APIs. We believe the final policy achieves the same goal as proposed and provides clearer guidelines for the regulated community to follow. Additionally, we have revised the phrase ''classes of persons and requests'' to ''API Information Sources and API Users'' in § 170.404(a)(3)(i)(B)(*1*) to clearly express the actors being charged fees by Certified API Developers. Additionally, we have revised the sentence structure and grammar in § 170.404(a)(3)(i)(B)(*2*) through (*4*) for simplification.

In response to comments requesting clarity on the nature and extent of permissible fees a Certified API Developer can charge and how a Certified API Developer should model such fees, specifically regarding the ''objective and verifiable'' requirement finalized in § 170.404(a)(3)(i)(B)(*1*), we emphasize that there will be significant variability in the fee models and specific fees charged by each Certified API Developer. Our goal with the requirement that fees be ''objective and verifiable'' is to require Certified API Developers to apply fee criteria that, among other things, will lead the Certified API Developer to come to the same conclusion with respect to the permitted fee's amount each time it administers a fee to an API Information Source or API User. Accordingly, the fee cannot be based on the Certified API Developer's subjective judgment or discretion.

Comments. A few commenters suggested that ONC allow API Data Providers the ability to recoup the costs for upgrading technology.

Response. This comment appears to misunderstand the scope and applicability of ONC's authority with respect to these Condition of Certification requirements. We clarify that these Condition of Certification requirements apply only to Certified API Developers. We note that similar to any IT investment, API Information Sources (as ''health care providers'') would generally be expected to recover these costs through fees administered while delivering health care services. Additionally, if an API Information Source were to recoup such costs they would need to do so consistent with the information blocking exceptions and other applicable laws and regulations.

Comments. Some commenters requested that ONC conduct evaluations after the implementation of the rule and use the results to drive future policy. Some commenters recommended a study to evaluate the real-world cost of APIs used by health systems in areas such as clinical decision support, payments, machine learning, and precision medicine. Commenters also suggested ONC conduct a study on whether these regulations improve patient access to their EHI.

Response. We appreciate the evaluation recommendations. We will consider these suggestions as we implement and administer the Program.

(C) Certified API Developer Prohibited Fees

We proposed in 84 FR 7595 in § 170.404(a)(3)(iii)(B) that permitted fees would not include costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets. Additionally, we proposed in § 170.404(a)(3)(iii)(C) that permitted fees would not include opportunity costs, except for the reasonable forward-looking cost of capital.

Comments. We did not receive any comments specific to the proposal for costs associated with intangible assets other than actual development or acquisition costs of such assets.

Response. We moved the proposed § 170.404(a)(3)(iii)(B) and (C) to the general conditions for permitted fees finalized in § 170.404(a)(3)(i)(C)(*1*) and (*2*), respectively, because they are general conditions on permitted fees rather than conditions for ''Recovering API usage costs.'' We did not make

other changes to the proposed regulation text in these two sections other than updating terms to the finalized definitions in § 170.404(c).

Additionally, in the discussion of the Fees Exception in this final rule (VIII.D.2.b), we discussed that one commenter expressed concern that the overlap between the Fees Exception and the Licensing Exception creates the potential for actors to recover the same costs twice. The commenter explained that licensing of IP is intended to recoup the costs of development of that IP, so where the IP is an interoperability element, the costs reasonably incurred for its development should be incorporated into the royalty rate. The commenter recommended that we be clearer that, in these circumstances, only a single recovery is permitted. In order to address this comment and align the API permitted fees with related provisions finalized in the Fees Exception (§ 170.302(a)(2)(vi)) and Licensing Exception (§ 170.303(b)(2)(iv)), we have added and finalized § 170.404(a)(3)(i)(C)(*3*), which states that the permitted fees in this section cannot include any costs that that led to the creation of IP if the actor charged a royalty for that IP pursuant to § 170.303 and that royalty included the development costs for the creation of the IP. We refer readers to the ''Basis for Fees Condition'' sub-section within section VIII.D.2.b for a more detailed discussion of the rationale for this addition.

(i) General Examples of Prohibited Fees

As discussed in the Proposed Rule in 84 FR 7481 and finalized in § 170.404(a)(3)(i)(A), any API-related fee imposed by a Certified API Developer that is not expressly permitted is prohibited. In the Proposed Rule, we provided the following non-exhaustive examples of fees for services that Certified API Developers would be prohibited from charging, and reiterate them here in the final rule for clarity:

(1) Any fee for access to the documentation that a Certified API Developer is required to publish or make available under this Condition of Certification requirement.

(2) Any fee for access to other types of documentation or information that a software developer may reasonably require to make effective use of certified API technology for any legally permissible purpose.

(3) Any fee in connection with any services that would be essential to a developer or other person's ability to develop and commercially distribute production-ready applications that use certified API technology. These services could include, for example, access to ''test environments'' and other resources that an application developer would need to efficiently design and develop apps. The services could also include access to distribution channels if they are necessary to deploy production-ready software and to production resources, such as the information needed to connect to certified API technology (*e.g.,* service base URLs) or the ability to dynamically register with an authorization server.

Comments. At least one commenter expressed concern about the open-ended nature of the examples of prohibited fees we provided in the Proposed Rule. In particular, that any fee in connection with any services that would be essential to a developer or other person's ability to develop and commercially distribute production-ready applications that use API technology would be prohibited. They stated that if the example were not more clearly defined and scoped, it could be used by API Users to create requirements for API Technology Suppliers beyond what would normally be considered necessary to successfully deploy apps in production. They requested ONC more clearly define ''essential services'' in final rulemaking or withdraw the reference.

Response. We appreciate the feedback from commenters. We disagree with commenters that the examples are too broad. We believe that in some cases they need to be general because of the diverse and varied practices that could be used by Certified API Developers to create special effort to use certified API technology. While we understand that the generality of the example regarding ''essential services'' may at first appear difficult for Certified API Developers to follow and, per the commenter, could be creatively used by an API User to request more support than necessary, we offer the following as additional guidance: A Certified API Developer is best positioned to know what an API User, for example, needs to have access to and do programmatically in order for the API User's application to be developed and commercially distributed as production-ready for use with certified API technology. From a Certified API Developer's perspective, if that requires any number of mandatory steps (*e.g.,* passing tests in sandbox/test environment, conducting a demo, submitting documentation or paperwork) in order for the application to be production-ready for use with certified API technology, then fees associated with those mandatory steps are prohibited. Conversely, fees for requirements beyond what a Certified API Developer considers necessary to successfully deploy applications in production are considered supplemental to the development, testing, and deployment of software applications that interact with certified API technology, and are permitted fees for value added services as finalized in § 170.404(a)(3)(iv).

(D) Record-Keeping Requirements

We proposed in § 170.404(a)(3)(v) that API Technology Suppliers must keep for inspection detailed records of all API technology fees charged, all costs incurred to provide API technology to API Data Providers, methodologies used to calculate such fees, and the specific costs to which such fees are attributed. We requested comment in 84 FR 7492 on whether these requirements provide adequate traceability and accountability for costs permitted under this API Condition of Certification and whether to require more detailed accounting records or prescribe specific accounting standards.

Comments. A majority of commenters expressed concerns with the level of granularity proposed for record keeping in § 170.404(a)(3)(v). These commenters stated that the required recordkeeping would exceed documentation performed for any other purpose. Some commenters stated that the requirement for health IT developers to track who pays fees and how fees enter the system will cause significant administrative burden, especially on smaller vendors or vendors with business models that require less operational overhead. Additionally, they stated that the requirement for clients to maintain and potentially publicly disclose records of fees for inspection would place a burden on IT providers, and could potentially allow bigger companies to engage in practices such as predatory pricing. Commenters suggested ONC have a more scaled-back method, and simply allow patients the ability to access their EHI without charge. These commenters recommended focusing on a good conduct approach rather than prescriptive requirements.

Response. We thank commenters for their feedback and perspective. We moved § 170.404(a)(3)(v) to 170.404(a)(3)(i)(D) for better organization because this provision applies to the permitted fee Condition of Certification requirements finalized in § 170.404(a)(3)(ii) through (iii). We have finalized in § 170.404(a)(3)(i)(D) that Certified API Developers must keep detailed records for inspection of all fees charged, all costs incurred to provide certified API technology to API Information Sources, methodologies

used to calculate such fees, and the specific costs to which fees are attributed. Considering the feedback on perceived burden, we believe transparency and documentation of API fees is necessary to mitigate unfair pricing practices that may stifle innovation or otherwise create barriers to the goals of enabling API-based access, exchange, and use of EHI without special effort. Further, we believe that the accounting practices already used by health IT developers will largely support the health IT developer to meet this requirement. Examples of these practices by health IT developers include the methods used to track their own investments, determine how to bill and issue invoices to their customers, document receipt of payment, and to maintain overall accurate financial records of business transactions. We find it difficult to believe, as some commenters appeared to indicate, that health IT developers are not already keeping such financial records and that this requirement would create substantial new documentation burden for Certified API Developers. The record-keeping requirements finalized in 170.404(a)(3)(i)(D) foster transparency and promote accountability in the Program. In response to the comments received, we have not added additional requirements for accounting records or standards.

(E) Permitted Fee for Development, Deployment, and Upgrades

We proposed in § 170.404(a)(3)(ii) to permit an API Technology Supplier to charge API Data Providers reasonable fees for developing, deploying, and upgrading Health IT Modules certified to § 170.315(g)(7) through (g)(11).

Comments. Many commenters applauded the permitted fee related to development, deployment, and upgrading API technology. The majority supported the proposal that fees would not be permitted if they interfere with an API User's ability to efficiently and effectively develop and deploy production-ready software. A few commenters expressed concern that our proposals regarding development, deployment, and upgrade fees were not restrictive enough. Commenters noted that API Technology Suppliers will use the allowable fees, such as for program upgrades, as a barrier to providing interoperability between systems or other applications and a means to eliminate competitive threats. Some of these commenters recommended that ONC explicitly prohibit API Technology Suppliers from charging any fees for implementing APIs and for facilitating the interoperable exchange of EHI and that this blanket prohibition apply to all new and updated API technology. A few commenters noted that it is possible that API Technology Suppliers will bundle or upcharge service fees to recoup API technology development costs and API Technology Suppliers should not be allowed to charge costs for development or impose surcharges for product feature development. They noted that product feature development should be considered a cost of doing business and can be amortized as a one-time capital expense across the vendor's entire customer base without the need for recovering costs from API Users. They emphasized that API access and use prices need to be transparent as the intent of Congress was to have APIs be made easily available and at no or low cost, not to be a source of revenue for profit. Other commenters noted that the development of the APIs themselves should be regarded as part of the license fee and the API Technology Suppliers should not be permitted to charge an additional license fee to either the API Data Provider or API User for what is an inherent part of the software. Another commenter requested that consideration be applied toward potential additional hidden integration fees.

Response. We appreciate the support, concerns, and recommendations from commenters. We finalized this proposal in § 170.404(a)(3)(ii) as proposed with updated terms based on the revised finalized definitions in § 170.404(c). We refer to the discussions below and 84 FR 7488 for additional details on what Certified API Developer fees for ''developing,'' ''deploying,'' and ''upgrading'' certified API technology comprise. We also note that the nature of the costs charged under this category of permitted fees depends on the scope of the work to be undertaken by a Certified API Developer (*i.e.,* how much or how little labor an API Information Source requires of the Certified API Developer to deploy and upgrade the certified API technology).

We sincerely thank commenters for the various recommendations to prohibit or restrict fees regarding certified API technology. In order to reconcile the recommendations specific to § 170.404(a)(3)(ii) and other conditions in this final rule, we have aligned related conditions to address concerns and mitigate potential fee practices that could limit API-based access, exchange, and use of EHI by patients and other stakeholders without special effort. As finalized, we believe the fees permitted in § 170.404(a)(3)(ii) and § 170.404(a)(3)(i)(B), transparency requirements in § 170.404(a)(2), and openness and pro-competitive conditions in § 170.404(a)(4) will ensure that fees permitted for upgrade costs will not be used as a barrier to providing interoperability between systems or other applications, or as a means to eliminate competitive threats. Additionally, the transparency requirements regarding the publication of fees finalized in § 170.404(a)(2)(ii)(B) will help prevent hidden integration fees cited by commenters.

We thank commenters for recommending and noting that development of the APIs themselves should be regarded as part of a license fee and that Certified API Developers should not be permitted to charge an additional license fee for what is an inherent part of the software. In response to this recommendation, we have added a provision in § 170.404(a)(3)(i)(C)(*3*) that states that permitted fees in § 170.404(a)(3)(ii) through (iv) may not include any costs that led to the creation of IP, if the actor charged a royalty for that IP pursuant to the information blocking Licensing Exception (§ 171.303). This provision aligns with similar provisions included in the information blocking section and will ensure that Certified API Developers cannot earn a double recovery in instances described by the commenter.

We will continue to work with stakeholders to advance policies that promote interoperability and deter practices that may stifle innovation or present barriers to the access, exchange, and use of EHI through APIs. Subject to the general conditions in § 170.404(a)(3)(i), our final policies support the ability of Certified API Developers to recover the full range of reasonable costs associated with developing, deploying, and upgrading API technology over time. It is important that Certified API Developers be able to recover these costs and earn a reasonable return on their investments so that they have adequate incentives to make continued investments in these technologies. In particular, we anticipate Certified API Developers will need to continually expand the data elements and upgrade the capabilities associated with certified APIs as the USCDI and HL7® FHIR® standard and associated implementation specifications mature. We refer readers to the information blocking section of this preamble (VIII) for additional information on activities that may constitute information blocking and for discussion about how the fees provisions in this Condition of Certification and within the information blocking section support innovation.

Comments. Some developers expressed concern regarding balancing and distributing costs with regard to the permitted fee for developing, deploying, and upgrading technology. The commenters noted ONC proposed that the cost for development be distributed among those who will use it, which they felt was problematic in many ways, but most fundamentally because it suggests a serious misconception about how software development is funded, priced, and sold. The commenters emphasized that requiring development costs to be divided among clients purchasing the API necessitates new and complex business processes and creates unsolvable scenarios that could easily create business conflicts between API Technology Suppliers and their clients. At least one commenter suggested that ONC should consider balancing the costs associated with API development and deployment across both API Data Providers and certain API Users to ensure that third-party software application developers also bear some of the financial burden, since they stand to generate revenue from the use of their apps. Commenters asked ONC clarify why it believes it is inappropriate to pass development, deployment, and upgrade costs on to API Users. Other commenters noted that the costs for updating information systems and Health IT Modules to the new standards and requirements should not be passed on to physicians and patients.

Response. We appreciate the feedback from commenters. We proposed and finalized this permitted fee for development, deployment, and upgrade costs because we believe that these costs should be negotiated solely between the Certified API Developer that supplies the capabilities and the API Information Source that implements them in their production environment. In our view, it is inappropriate for Certified API Developers to go around the API Information Source to directly impose financial cost burdens on API Users for the benefit of working with or connecting to the API Information Source. Based on our experience, the practice of a Certified API Developer going around its customer (the API Information Source) to also charge API Users erodes an API Information Source's choice and the independence of their relationship with API Users. As such, that kind of business practice would be something that we would consider creating special effort on the part of the API Users if they had to continue to face additional fees just for permission to work with or connect to an API Information Source's certified API technology.

While the development, deployment, and upgrade permitted fee is limited between the Certified API Developer and API Information Source as a way to recoup a Certified API Developer's costs to supply certified API technology to a particular API Information Source, we again reiterate that the value added services permitted fee providers Certified API Developers a wide range of options to make additional revenue related to their certified API technology.

Should API Users stand to generate revenue from the use of their apps, any fee an API Information Source may impose would not be in scope for this Condition of Certification but would be likely be covered by information blocking. Accordingly, we emphasize that such stakeholders should take care to ensure they are compliant with other Federal and State laws and regulations that may prohibit or limit certain types of relationships involving remuneration.

In response to comments suggesting that costs for updating information systems and Health IT Modules to the new standards and requirements would be passed on to physicians and patients, we disagree. We emphasize that most of the information contained in a patient's electronic record has been documented during the practice of medicine or has otherwise been captured in the course of providing health care services to patients. In our view, patients have effectively paid for this information, either directly or through their employers, health plans, and other entities that negotiate and purchase health care items and services on their behalf, and should be able to access the information via certified API technology without fees.

Comments. Some developers suggested that API Technology Suppliers should be able to charge fees for access to a test environment and requested clarification as to whether an API Technology Supplier can charge for the use of sandboxes by API Users.

Response. We appreciate the feedback from commenters. As detailed in the ''General Examples of Prohibited Fees'' section of the preamble text and included in the general prohibition finalized in § 170.404(a)(3)(i)(A), Certified API Developers are prohibited from charging fees in connection with any services essential to a developer or other person's ability to develop and commercially distribute production-ready applications for use with certified API technology. In general, if a test environment or sandbox is required to be used by a Certified API Developer and is essential for an application to be developed in order to be considered production-ready by the Certified API Developer for use with its certified API technology, then fees associated with that kind of test environment would be prohibited as they would impose special effort. However, we note that this prohibition is not globally applicable. If instead, the purpose of the testing environment was to provide specific testing above-and-beyond production-readiness for use with certified API technology, then fees could be charged for such testing as part of the value-added services permitted fee.

Comments. A few commenters requested guidance on how ONC expects API Technology Suppliers to account for the costs incurred to develop, deploy, and upgrade the API technology, which is part of, and not necessarily separable from, the broader EHR product. Several commenters opposed the prohibition against charging for work to upgrade the broader EHR product, expressing that this is essential work needed to modernize their solutions as broader technologies evolve. One commenter noted that the Proposed Rule does not set specific guidelines on what constitutes an upgrade or how much the fee could be, and it is the commenter's experience that EHR systems often charge fees for such services as integrating with a clinical data registry or using outside or non-preferred software.

Response. We thank stakeholders for their comments. While we understand that there is overlap between features of the certified API technology and the ''broader EHR product,'' we refer specifically to development, deployment, and upgrades made to ''certified API technology'' as defined in § 170.404(c). Namely, development, deployment, and upgrades made to the capabilities of certified Health IT Modules that fulfill the API-focused certification criteria adopted at § 170.315(g)(7) through (10). In response to commenters concerned that EHR developers often charge fees for services such as integrating with a clinical data registry or using outside or non-preferred software, we note that, as described in § 170.404(a)(3)(i)(A), Certified API Developers are prohibited from imposing fees associated with certified API technology unless included as a permitted fee in § 170.404(a)(3)(ii) through (iv). We do not include specific price information for permitted fees to develop, deploy, or upgrade API technology, because these costs are subject to change over time with new technology and varying development, deployment, and upgrade

efforts. Instead, we allow Certified API Developers to recover their costs (including costs that result in a reasonable profit margin for permitted fees in § 170.404(a)(3)(ii) and § 170.404(a)(3)(iv)) in providing certified API technology while being compliant with the Condition and Maintenance of Certification and Program requirements. We include descriptions of fees for developing, deploying, and upgrading API technology in the sections that follow, in which we offer additional clarity, as discussed in the Proposed Rule at 84 FR 7488, on the fees for developing, deploying, and updating API technology.

(i) Fees for Developing Certified API Technology

Fees for ''developing'' certified API technology comprise the Certified API Developer's costs of designing, developing, and testing certified API technology. In keeping with our discussion at 84 FR 7488, fees for developing certified API technology must not include the Certified API Developer's costs of updating the non-API related capabilities of the Certified API Developer's existing Health IT Modules, including its databases, as part of its development of the certified API technology. As we further discussed in 84 FR 7488 in our Proposed Rule, these costs are connected to past business decisions made by the Certified API Developer and typically arise due to Health IT Modules being designed or implemented in nonstandard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI. The recovery of costs associated with updating a Certified API Developer's non-API related Health IT Modules capabilities would be inconsistent with the Cures Act requirement that API technology be deployed ''without special effort.''

(ii) Fees for Deploying Certified API Technology

Certified API Developer's fees for ''deploying'' certified API technology comprise the Certified API Developer's costs of operationalizing certified API technology in a production environment. Such fees include, but are not limited to, standing up hosting infrastructure, software installation and configuration, and the creation and maintenance of API Information Source administrative functions. We discussed in our Proposed Rule that a Certified API Developer's fees for ''deploying'' certified API technology does not include the costs associated with managing the traffic of API calls that are used to access the certified API technology, which a Certified API Developer can only recover under the permitted fee for usage support costs (§ 170.404(a)(3)(iii)). We emphasize that for the purpose of this Condition of Certification, we consider that certified API technology is ''deployed'' by the customer—the API Information Source—that purchased or licensed it.

(iii) Fees for Upgrading Certified API Technology

The Certified API Developer's fees for ''upgrading'' certified API technology comprise the Certified API Developer's costs of supplying an API Information Source with an updated version of certified API technology. Such costs would include the costs required to bring certified API technology into conformity with new requirements of the Program, upgrades to implement general software updates (not otherwise covered by development fees or under warranty), or developing and releasing newer versions of the certified API technology at the request of an API Information Source. The nature of the costs that can be charged under this category of permitted fees depends on the scope of the work undertaken by a Certified API Developer (*i.e.,* how much or how little labor an API Information Source requires of the Certified API Developer to upgrade the certified API technology being supplied from one version or set of functions to the next).

(F) Permitted Fee to Recover Costs of Supporting API Usage

We proposed in 84 FR 7489 in § 170.404(a)(3)(iii) to permit an API Technology Supplier to charge API usage-based fees to API Data Providers to recover the API Technology Supplier's reasonable incremental costs for purposes other than facilitating the access, exchange, or use of EHI by patients or their applications, technologies, or services. We considered ''usage-based'' fees to be the fees imposed by an API Technology Supplier to recover the costs that would typically be incurred supporting API interactions at increasing volumes and scale within established service levels. Additionally, in 84 FR 7489 under § 170.404(a)(3)(iii), we proposed that any usage-based fees associated with API technology be limited to the recovery of the API Technology Supplier's ''incremental costs.'' Additionally, we proposed in § 170.404(a)(3)(iii)(A) that the permitted fee would not include any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their EHI. Finally, we proposed in § 170.404(a)(3)(iii)(B)–(C) restrictions for permitted fees that were moved to the general permitted fees section finalized in § 170.404(a)(3)(i)(C).

Comments. Commenters generally supported our proposal to permit an API Technology Suppliers to charge usage-based fees to API Data Providers to the extent that the API technology is used for purposes other than facilitating the access, exchange, or use of EHI by patients or their applications, technologies, or services.

Response. We appreciate support from commenters and have finalized this proposal in § 170.404(a)(3)(iii) with some modification. We amended the title of the regulation text for clarity in § 170.404(a)(3)(iii) to ''Permitted fee—Recovering API usage costs.'' Additionally, we amended the regulation text to focus on usage-based fees and Certified API Developer's reasonable incremental costs. We did not finalize the specific prohibition on permitted fees proposed in § 170.404(a)(3)(iii)(A) that the ''permitted fee does not include costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use electronic health information.'' We did not finalize this aspect of the provision because upon further consideration of this cost and the fee prohibition included in information blocking related to patient access, we determined that these fees remain necessary in order to allow Certified API Developers to recover incremental costs reasonably incurred during the process of hosting certified API technology on behalf of the API Information Source. We reiterate that a Certified API Developer's ''incremental costs'' comprise the Certified API Developer's costs that are directly attributable to supporting API interactions at increasing volumes and scale within established service levels. A Certified API Developer should ''price'' its costs of supporting access to the certified API technology by reference to the additional costs that the Certified API Developer would incur in supporting certain volumes of API use. For comments and responses related to the proposed provisions in § 170.404(a)(3)(iii)(B) and (C), we refer readers to the header ''Certified API Developer Prohibited Fees.''

Comments. We received a few comments focused on volume thresholds and incremental costs. A few commenters supported a reasonable cap for API call fees. Several recommended changing the parameters around API usage-based fees to focus on volume

thresholds being included in any contractual language related to these fees, to ensure that any incremental costs attributable to supporting API interactions at increasing volumes and scale are addressed appropriately. Commenters noted that if an API Technology Supplier is receiving fees to develop, deploy, and upgrade API technology, it is unlikely that they would also need to charge for usage of the APIs, as long as their usage remains under a pre-determined volume threshold. A few commenters noted that the volume of requests that will be pinging APIs may compromise the performance of data retrieval and effective user experience. In order to protect against denial of service attacks whether intentional or inadvertent, they stated ONC should consider an additional throttling or rate-limiting layer or capability onto the API in order for the API to accept and digest the data being entered or extracted. A few commenters noted that our proposal could create loopholes that would enable certain organizations to charge highly burdensome, excessive fees to clinical registries to access their data.

A few commenters expressed concern that this proposal is not restrictive enough. Some commenters requested that ONC provide more definitive guidance, including a range of prices based on examples from the current marketplace, to ensure providers are not charged unreasonable fees by API Technology Suppliers and can reasonably charge API Users for the cost of accessing their API technology.

Response. We appreciate the feedback from commenters. This Condition of Certification requirement offers the flexibility necessary to accommodate reasonable pricing methodologies and will allow Certified API Developers to explore innovative approaches to recovering the costs associated with supporting the use of certified API technology with a permitted fee. As described in the Proposed Rule (84 FR 7489), ''usage-based'' fees are fees imposed by a Certified API Developer to recover costs typically incurred for supporting API interactions at increasing volumes and scale within established service levels. That is, ''usage-based'' fees recover costs incurred by a Certified API Developer due to the actual use of the certified API technology once it has been deployed (*e.g.,* costs to support a higher volume of traffic, data, or number of apps via the certified API technology). Certified API Developers can adopt a range of pricing methodologies when charging for the support of API usage. We appreciate commenters' request to establish a reasonable cap for API usage-based fees, but the focus of our policy is to identify usage fees as a type of permitted fee and not to dictate a singular fee model, which we believe could limit Certified API Developers ability to create innovative fee models that serve to benefit themselves and API Information Sources. We decline to include a price cap for API usage-based fees or a range of prices for API fees based on examples from the current marketplace because we anticipate the cost of technology will change over time and so too will the way in which usage costs are calculated. Additionally, while we understand and expect that Certified API Developers and API Information Sources will deploy particular security methods to mitigate the risk of denial of service attacks and other impacts on API availability, these types of technology layers are separate from the focus of our policy on permitted API usage fees.

Comments. Several commenters requested that ONC further clarify that API Technology Suppliers should not attempt to charge different fees for different API transactions as they frequently do today.

Response. We appreciate this information and feedback from commenters. We clarify that Certified API Developers are permitted to charge ''usage-based'' fees to recover the costs that would typically be incurred supporting API transactions at increasing volumes and scale within established service levels. To clarify, usage-based fees recover costs incurred by a Certified API Developer related to the actual use of certified API technology once it has been deployed (*e.g.,* costs to support a higher volume of traffic, data, or number of apps via the API Technology). We acknowledge that Certified API Developers could adopt a range of pricing methodologies when charging for the support of API usage, including potentially charging higher prices for some API transactions that incur relatively higher costs than others. However, in combination with this flexibility, Certified API Developers will still need to be mindful of not violating any overarching information blocking policies. We refer readers to a discussion in the Proposed Rule in 84 FR 7489 for additional discussions on usage-based fees.

Comments. Some commenters emphasized that it is unreasonable to presume that API User-driven data overages should be the responsibility of the API Data Provider. While other commenters expressed concern that our proposal will leave providers, who are mandated to use certified EHRs that include API technology and provide patients with access to data via those APIs, responsible for a variety of unwarranted costs with little recourse to recover those costs.

Response. While we understand the perspective from which these concerns arise, especially regarding unpredictable overuse of certified API technology, an API Information Source has financial responsibility for its overall technology infrastructure. This accountability is no different for certified API technology than it is for non-certified APIs and other interfaces that may also create costs for the API Information Source (*i.e.,* health care provider). Given that API Users can also include an API Information Source's own employees/internal tools and 3rd party partners' tools, an API Information Source is best positioned and generally accountable for its financial commitments. Again, as noted above, we do not limit who may pay for the charges an API Information Source incurs. An API Information Source should have full knowledge and ability to assess what employees, internal applications, and 3rd party services it has granted access to use and interact with its certified API technology. With respect to potential overages as a result of patient access, as we have stated before, we believe patients have effectively paid for this information, either directly or through their employers, health plans, and other entities that negotiate and purchase health care items and services on their behalf, and believe they should not be charged.

Additionally, as stated in the Proposed Rule (84 FR 7489) and finalized here, usage fees for certified API technology will only apply when the Certified API Developer acts on behalf of the API Information Source to deploy its certified API technology. In scenarios where the API Information Source, such as a large hospital system, assumes full responsibility for the technical infrastructure necessary to deploy and host the certified API technology it has acquired, the volume and scale of its usage would be the API Information Source's sole responsibility, and a Certified API Developer would not be permitted to charge usage-based fees. Instead, the Certified API Developer would be limited to charge fees under the ''development, deployment, upgrade'' permitted fee in § 170.404(a)(3)(ii). Additionally, the costs recovered under ''usage-based'' fees can only reflect ''post-deployment'' costs. As such, ''usage-based'' fees cannot include any costs necessary to prepare and ''get the certified API technology up, running, and ready for use,'' which are costs that must be

recovered as part of the deployment services delivered by the Certified API Developer if permitted under § 170.404(a)(3)(ii).

Comments. Several commenters supported ONC's efforts to bolster patient access, noting that the capacity to offer a patient's access to all elements of their electronic medical record, through an API, without cost, is well-supported in the Proposed Rule. One commenter noted that the proposed provisions regarding fees supports uses of the API technology that facilitate a patient's ability to access, exchange, or use their EHI. The commenters noted that the clear language in the Proposed Rule will prevent any potential confusion or friction in the future.

A few commenters expressed concern that application developers will attempt to leverage the patient access fee limitations by claiming to be patient facing. One commenter suggested that the proposed fee limitations regarding patient access applied only with respect to fees API Technology Providers impose on API Data Providers, should also apply to fees charged to consumer-facing application developers who in the past have been charged high fees by CEHRT developers. One commenter recommended making it clear that provider organizations and health IT developers cannot charge patients, or the apps that they use, for using patient-facing APIs. At least one commenter requested that ONC clarify that permitted usage-based fees do not apply to patients or patient designees.

Response. We thank commenters for their support for restricting API-related fees. As noted above, we have reconfigured the permitted fee for usage costs in response to public comments and our assessment of the intersection of API permitted fees policies and information blocking policies. We have finalized an approach that permits Certified API Developers to recover incremental usage costs reasonably incurred during the process of hosting certified API technology on behalf of an API Information Source, which could include fees to the API Information Source for providing and supporting patient access. However, the Certified API Developers and API Information Sources cannot recover these costs from patients or the developers of applications that facilitate access to and receipt of patients' EHI. Patients have already effectively paid for their EHI, either directly or through their employers, health plans, and other entities that negotiate and purchase health care items and services on their behalf. We refer readers to the Fees Exception in the information blocking section of this final rule in VII.D.2.b, which applies to health IT developers and a broader set of actors than these Condition and Maintenance of Certification requirements, for a discussion of the restrictions on charging patients for access to their EHI.

Comments. Several commenters requested that ONC provide further guidance on the types of costs that a developer could charge to permit API Data Suppliers to offer population-level queries to API Users. They requested ONC clarify that such usages fees must relate to the costs associated with actual hardware (*e.g.,* server space) needed to support the increased volume of queries for non-patients and not the cost of implementing the population-level query functionality itself.

Response. We clarify that API usage fees related to API ''read'' services for multiple patients would be calculated using a similar methodology to calculate API usage fees related to API ''read'' services for single patients. These ''usage-based'' fees are fees imposed by a Certified API Developer to recover the costs typically incurred to support API interactions for API ''read'' services for multiple patients once these services have been deployed. This could include, but not be limited to, costs to support a higher volume of traffic, data, or number of apps via the certified API technology (which could include higher costs for hardware, including server space). We appreciate the recommendation from commenters; however, we have not prescribed the centralization of all of this content.

Comments. Some commenters suggested that API Technology Suppliers publish their fees on the same website as their API documentation so there is full transparency and an API Data Supplier and API User can easily understand costs before embarking upon development.

Response. We appreciate the recommendation and support from commenters. As finalized under § 170.404(a)(2)(ii)(B), a Certified API Developer must publish all terms and conditions for its certified API technology, including any fees. Any and all fees charged by a Certified API Developer for the use of its certified API technology must be described in detailed, plain language, including the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

Comments. Some commenters stated that usage-based fees may not be appropriate. They stated that, in the case of TEFCA, HIEs and providers must be responsive to inbound requests to broadcast data and should not be charged a fee for responding to such requests. They explained that such an arrangement could be used maliciously between market participants seeking to increase the operational expenses of their competitors.

Response. We appreciate this comment, but we continue to believe that that usage-based fees should be permitted subject to the conditions described in § 170.404(a)(3)(iii). We have addressed commenter's concern regarding potential anticompetitive behavior through the final provisions in § 170.404(a)(3)(i)(B). Specifically, in § 170.404(a)(3)(i)(B)(*1*), a Certified API Developer must ensure that fees are based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons and requests. In addition, under § 170.404(a)(3)(i)(B)(*4*), a Certified API Developer must ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the certified API technology in a way that facilitates competition with the Certified API Developer.

Comments. Several commenters expressed concern about incremental costs that can be recovered by actors supporting the use of APIs for purposes other than patient access. They requested ONC clarify that recovery of incremental costs for these other purposes should not be allowed, because they believed the incremental costs do not add any efficiency to the health care system, do not benefit patients, and do not serve any other procompetitive purpose.

Response. We appreciate these comments, but continue to believe that ''incremental costs'' should be allowed. A Certified API Developer's ''incremental costs'' comprise the Certified API Developer's costs that are directly attributable to supporting API interactions at increasing volumes and scale within established service levels. We believe a Certified API Developer should ''price'' its costs of supporting access to the certified API technology by reference to the additional costs that the Certified API Developer would incur in supporting certain volumes of API use. In practice, we expect that this means that a Certified API Developer will offer a certain number of ''free'' API calls based on the fact that, up to a certain threshold, the Certified API Developer will not incur any material costs in supporting certified API technology in addition to the costs recovered for

deployment services. However, after this threshold is exceeded, we expect that the Certified API Developer will impose usage-based costs commensurate to the additional costs that the Certified API Developer must incur to support certified API technology use at increasing volumes and scale.

We expect that Certified API Developers will charge fees that are correlated to the incremental rising of costs required to meet increased demand. For example, if, at a certain volume of API calls, the Certified API Developer needed to deploy additional server capacity, the associated incremental cost of bringing an additional server online could be passed on to the API Information Source because the certified API technology deployed on behalf of the API Information Source was the subject of the higher usage. In this example, up until the point that the threshold is reached, the additional server capacity is not required, so the Certified API Developer would not be permitted to recover the costs associated with it. Moreover, the additional server capacity would support ongoing demand up to a certain additional volume, so the Certified API Developer would not be permitted to recover the costs of further additional server capacity until the existing capacity was exhausted.

(G) Permitted Fee for Value-Added Services

We proposed in 84 FR 7490 and 7491 in § 170.404(a)(3)(iv) to permit an API Technology Supplier to charge fees to API Users for value-added services supplied in connection with software that can interact with the API technology. We also clarified in 84 FR 7491 that a fee will only be permitted if it relates to a service that an API User, such as a software developer, can elect to purchase, but is not required to purchase in order to develop and deploy production-ready apps for API technology.

Comments. Several commenters supported our proposal to permit an API Technology Supplier to charge fees to API Users for value-added services supplied in connection with software that can interact with certified API technology. Some commenters requested certain clarifications regarding our proposal. One commenter requested that we clarify within the discussion of value-added services, that references to ''app stores'' and ''listing processes'' for software applications that register to connect with the API technology are solely intended as examples to illustrate when a fee would or would not qualify as a ''value-added service,'' and are not meant to convey a requirement or expectation that API Technology Suppliers provide an app store with application listing free of charge. A few commenters requested that ONC clarify that EHR developers can charge value-add fees without triggering the information blocking provision. A couple other commenters requested additional examples of what constitutes a ''value-added'' service for which an API Technology Supplier can charge fees to an API User.

Response. We thank commenters for the feedback. We have finalized § 170.404(a)(3)(iv) as proposed, with the exception of updating terms based on the definitions finalized in § 170.404(c). Our final policy permits Certified API Developers to charge fees, including a reasonable profit margin, to API Users for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology. We clarify that the value-added services need to be provided in connection with and supplemental to the development, testing, and deployment of production-ready software applications that interact with certified API technology. A fee is permitted if it relates to a service that a software developer can elect to purchase from a Certified API Developer, but is not required to purchase in order to develop and deploy production-ready apps for certified API technology.

In response to comments for clarity, we note that examples used to illustrate when a fee would or would not qualify as a ''value-added service,'' such as app store listing, are demonstrative, but not required unless otherwise noted in the regulation text. Under this condition, we permit fees for services associated with the listing and promotion of apps beyond basic application placement so long as the Certified API Developer ensures that basic access and listing in the app store is provided free of charge (if an application developer depended on such listing to efficiently and effectively develop and deploy production-ready apps for use with certified API technology). Fees charged for additional/specialized technical support or promotion of the API User's application beyond basic access and listing services would be examples of permitted value-added services. We caution health IT developers not to over-interpret the scope of this Condition of Certification, which is focused on certified API technology. To the degree that a health IT developer administers an ''app store'' and offers value-added services associated with certified API technology, the Condition of Certification covers its practices related to certified API technology only. Conversely, this Condition of Certification would not apply to any practices that do not involve certified API technology. However, health IT developers would need to be mindful of any applicable information blocking rules that may apply to their app store practices given applicable facts and circumstances. Regarding the request for specific value-added fees that would not constitute information blocking, we refer readers to the information blocking section (VIII) of this preamble.

(H) Request for Comment on § 170.404(a)(3)

We requested comment at 84 FR 7491 on any additional specific ''permitted fees'' not addressed in our Proposed Rule (84 FR 7491) that commenters felt API Technology Suppliers should be able to recover in order to assure a reasonable return on investment. Furthermore, we requested comment on whether it would be prudent to adopt specific, or more granular, cost methodologies for the calculation of the permitted fees. We encouraged commenters to consider, in particular, whether the approach we described would be administrable and appropriately balance the need to ensure that stakeholders do not encounter unnecessary costs and other special effort with the need to provide adequate assurance to API Technology Suppliers, investors, and innovators that they will earn a reasonable return on their investments in API technology. We welcomed comments on whether the approach adequately balances these concerns and achieves our stated policy goals. We also welcomed comments on potential revisions or alternative approaches. We encouraged detailed comments that included, where possible, economic justifications for suggested revisions or alternative approaches.

Comments. Commenters suggested we alter our approach to APIs so that it is tiered fee structure. They suggested that ONC could establish categories where the technology requirements designate the fees: (1) A ''no fee'' category would limit API Technology Suppliers from charging API Data Providers or API Users any fees for exchanging data in compliance with Federal requirements; (2) an ''at cost'' category would allow API Technology Suppliers to charge API Data Providers or API Users the cost of interfacing APIs with a non-API Technology Supplier's commercial technology; and (3) a ''cost plus reasonable profit'' category would allow

API Technology Suppliers to charge API Data Providers or API Users a reasonable profit when conducting legitimate custom API development or creating custom apps.

Response. We appreciate the recommendation from commenters, but we have not adopted a tiered fee structure in the final rule because it would require unnecessary specificity and prescribe a particular method that could have unintended effects of limiting the market's evolution over time. We believe the current structure for prohibited and permitted fees allows for the adequate cost recovery and reasonable profit by Certified API Developers while also establishing the guardrails around which API access can be enabled without special effort.

Comments. Many commenters expressed concerns related to the effect our proposals regarding API fees would have on innovation and business. Several commenters noted that the structure of permitted fees could have unintended consequences that will ultimately work to impede innovation, increase administrative burden, and focus on cost recovery rather than creation of novel ways to improve data access.

Several developers stated that the proposed fee structure specifically works to sever business relationships between API Technology Providers and API Users for anything other than ''value added services'' and effectively eliminates the ability for API Users to work directly with API Technology Suppliers to innovate and accelerate API development, and to achieve truly integrated and supported products throughout the product lifecycle. They suggested that a better model would be one that gives API Data Providers rights to leverage APIs ''without special effort,'' while supporting the ability for API Technology Suppliers and API Users to voluntarily engage in direct business relationships under mutually agreeable terms that are fair and equitable. Some developers stated that the market should determine permitted fees. They stated that in order to maintain a vigorously competitive market, API Technology Suppliers must be adequately compensated for their work to create and deploy non-standard APIs and support expanding standards. They explained that without this compensation, there will be far fewer entrants into the certified health IT space and current participants will depart.

A couple of developers recommended that ONC allow revenue-sharing models for certain components of certified APIs. The commenters suggested that ONC should view revenue sharing arrangements as a type of market-based compensation that will ultimately benefit innovation and competition. Conversely, one commenter stated that it is essential that API Technology Suppliers be expressly prohibited from conditioning access to API technology on charging revenue-sharing or royalty agreements to API Data Providers or API Users outside of actual usage costs incurred. The commenter noted this rent-seeking behavior is anti-competitive in nature and can have a significant impact on squelching any new market entrants and allow existing health IT actors to prevent all the positive outcomes that could arise from the ONC's proposed rules. Some developers stated that the prohibition against health IT developers charging for work to update their code structure is unreasonable, emphasizing that this is important work that is necessary for companies to be able to modernize their solutions as broader technologies evolve.

Response. We appreciate these comments, but disagree with commenters regarding the potential negative effect of the final permitted fee structure on innovation. We also note that the value-added services permitted fee does permit a direct relationship between Certified API Developers and API Users. What is generally prohibited and what we noted presented ''special effort'' in the Proposed Rule were Certified API Developer practices that required an API Information Source to seek permission to use its own certified API technology from the Certified API Developer.

We reiterate that complying with the requirements of this permitted fee and the information blocking exception will generally *not* prevent an actor from making a reasonable profit in connection with the access, exchange, or use of EHI. To be responsive to comments, we have added a provision in § 171.404(a)(3)(i)(A) to clarify this point. This final provision states that certain permitted API fees (§ 170.404(a)(3)(ii) and § 170.404(a)(3)(iv)) may include fees that result in a reasonable profit margin in accordance with the Costs Exception (§ 171.302). We believe that the allowance of reasonable profits is necessary to incentivize innovation and allow innovators to earn returns on the investments they have made to develop, maintain, and update innovations that ultimately improve health care delivery and benefit patients. Our finalized approach to API fees strikes the appropriate balance of addressing the rent-seeking and exclusionary pricing practices noted by the commenters while enabling and supporting innovation.

We also emphasize that a majority of the EHI has been generated and recorded in the course of furnishing health care services paid with public dollars through Federal programs, including Medicare and Medicaid, or directly subsidized through the tax preferences for employer-based insurance. Yet, this EHI is not readily available where and when it is needed. We believe the overwhelming benefits of publishing certified APIs that allow EHI from such technology to be accessed, exchanged, and used without special effort far outweigh the potential burden on Certified API Developers and API Information Sources.

Comments. A few commenters requested that ONC clarify whether API Data Suppliers would be allowed to recoup costs from API Users in light of the information blocking provisions. A few commenters expressed confusion that fees are addressed under the API Condition and Maintenance of Certification and information blocking. The commenters suggested that ONC address fees in one consolidated section.

Response. We appreciate this comment and refer readers to the information blocking section of this rule. We do not believe that a discussion of fees should be consolidated in one section for a couple of reasons. First, the information blocking provision has a much broader reach than the Condition and Maintenance of Certification requirements and regulates conduct of health IT developers of certified Health IT Modules, health care providers, health information networks, and health information exchanges. The Condition and Maintenance of Certification requirements only relate to conduct by health IT developers of certified Health IT Modules. Second, the API Condition of Certification covers a much narrower scope of potential fees, as the fees in this section are specific to certified API technology only while fees in the information blocking section generally relate to the access, exchange, or use of EHI regardless of the particular technology used.

We emphasize that we have finalized a provision in § 171.302(c) that if the actor is a health IT developer subject to the Condition of Certification requirements in § 170.402(a)(4) (Assurances), § 170.404 (API), or both, the actor must comply with all requirements of such conditions for all practices and at all relevant times. Under this provision, health IT developers of certified Health IT

Modules subject to the API Condition of Certification requirements may not charge certain types of fees and are subject to more specific cost accountability provisions than apply generally under the Costs Exception. We explain in the Costs Exception that a failure of developers to comply with these additional requirements would impose impediments to consumer and other stakeholder access to EHI without special effort and would be suspect under the information blocking provision.

vi. Openness and Pro-Competitive Conditions

We proposed in 84 FR 7595 in § 170.404(a)(4) that an API Technology Supplier must grant API Data Providers the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider in a non-discriminatory manner; provide all reasonably necessary support and other services to enable the effective development, deployment, and use of API technology by API Data Providers and its API Users to access, exchange, and use EHI in production environments; not impose collateral terms or agreements that could interfere with the use of API technology; and provide reasonable notice prior to making changes to its API technology or terms and conditions.

Comments. The majority of commenters supported the proposed openness and pro-competitive conditions. Several commenters requested clarification about API Data Providers' rights and responsibilities when providing access to an application of a patient's choice. Specifically, they sought clarification on whether they can vet, deny, or limit access by applications that are using the API technology inappropriately. Another commenter proposed that app developers be required to obtain a business associate agreement (BAA) with providers prior to the application developer gaining access to a patient's EHI on behalf of a patient.

Response. We appreciate the feedback from commenters. Based on the support from commenters, we have finalized that a Certified API Developer must grant API Information Sources the independent ability to permit API Users to interact with the certified API technology deployed by the API Information Source in § 170.404(a)(4).

Under the HIPAA Privacy Rule, a business associate relationship exists if an entity creates, receives, maintains, or transmits ePHI on behalf of a covered entity (directly or through another business associate) to carry out the covered functions of the covered entity. HIPAA does not require a covered entity (*e.g.,* API Information Source) or its business associate (*e.g.,* API Technology Supplier) to enter into a business associate agreement with an app developer that does not create, receive, maintain, or transmit ePHI on behalf of or for the benefit of the covered entity (whether directly or through another business associate). However, if the app was developed to create, receive, maintain, or transmit ePHI on behalf of the covered entity (API Information Source), or was provided by or on behalf of the covered entity (directly or through its API Technology Supplier, acting as the covered entity's business associate), then a business associate agreement would be required.[106] In such cases, API Information Sources have the ability to conduct whatever ''vetting'' they deem necessary of entities (*e.g.,* app developers) that would be their business associates under the HIPAA Rules before granting access and use of EHI to the entities. In this regard, covered entities must conduct necessary vetting in order to comply with the HIPAA Security Rule.

For third-party applications chosen by individuals to facilitate their access to their EHI held by actors, there would not be a need for a BAA as discussed above. There would also generally not be a need for ''vetting'' on security grounds and such vetting actions otherwise would be an interference. Please see our discussion of ''vetting'' in the ''*Interference Versus Education When an Individual Chooses Technology to Facilitate Access*'' discussion in the Information Blocking section of the preamble (Section VIII). We also refer readers to our discussion of ''vetting'' versus verifying an app developer's authenticity under the API Condition of Certification later in this section of the preamble.

Comments. Several commenters requested clarification about the types of business relationships permitted between API Technology Suppliers and API Users and requested examples of permitted activities and responsibilities under each role. These comments expressed concern about prohibiting API Technology Suppliers from being able to form direct relationships with API Users for the purpose of joint development and commercialization of their products. Other commenters requested clarifications about relationships that existed prior to the involvement of an API Data Provider.

Response. We appreciate the feedback from commenters. Based on the general support, we have finalized in § 170.404(a)(4)(i)(A) that a Certified API Developer must provide certified API technology to API Information Sources on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship. Additionally, we have finalized in § 170.404(a)(4)(i)(B) that the terms on which a Certified API Developer provides certified API technology must be based on objective and verifiable criteria that are uniformly applied to all substantially similar or similarly situated classes of persons and requests. Furthermore, we have finalized in § 170.404(a)(4)(i)(C) that a Certified API Developer must not offer different terms or services on the basis of: Competition or potential for competition and revenue or other value the other party receiving the services may receive from using the certified API technology. We note that we slightly modified the finalized requirements in § 170.404(a)(4)(i) based on the revised definitions finalized in § 170.404(c). We clarify that this rule does not prohibit Certified API Developers from forming business relationships with API Users. To the degree that a Certified API Developer seeks to charge an API User for particular services associated with its certified API technology, it would need to do so pursuant to the ''value-added services'' permitted fee.

Comments. Commenters requested clarification about how ''the sole authority and autonomy to unilaterally permit connections to their health IT through certified API technology'' applies to application registration. Specifically, they asked whether API Users are required to register once with the API Technology Supplier, or several times with each instance of API technology deployed by API Data Providers.

Response. We appreciate the feedback from commenters. We refer commenters to § 170.315(g)(10)(iii) for the application registration requirements for Health IT Modules presented for certification. In general, we do not prescribe the registration paradigm that Certified API Developers create for themselves and their customers. Thus, in different scenarios, an API User may only be required to register once with an Certified API Developer, or several times with each instance of a § 170.315(g)(10)-certified Health IT Module deployed by an API Information Source. When it comes to apps that focus on the ''launch-ehr'' ''SMART on FHIR Core Capability'' from the

[106] *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html.*

implementation specification adopted in 170.215(a)(3), such an approach will be tightly integrated with the Health IT Modules deployed by API Information Sources. Because of the tight integration between API Information Sources and Health IT Modules, registration for these apps could more often fall to the API Information Source. When it comes to apps that enable patient access, registration could be handled centrally by Certified API Developers or in a distributed manner with each API Information Source, especially in cases where API Information Sources take full responsibility for administering their § 170.315(g)(10)-certified Health IT Modules.

Regarding ''the sole authority and autonomy to unilaterally permit connections to their health IT through certified API technology,'' we have finalized in 170.404(a)(4)(ii)(A) that Certified API Developer must have and, upon request, must grant to API Information Sources and API Users all rights that may be reasonably necessary to (1) access and use certified API technology in a production environment; (2) develop products and services that are designed to interact with the Certified API Developer's API technology; and (3) market, offer, and distribute products and services associated with the Certified API Developer's certified API technology.

Additionally, we have finalized in § 170.404(a)(4)(ii)(B) that a Certified API Developer must not condition any of the rights described in § 170.404(a)(4)(ii)(A) on: (1) Receiving a fee, including but not limited to a license fee, royalty, or revenue-sharing arrangement; (2) agreeing to not compete; (3) agreeing to deal exclusively with the Certified API Developer; (4) Obtaining additional services that are not related to the certified API technology; (5) sharing intellectual property with the Certified API Developer; (6) meeting any Certified API Developer-specific testing or certification requirements; and (7) providing the Certified API Developer or technology with reciprocal access to application data. We slightly modified the conditions from the Proposed Rule for what we finalized in § 170.404(a)(4)(ii)(B) for clarity, and amended terms to the revised definitions finalized in § 170.404(c). Additionally, we clarify that while Certified API Developers are not permitted to condition the rights described in § 170.404(a)(4)(ii)(A) on receiving a fee, Certified API Developers are permitted to charge fees compliant with the permitted fees described in § 170.404(a)(3). We also clarify that ''meeting any Certified API Developer-specific testing or certification requirements'' would include preconditions like registering and testing in a testing environment prior to moving to production, and meeting Certified API Developer-created certification requirements.

Comments. Commenters expressed concern about software applications maintaining compatibility when upgrading API technology, and highlighted the importance of adopting backwards-compatible standards.

Response. We appreciate the feedback from commenters. We share the concern expressed by commenters. We specifically consider features of standards like backwards compatibility when proposing and finalizing testing and certification requirements for the Program. As mentioned above, we have finalized the standard adopted in § 170.215(a)(1) as the base standard for the certification criterion adopted in § 170.315(g)(10) Standardized API for Patient and Population Services. We note that the standard adopted in § 170.215(a)(1) includes many FHIR resources that need to retain their compatibility over time, which will help as upgrades to newer standards occur. Additionally, we have finalized in § 170.404(a)(4)(iii) the service and support obligations required by a Certified API Developer, including the requirements that a Certified API Developer must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of certified API technology by API Information Sources and API Users in production environments. These include requirements for changes and updates to API technology finalized in § 170.404(a)(4)(iii)(A), where Certified API Developers must make reasonable efforts to maintain the compatibility of its certified API technology and to otherwise avoid disrupting the use of certified API technology in production environments, and requirements for changes to terms and conditions finalized in § 170.404(a)(4)(iii)(B), where Certified API Developers must provide notice and reasonable opportunity for its API Information Source customers and registered API Users to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

e. API Maintenance of Certification Requirements

i. Authenticity Verification

We proposed in 84 FR 7486 in § 170.404(a)(2)(ii)(C) to permit API Technology Suppliers to verify the authenticity of application developers, limited to a duration of no greater than five business days of receipt of a request to register an application developer's software with the API technology. We noted the authenticity verification process would need to be objective, apply to the application developer and not their software, and be the same for all application developers. We sought comment in 84 FR 7486 on factors that would enable registration with minimal barriers, including options and associated trade-offs. Additionally, we sought comment at 84 FR 7486 on other timing considerations for application developer authenticity verification.

Comments. Commenters asked for a longer timeframe to complete the authenticity verification process of application developers. Some commenters asked to extend the authenticity verification timeframe to ten business days. Commenters suggested adding ''and any receipt of any additional requested information needed in order to verify the developer's authenticity'' to ''within five business days of receipt of an application developer's request to register their software application with the API technology provider's authorization server.''

Commenters suggested various methods for verifying the authenticity of application developers and applications, including by proposing required registration information, or required attestation to model privacy guidelines or industry best practices. Other commenters suggested various approaches for verifying application developers and applications, including by working with industry to establish a verification body, privacy and security trust or certification framework, and other more detailed recommendations. Several commenters suggested requiring application developers to attest to providing a model privacy notice to patients. Commenters suggested mandating terms and conditions and consent requirements as part of the registration process.

Response. We appreciate feedback from commenters. To improve the organization of these Condition and Maintenance of Certification requirements, we moved the requirements proposed in § 170.404(a)(2)(ii)(C) to the finalized § 170.404(b)(1)(i) under the combined § 170.404(b)(1), ''Authenticity verification and registration for production use.'' We accept commenters' requests to establish a longer time period for this permitted, but not required, process to verify the authenticity of application developers

who seek to register their software application for use with the Certified API Developer's certified API technology. We have adopted ten business days as the timeframe by which this process would need to be completed and as a result find it unnecessary to add the text contemplating a back and forth between the Certified API Developer and API User. We recommend that Certified API Developers who elect to institute a verification process implement a process that is as automated as possible to ensure they remain in compliance with our final policy. Given that we combined authenticity verification and registration for production use in one requirement finalized in § 170.404(b)(1), we reduced the scope of these requirements to Certified API Developers with a Health IT Module certified to the certification criterion adopted in § 170.315(g)(10) to remain consistent with the scope of applicability of registration for production use from the Proposed Rule.

We also note that authenticity verifications would likely occur more frequently for patient-facing applications that are not sponsored by API Information Sources. We anticipate that an API Information Source (*e.g.,* a health care organization) that is a HIPAA covered entity would vet and enter into a HIPAA business associate agreement with a provider-facing application developer prior to using the application within their internal technical enterprise. In comparison, a patient-facing application is likely to connect to an API Information Source's resource server using a public service base URL of a § 170.315(g)(10)-certified Health IT Module in service to the patient's HIPAA Privacy Rule right of access (45 CFR 164.524) or based on a patient's HIPAA authorization (45 CFR 164.508) without first establishing a relationship with the API Information Source. For patient-facing applications, and to the comments suggesting we require various modes of attestation to privacy guidelines in such contexts, we refer commenters to the information blocking provisions in section VIII for a discussion of permitted behaviors regarding privacy attestations.

Comments. Commenters suggested including a warning by the API Data Provider that the application developer selected by the patient or patient-designee is untrusted.

Response. We thank commenters for their feedback. An API Information Source would not be prohibited from showing a warning to patients as part of the patient authorization for an application to receive their EHI from an API Information Source. This could include a warning that an application attempting to access data on behalf of a patient is untrusted. We refer commenters to the information blocking provisions in section VIII for additional information about providing warnings to patients.

ii. Registration for Production Use

We proposed in 84 FR 7494 in § 170.404(b)(1) to require API Technology Suppliers to register and enable all applications for production use within one business day of completing its verification of an application developer's authenticity.

Comments. Commenters generally supported the proposed registration requirements. Most commenters suggested extending the registration timeframe to five business days.

Response. We appreciate the feedback from commenters. We have reorganized this section of the regulation text for readability by combining ''Authenticity verification'' with ''Registration for production use'' under the heading ''Authenticity verification and registration for production use'' in § 170.404(b)(1). We accepted the recommendation from commenters to extend the registration timeline and have finalized in § 170.404(b)(2)(ii) a requirement for Certified API Developers with Health IT Modules certified to the certification criterion finalized in § 170.315(g)(10) to register and enable all applications for production use within five business days of completing its verification of an application developer's authenticity pursuant to requirements finalized in § 170.404(b)(1)(i).

iii. Service Base URL Publication

We proposed in 84 FR 7595 in § 170.404(b)(2) to require an API Technology Supplier to support the publication of service base URLs for all of its customers, and make such information publicly available, in a computable format, at no charge.

Comments. A majority of commenters supported the proposal requiring API Technology Suppliers to publish service base URLs for all of its customers. Several commenters recommended the creation of a single, publicly available repository to maintain all client endpoints. Some stakeholders recommended ONC require additional facility information be published with the service base URL. Commenters who disagreed with this proposal stated that health IT developers cannot publish client information without their consent, and that API Data Providers should have the sole authority to publish their endpoints.

Response. We thank commenters on their feedback on our proposal requiring a Certified API Developer to publish service base URLs for all of its customers. The public availability and easy accessibility of this information is a central necessity to assuring the use of certified API technology without special effort, particularly for patient-facing applications. We agree with the points made by commenters on the need for a single or multiple publicly available repositories that maintain provider service base URLs. We encourage industry to coalesce around the development of a public resource from which all stakeholders could benefit. We believe this would help scale and enhance the ease with which service base URLs could be obtained and used. While we support the concept of repositories for service base URLs, we do not believe that creating a requirement under the Program is the appropriate mechanism to foster industry support around this concept at this time.

We acknowledge that stakeholders expressed concern about Certified API Developers publishing client service base URLs and revised our approach to focus on service base URLs necessary to support patient access. We anticipate that many services related to certified API technology will be developed and made available and do not believe it is appropriate to burden Certified API Developers with publishing all service base URLs for these services for all of their customers. We considered several options, including requiring Certified API Developers to publish service base URLs for only those API Information Source customers for whom they manage/host an authorization server centrally. However, we determined that alternative options would not meet our policy interests and would lead to unnecessarily complex and burdensome approaches and would not achieve the Cures Act's goals of enabling EHI to be accessed, exchanged, and used without special effort. Additionally, we considered requiring that all Certified API Developers with certified API technology, that is, health IT developers with a Health IT Module certified to § 170.315(g)(7) through (10), meet this requirement. However, we determined that it would be more beneficial to allow health IT developers to focus energy and resources on upgrading their technology to the certification criterion finalized in § 170.315(g)(10). Therefore, we have finalized in § 170.404(b)(2) that a Certified API Developer must publish service base URLs for all Health IT

Modules certified to § 170.315(g)(10) that can be used by patients to access their EHI. We further require that a Certified API Developer must publicly publish service base URLs for all customers in a machine-readable format at no charge regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source. We note our focus for this criterion on ''service base URLs for Health IT Modules certified to § 170.315(g)(10) that can be used by patients to access their EHI.'' We believe that Certified API Developers will have adequate relationships with API Information Sources in the process of providing Health IT Modules certified to § 170.315(g)(10) and will be able to collect and publish all service base URLs that support patient access on behalf of their customers. Furthermore, we note that API Information Sources would be obligated to share such service base URLs with Certified API Developers to avoid violating the Technical Interference Information Blocking provisions as discussed further in section VIII. Certified API Developers must make available appropriately scoped service base URLs that can be used by patients to access their EHI for Health IT Modules certified to § 170.315(g)(10).

iv. Providing (g)(10)-Certified APIs to API Data Providers

We proposed in 84 FR 7494 in § 170.404(b)(3) that an API Technology Supplier with Health IT Modules previously certified to § 170.315(g)(8) must provide all API Data Providers Health IT Modules certified to § 170.315(g)(10) within 24 months of this final rule's effective date.

Comments. The majority of comments received urged ONC to extend the timeline beyond the 24 months proposed. Many commenters requested separate timelines for developers and providers. Several commenters recommended 36 months. Some commenters offered alternatives ideas for timelines, including a stepwise approach, or ONC only determining technical timelines, and allowing CMS to cover provider timelines. Only a few commenters encouraged faster adoption.

Response. We appreciate commenters' feedback on our proposal. Given the reduced scope of the overall updates required by this final rule, our belief that the industry is well-prepared to meet this certification criterion's requirements once the final rule is published, and the Cure's Act expectation that secure, standards-based APIs would be made available in a timely manner, we have retained a 24 month compliance timeline, which will start from the publication date of the final rule. At that point, it will be approximately five years since the Cures Act's passage and we believe its implementation should not be delayed any further. We also remind stakeholders that this is within 24 months of this rule's publication compliance date for supplying all API Information Sources with Health IT Modules certified to § 170.315(g)(10) enables Certified API Developers (based on their client base and IT architecture) to determine the most appropriate timeline for development, testing, certification, and product release cycles. Thus, we have finalized in § 170.404(b)(3) that a Certified API Developer with certified API technology previously certified to the certification criterion at § 170.315(g)(8) must provide all API Information Sources with such certified API technology deployed with certified API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of the publication date of the final rule.

v. Compliance for Existing Certified API Technology

We proposed in 84 FR 7486 that API Technology Suppliers with Health IT Modules certified to § 170.315(g)(7), (8), or (9) must revise their existing API documentation within six months from the final rule's effective date.

Comments. Some commenters supported the requirement to revise existing API documentation within six months of the final rule's effective date. Others requested more time to allow documentation and all other websites to come into alignment before enforcement of this Condition of Certification requirement. One commenter requested clarification on which documentation requires revision within the six-month timeframe.

Response. In order to align the API Condition of Certification requirements policies, we have broadened the scope of the provision finalized in § 170.404(b)(4) to apply to all API Condition of Certification requirements finalized in § 170.404(a), including § 170.404(a)(1) through (4). Given the change of scope, we renamed this section to ''Compliance for existing certified API technology.'' We considered commenters' request for more time, but given the already delayed effective date of Part 170 we believed the proposed time of six months sufficient to enable Certified API Developers to become compliant with the Condition of Certification requirements finalized in § 170.404(a). This additional time provides Certified API Developers with Health IT Modules already certified to § 170.315(g)(7), (8), or (9) a total of eight months from the final rule's publication to update their policies and documentation to comply with the requirements finalized in § 170.404(a). We did not allow a longer time period than six months in § 170.404(b)(4) due to the fact that we have finalized our proposal in § 170.404(b)(3) to require Certified API Developers with Health IT Modules previously certified to the certification criterion in 170.315(g)(8) to provide § 170.315(g)(10)-certified APIs to API Information Sources within 24 months of final rule's publication date. These policies finalized in § 170.404(b)(4) provide API Information Sources with Health IT Modules certified to § 170.315(g)(8) with 18 months of updated documentation before the new requirements finalized in § 170.404(b)(3) become effective. Setting a more delayed compliance date than the one finalized in § 170.404(b)(4) would have unreasonably delayed and ultimately diminished the benefits of the Program requirements we have finalized in this rule. In summary, we finalized in § 170.404(b)(4) that Certified API Developers with Health IT Modules certified to § 170.315(g)(7), (8), or (9) must comply with § 170.404(a) no later than six months after this final rule is published in the **Federal Register**, including by revising their existing business and technical API documentation and making such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

5. Real World Testing

The Cures Act requires, as Condition and Maintenance of Certification requirements under the Program, that health IT developers successfully test the real world use of the technology for interoperability [107] in the type of setting in which such technology would be marketed. As discussed in the Proposed Rule (84 FR 7495), the objective of real world testing is to verify the extent to which certified health IT deployed in production contexts continues to demonstrate conformance to the full scope of applicable certification criteria and functions with the intended use cases as part of the overall maintenance

[107] Defined in statute in section 3000 of the Public Health Service Act (as modified by section 4003 of the Cures Act) and defined in regulation at 45 CFR 170.102.

of a health IT's certification. Real world testing should assess that the certified health IT is meeting the intended use case(s) of the certification criteria to which it is certified within the workflows, system architectures, and type(s) of care setting(s) for which it is marketed (advertised, promoted, or sold).

For the purpose of this Condition of Certification requirement, in § 170.405(a), we proposed (84 FR 7495) that successful real world testing means:

- The certified health IT continues to be compliant to the full scope of the certification criteria to which it is certified, including the required technical standards and vocabulary codes sets;
- The certified health IT is exchanging electronic health information in the care and practice settings for which it is intended for use; and
- Electronic health information is received by and used in the certified health IT.

To fully implement the real world testing Condition of Certification requirement, we proposed Maintenance of Certification requirements that would require health IT developers to submit publicly available prospective annual real world testing plans and retrospective annual real world testing results for the certification criteria focused on interoperability to which each of its Health IT Modules is certified (84 FR 7496).

Comments. Comments on the whole support the establishment of a robust process of real world testing. Several commenters expressed concerns regarding the quality and usability of health IT. Specifically, commenters indicated that issues related to health IT usability may be contributing to clinician burn-out or impacting patient safety, noting that they therefore strongly support the inclusion of robust real world testing requirements.

Response. We appreciate all comments, and have finalized real world testing Condition and Maintenance of Certification requirements in § 170.405(a) and (b) as proposed, with minor adjustments to due dates and clarifications of several points in response to specific comments as discussed below.

Comments. Commenters indicated that additional clarification of the real world testing requirements would make these Condition and Maintenance of Certification requirements less burdensome to implement. These commenters specifically sought additional guidance around the expectations for an appropriate testing plan and method of execution. One commenter recommended that ONC provide more guidance around what care settings must be covered by test plans, and establish a minimum number of settings and test sites that are applicable for certified Health IT Modules.

Response. In response to comments requesting additional guidance around expectations and acceptable methods for real world testing, we provide below additional discussion, explanation, and illustrative examples. At this time, we have decided not to establish a minimum number of settings or minimum percentage or fraction of production instances of the developer's applicable certified Health IT Modules that must be included in the developer's annual real world testing activities. While health IT developers are not required to test their certified health IT in each and every setting in which it is intended for use, we would expect a developer's real world testing plan to address each type of clinical setting for which their health IT is marketed. Developers must address in their real world testing plans their choice of care and/or practice settings to test and provide a justification for their chosen approach. We also remind developers that although we are not requiring testing in every setting for which the certified health IT is marketed, we encourage real world testing in as many specific settings as feasible within each type of setting for which the certified health IT is marketed.

Comments. Some commenters expressed a view that there has been too much focus on the export capabilities of systems and not enough attention paid to providers being able to ingest data received in standardized formats—such as the Continuity of Care Document (CCD) standard—from other providers, including other providers who use the same developer's Health IT Modules certified to produce exports in conformance with the standards.

Response. The interoperability focused criteria listed in § 170.405(a) include required capabilities for receiving and incorporating data in accordance with referenced standards and implementation specifications adopted by the Secretary in part 170 subpart B. We believe this appropriately aligns requirements for real world testing of Health IT Modules' ability to ingest data with the capabilities their certifications address.

Comments. A commenter recommended that, for real world testing of Health IT Modules certified to the API criterion, the final rule require health IT developers to provide a testing environment (or ''developer sandbox'') and require the use of a testing platform and test scripts that validate the ability of the API to meet the underlying requirements for the version of FHIR® to which Health IT Module(s) are certified, any applicable FHIR® profiles, and implementation guides.

Response. As discussed in the Proposed Rule (84 FR 7496), we believe health IT developers are in the best position to design and facilitate implementation of real world testing approaches that balance the burdens of this statutory requirement with its intended assurances that certified health IT as deployed in the types of clinical settings for which it is marketed (advertised, promoted, or sold) continues to meet the Program requirements, including but not limited to interoperability performance, applicable under the certification it holds. While we recognize that testing environments can be useful for a variety of purposes, and would not generally discourage developers from offering test platforms specific to their products or participating in the development and use of open-source testing platforms, the purpose of real world testing is to demonstrate that Health IT Modules continue to perform in conformance to their certification when and as they are deployed in production environments supporting the types of clinical settings for which the Health IT Modules are marketed. Thus, real patient data and real production environments will in most cases best meet that need and should be first considered when developing real world testing plans. Mandating creation or use of testing environments for real world testing would compete for developers' time and effort with the focus on innovative ways to best serve the purpose of the real world testing Conditions and Maintenance of Certification requirements at the least burden on their customers and end users. We have therefore not required health IT developers to provide a testing environment (or ''developer sandbox'') nor have we required the use of a testing platform or test scripts in order to satisfy real world testing Condition and Maintenance of Certification requirements.

Comments. Several commenters requested that ONC be mindful of the burdens this testing could place on health care providers in terms of time and cost and take all necessary steps to minimize such burdens. Commenters specifically stated real world testing would require significant work by providers for whom, in the commenters' stated view, there is no incentive to

participate in real world testing. Some commenters specifically recommended that HHS incentivize providers to participate, stating that without providers' participation, this proposal would become an untenable requirement. One commenter requested HHS clarify whether a developer would be permitted to compensate its customers for the time the customer spends supporting the developer's real world testing activities.

Response. We thank commenters for their feedback noting the potential for health IT developers' real world testing activities to impose burden on providers. We do appreciate the importance of recognizing that providers engage directly and actively in various types of activities supporting advancement of health IT. The fact that many of these activities could be included in robust real world testing regimes suggests that we should provide developers with extensive flexibility to develop innovative real world testing plans. We have therefore built into our real world testing policy flexibility that offers the developer a substantial opportunity to design real world testing approaches that minimize burden and fully optimize value of the real world testing activities and results to current and prospective customers. We do not believe that HHS incentives to providers participating in real world testing would be the most effective means of alleviating burdens on health care providers specifically attributable to developers' real world testing activities. Rather, the flexibility of our policy allows for, and encourages, developers to approach real world testing in an innovative mode so that they can maximize efficiency and minimize burden of real world testing for both the developer and its customers. A wide range of practical strategies are available for developers to potentially consider in creating such optimized solutions for real world testing of their specific health IT with their particular customer base. Examples of this range of practical strategies include, but are not necessarily limited to: Avoiding some activities that satisfy only the real world testing Maintenance of Certification requirements by including in its overall real world testing plans the testing typically associated with confirming functionality of new installations and upgrades of their software; and innovating methods of measuring products' performance in real time use through system metadata and/or feedback from health information networks and other exchange partners of their customers.

In response to the recommendation that developers be allowed to compensate their customers for participating in the developer's real world testing activities, we note that nothing in our proposed or finalized policy under part 170 would prohibit that. In the event a developer concludes that its real world testing approach imposes on its customers directly participating in real world testing activities a burden that the developer would like to offset for those customers, we would not discourage the developer from considering whether there may be opportunities within the bounds of other applicable laws or regulations for developers of certified health IT to offer customers some types of burden-offsetting compensation or other incentive for real world testing participation. Analysis, interpretation, or changes to such other law or regulation is outside the scope of this particular rulemaking action. Moreover, outside the rulemaking process, developers should be aware that ONC is not in a position to provide general guidance on Federal laws specific to compensation arrangements or advice specific to any particular circumstances or contemplated conduct related to developers compensating providers for participating in developers' real world testing activities. However, if developers or providers may be contemplating a potential compensation arrangement related to offsetting providers' cost or burden of engagement in developers' real world testing, we offer as a point of information that one publicly stated purpose of the HHS Office of the Inspector General advisory opinion process is to provide meaningful advice about of the applicability of the anti-kickback statute or other OIG sanction statutes in specific factual situations.[108]

Comments. One commenter expressed concern that developers with small customer bases will have smaller pools of participants willing to undergo a lengthy process which will require significant resources and suggested developers submit results from a more limited scope of testing only every three years.

Response. We reiterate that the policy we have finalized includes substantial flexibility for developers to assess how to meet the real world testing Condition and Maintenance of Certification requirements in a way that appropriately minimizes burden on the current users of their certified health IT.

[108] For more information about HHS Office of the Inspector General advisory opinions and advisory opinion process, please visit: *https://oig.hhs.gov/compliance/advisory-opinions/index.asp.*

Comments. A commenter expressed concern that health care providers might be unwilling to use health IT that had not yet been certified, and that this could make real world testing of Health IT Modules prior to certification impractical.

Response. In our Proposed Rule (84 FR 7429), we proposed in § 170.405(a) to limit the applicability of this Condition of Certification to health IT developers with Health IT Modules that are certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange. We also proposed that the real world testing Condition of Certification would be met through meeting the real world testing Maintenance of Certification requirements in § 170.405(b). We have finalized this proposal as proposed. Thus, the real world testing Condition and Maintenance of Certification requirements do not mandate testing real world use of a Health IT Module in actual production environments before it is certified.

a. Unit of Analysis at Which Testing Requirements Apply

Comments. One commenter requested confirmation if real world testing is required per CHPL listing, per product, or per company.

Response. The real world testing Condition and Maintenance of Certification requirements apply to each developer that has at least one Health IT Module certified to at least one of the interoperability and exchange focused criteria listed in § 170.405(a), because Condition and Maintenance of Certification requirements apply to the developer of certified health IT. However, each developer of certified health IT to which the real world testing Condition and Maintenance of Certification requirements apply must conduct real world testing for each criterion within the scope of real world testing (§ 170.405(a)) to which each developer presents for certification a Health IT Module that is part of a health IT product to be listed on the CHPL are certified. A health IT developer with multiple products that are listed on the CHPL and that include one or more Health IT Module(s) certified to one or more of the criteria listed in § 170.405(a) need only submit one real world testing plan, and one real world testing results report, for any given annual cycle of real world testing, but the real world testing plan and results report must address each of the developer's products that is listed on the CHPL. Health IT developers with multiple health IT products that may include the same Health IT Module(s) certified to one or

more of the criteria listed in 170.405(a) have discretion to design their real world testing plans in a way that efficiently tests a combination of products that include Health IT Modules certified criteria listed in § 170.405(a) so long as testing plans and results are traceable to specific certified Health IT Modules and each criterion to which the Health IT Module(s) are certified, and address the types of settings for which the products are marketed. Because the purpose of real world testing is to test health IT products as they are deployed in production, developers of health IT products deployed through the cloud who offer their products for multiple types of clinical settings will be required to test the same capability for those different types of settings even if it uses a single instance of the deployed capability to serve all of those types of settings.

b. Applicability of Real World Testing Condition and Maintenance of Certification Requirements

We proposed (84 FR 7495) to limit the applicability of the real world testing Condition of Certification requirement to health IT developers with Health IT Modules certified to one or more of the certification criteria focused on interoperability and data exchange or availability listed in (then-proposed) § 170.405(a):

- The care coordination criteria in § 170.315(b);
- The clinical quality measures (CQMs) criteria in § 170.315(c)(1) through (c)(3);
- The ''view, download, and transmit to 3rd party'' criterion in § 170.315(e)(1);
- The public health criteria in § 170.315(f);
- The application programming interface criteria in § 170.315(g)(7) through (g)(10); and
- The transport methods and other protocols criteria in § 170.315(h).

We solicited comment on whether to also include the ''patient health information capture'' certification criteria in § 170.315(e)(3), including the value of real world testing these functionalities compared to the benefit for interoperability and exchange (84 FR 7496). We also solicited comment on whether any other 2015 Edition certification criteria should be included or removed from the applicability list (to be codified at 170.405(a)) for this Condition of Certification requirement.

Comments. The vast majority of commenters addressing this proposal were in support of the specific criteria proposed to be within the scope of real world testing and expressed agreement that required testing should be limited to Health IT Modules certified to one or more of the certification criteria listed in § 170.405(a) as proposed.

Response. We appreciate all feedback received. The list of criteria to which real world testing Condition and Maintenance of Certification requirements apply is finalized in § 170.405(a) as proposed.

Comments. We received one comment supporting and two comments opposing the addition of patient health information capture criterion in § 170.315(e)(3) to the scope of real world testing. One commenter specifically recommended against including the patient health information capture criterion in § 170.315(e)(3) in real world testing because of the significant variability in how health IT certified to this criterion is implemented. They stated that this variability in the real world could make cross-implementation comparisons difficult, and stated that testing for this criterion could present a particular challenge based on difficulty they anticipated would be encountered in securing needed engagement from patients as well as the exchange partners who would presumably receive the data as a result of the patient using the ''transmit'' functionality. Commenters opposed to addition of this criterion to the real world testing Condition and Maintenance of Certification requirements also stated this addition would add cost to the developer which would then flow down to end users and be burdensome to clinician practices.

Response. On balance, the comments received do not support expansion of the scope of real world testing requirements to include the patient health information capture criterion in § 170.315(e)(3) at this time. In developing the proposed list of criteria to which real world testing Condition and Maintenance of Certification requirements would apply, we concluded an initial focus on those particular criteria would strike an appropriate balance between the magnitude of the challenge represented by the new real world testing requirements and the potential benefits of their broader application. The concerns raised by the commenters recommending against adding the patient health information capture criterion in § 170.315(e)(3) to the scope of real world testing requirements at this time, combined with other comments more generally recommending against a broader scope at this time, tend to support the conclusion that the scope we proposed strikes an appropriately practical balance until we and the industry have benefit of experience and innovation in real world testing. Thus, the finalized list of criteria to which real world testing requirements apply (§ 170.405(a)) does not include the patient health information capture criterion in § 170.315(e)(3).

Comments. A few commenters suggested expanding the scope of real world testing requirements to include the proposed ''EHI export'' criterion in § 170.315(b)(10).

Response. We appreciate the confirmation that commenters supported inclusion of the ''EHI export'' criterion in § 170.315(b)(10) alongside the rest of the care coordination criteria in § 170.315(b). We have finalized the criteria listed in § 170.405(a) including, as proposed, all criteria within § 170.315(b).

Comments. One commenter expressed an opinion that the initial scope of criteria is more expansive than the commenter would suggest for an introductory set, and asked that fewer criteria be required for the initial rollout of real world testing, delaying application of the requirement to more interoperability focused criteria until experience has been amassed with real world testing for a narrower selection of criteria than we had proposed.

Response. Noting that the majority of comments received were supportive of the scope as proposed, we also balance suggestions such as that offered by this commenter against the Program's needs and the purpose of the real world testing Condition and Maintenance of Certification requirements. We do not believe it would be in the best interest of the Program or the health care providers and patients who rely on certified health IT to meet their needs for interoperable health IT to narrow the applicability of the real world testing Condition and Maintenance of Certification requirements further than we proposed. We have, therefore, finalized the criteria listed in § 170.405(a) as proposed.

Comments. Some commenters advocated expanding the scope of the real world testing requirement to include select functionally-based ''clinical'' criteria within § 170.315(a) that are included in the base EHR definition.

Response. As explained in the Proposed Rule (84 FR 7495), we did not propose to include in the scope of real world testing functionally-based criteria, administrative criteria, or other criteria that do not focus on interoperability and exchange or availability of data. The ''clinical'' certification criteria in § 170.315(a) were noted in the Proposed Rule as an

example of criteria not proposed because they require only that the health IT enable the provider to record, change, and access specific types of data within the Health IT Module being certified (or within a product that includes the Health IT Module being certified to the particular criteria). However, real world testing of health IT's ability to exchange the types of data these clinical criteria reference is addressed through the inclusion of the USCDI in the interoperability-focused criteria listed in § 170.405(a) as proposed, which is finalized as proposed. In order to successfully exchange interoperable EHI, the health IT must be able to access it, and in order to incorporate a type of data, the health IT must be able to record it.

Comments. The majority of comments received specifically referencing the proposed inclusion of public health criteria in the real world testing requirement in § 170.405(a) support the importance and inclusion of the public health criteria in the scope of real world testing requirements. One commenter questioned the inclusion of the public health criteria in § 170.315(f), stating the commenter's perception that extensive variation between registries would make this a challenging functionality to demonstrate.

Response. Variations in system configurations across different public health agencies' infrastructures may suggest different real world testing strategies may be most appropriate, or most relevant to customers, compared to what might be the case for some other criteria within the scope of real world testing. However, as noted below about testing tools, we are aware of a wide variety of resources and opportunities to test real world interoperability performance of Health IT Modules certified to the public health criteria in § 170.315(f). Because interoperability performance in actual production environments is an important feature of health IT certified to the public health criteria in § 170.315(f), and noting the support for its inclusion expressed by most commenters, and we have determined that the most appropriate course is to finalize the inclusion of the public health criteria in§ 170.315(f) in the scope of real world testing in § 170.405(a).

Comments. One commenter expressed concern that some of the criteria proposed for inclusion in § 170.405(a) be re-examined because they do not include all three of the characteristics our Proposed Rule described as being demonstrated through real world testing. Examples offered included that some criteria proposed for inclusion in § 170.405(a) require exporting but do not require receipt and use of electronic health information by the certified health IT.

Response. We appreciate commenters' bringing to our attention that additional discussion about the requirements would be helpful to the community. For the criteria proposed and finalized in the real world testing scope in § 170.405(a), such real world testing needs to address the interoperability characteristics and all other functionalities and capabilities applicable based on the specific criteria to which the Health IT Module is certified. For example, even if a Health IT Module is not certified to any criterion that specifically requires it to demonstrate, in order to be certified, that the Health IT Module has the capability to incorporate and use data received directly from sources outside the production environment in which it is deployed, that Health IT Module will still need to demonstrate conformance to the full scope of each criterion to which it is certified. This includes, though it is not limited to, the technical standards and vocabulary codes sets included in each criterion to which it certified.

c. Testing Plans, Methods, and Results Reporting

We proposed (84 FR 7496) that a health IT developers must submit an annual real world testing plan to its ONC–ACB via a publicly accessible hyperlink no later than December 15, of each calendar year for each of its certified Health IT Modules that include certification criteria specified for this Condition of Certification. We proposed (84 FR 7497) that a health IT developer must submit an annual real world testing plan to its ONC–ACB via a publicly accessible hyperlink no later than January 31, of each calendar year for the preceding calendar year's real world testing.

We proposed that the real world testing plan, which will be required to be available to ONC and the public via the CHPL no later than December 15 of each year once this final rule is effective, will need to address the health IT developer's real world testing that will be conducted the upcoming calendar year and must include, for each of the certification criteria in scope for real world testing in § 170.405(a) and each Health IT Module certified to one or more of these criteria (84 FR 7496):

- The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability, including a mandatory focus on scenario- and use case-focused testing;
- The care and practice setting(s) that will be tested for real world interoperability, including conformance to the full scope of the certification criteria requirements, and an explanation for the health IT developer's choice of care setting(s) to test; [109]
- The timeline and plans for voluntary updates to standards and implementation specifications that ONC has approved (further discussed below);
- A schedule of key real world testing milestones;
- A description of the expected outcomes of real world testing;
- At least one measurement/metric associated with the real world testing for each certification in scope; and
- A justification for the health IT developer's real world testing approach.

We sought comment (84 FR 7497) on whether we should specify a minimum ''core'' set of metrics/measurements and examples of suggested metrics/measurements as well as on the timing of required real world testing results reporting. We also invited comment on the annual frequency and timing of required real world testing results reporting.

Comments. Most comments received supported the proposed requirement for Health IT Modules to undergo real world testing. In addition, commenters indicated that real world testing should occur on a regular basis to ensure various types of changes in the Health IT Modules or production environments have not affected functionality required by the certification. Several commenters recommended development of more specific minimum requirements for test plans and measurement of results. They further recommended that ONC provide additional guidance about what will constitute a minimally acceptable testing plan with explicit content depicting the minimum requirements for each component of the testing plan.

Response. We thank commenters for their feedback. As discussed in the Proposed Rule and above, we believe health IT developers are in the best position to design and facilitate implementation of real world testing approaches that balance the burdens of this statutory requirement with its intended assurances that certified health

[109] We do not specifically define or limit the care settings and leave it to the health IT developer to determine. As an example, health IT developers can consider categories, including but not limited to, those used in the EHR Incentive Programs (*https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/UserGuide_QNetHospitalObjectivesCQMs.pdf*); long-term and post-acute care; pediatrics; behavioral health; and small, rural, and underserved settings.

IT meets Program requirements, including interoperability performance, applicable under the certification it holds. We have therefore finalized requirements in § 170.405(b)(1) designed to avoid the risk of a ''one size fits all'' set of testing tools (discussed at 84 FR 7496) that might not fully address the concerns raised or provide the assurances of interoperability performance sought across the various types of care settings. By establishing in § 170.405(b)(1)(iii) the topics and considerations every developer must address in its required real world testing plan but not specifying how they must address these required aspects we have provided health IT developers with a requirement that at the same time provides them with the flexibility to develop and implement successful real world testing plans that will best balance burden and value for the customers of each of their products. The ONC–ACBs will be responsible for assessing real world testing plans and results reports for completeness in comparison to what § 171.405(b)(1) requires the plan and results reports to include or address, but will otherwise not be formally evaluating the testing approach for quality as a testing approach. We note for clarity that while ONC–ACB's will not be judging a developer's real world testing approaches as planned or as executed, the contents of a developer's publicly available real world testing results could be used by an ONC–ACB as part of its ongoing surveillance of certified health IT. Additionally, we have finalized our proposed requirement in § 170.405(a) and (b) that requires developers subject to the real world testing Condition and Maintenance of Certification requirements (see § 170.405(b)(2)(i)) who discover in the course of their real world testing any non-conformities with the standards, functionalities, or other requirements of any certification criterion under the Program, to address these non-conformities in order for their Health IT Modules to remain certified. This requirement will apply in the same manner to Health IT Modules certified under the SVAP flexibility in § 170.405(b)(8) or (9) as to Health IT Modules not certified under the SVAP flexibility. Thus, developers who discover non-conformity to any Program requirement(s) will be required to report those non-conformities to their ONC–ACB(s). In order to provide a clear threshold for determining whether a developer has acted on this requirement in a timely manner, we have finalized the requirement to report non-conformities within 30 days of discovering them (see § 170.405(b)(2)(i)). We believe 30 days is an appropriate timeframe to allow developers the opportunity to gather all facts and report to their ONC–ACBs the details and nature of the non-conformity. Furthermore, we believe more than the 30 days would extend beyond the timeframe by which a non-conformity should be investigated by an ONC–ACB and corrective action implemented, if necessary.

We are aware that by choosing not to specify particular methods, tools, or checklists of activities that must be included in real world testing, and providing instead extensive flexibility for developers to select tools and design overall methodologies based on their knowledge of their products and customers, we are asking developers to apply innovation and problem solving skills to their real world testing. We believe that the alternative of developing a catalog of detailed specifications and checklists, as some commenters suggested, would be undesirably complex, less supportive of ongoing innovation in the market, and not ultimately less burdensome for developers or their customers. As we have noted in the context of prior Program rulemaking actions, we often make additional information resources and non-binding guidance regarding real world testing available through familiar communications channels, such as the *HealthIT.gov* website.

Comments. Several commenters expressed concerns about the burden of real world testing in specific reference to ONC–ACB processes for in-the-field surveillance of certified products' continued conformance to applicable certification criteria. Some comments raised concerns about the burden that could be placed on developers' customers should developers choose to rely heavily on the procedures used by ONC–ACBs for randomized or reactive in-the-field surveillance. Some comments indicated concern that ONC would expect, encourage, or view more favorably real world testing approaches that rely heavily or exclusively on use of ONC–ACB in-the-field surveillance protocols.

Response. In the Proposed Rule, we stated that ''developers may consider working with an ONC–ACB and have the ONC–ACB oversee the execution of the health IT developer's real world testing plans, which could include in-the-field surveillance per § 170.556, as an acceptable approach to meet the requirements of the real world testing Condition of Certification'' requirement (84 FR 7497). Having considered all comments received, we have decided not to finalize the flexibility for developers to use ONC–ACBs' in-the-field surveillance as part of the developer's real world testing plan. We do not believe that use or replication of methods or protocols used by ONC–ACBs for in-the-field surveillance of certified Health IT Modules would be the most effective or the least burdensome approach available to health IT developers and are concerned accepting real world testing approaches that rely on ONC–ACB in-the-field surveillance could slow rather than accelerate development of more innovative approaches to real world testing. We are also concerned that inclusion of ONC–ACB execution of in-the-field surveillance within a developer's real world testing approach could lead to confusion as to whether the organization that is an ONC–ACB was applying in-the-field surveillance protocols in its capacity as an ONC–ACB as part of its oversight responsibilities on behalf of ONC or in its private capacity on behalf of the health IT developer. We believe it is important, to protect HIPAA covered health care providers and other HIPAA covered entities and their business associates from inadvertently violating requirements related to disclosure of health information, to maintain a clear distinction of when an organization that is an ONC–ACB is acting in the ONC–ACB capacity and when it is acting in its private capacity. We note and emphasize this because, in the event a developer may choose to engage services in support of developing or implementing the developer's real world testing plans from an organization or entity that also happens to be an ONC–ACB, all activities undertaken by the organization or entity to develop, execute, or support the development or execution of the developer's real world testing plan would be activities outside the ONC–ACB role. In such circumstances, the organization that is an ONC–ACB would be acting in a separate, private capacity. Note that an organization providing such private services that involve ePHI would likely be characterized under the HIPAA Rules as a business associate to the health care provider and subject to the HIPAA Rules. The oversight authorities attached to its ONC–ACB role would not apply to the organization's requests to gain access to health care provider facilities or to EHI for purposes of providing these separate support services to health IT developers for conduct of the developers' real world testing.

Comments. Several commenters sought confirmation that a test server could be used for real world testing instead of a production environment, given the permissible use of synthetic data.

Response. After considering the totality of comments received, we have decided to finalize that a test server could be used for real world testing and provide the flexibility included in the Proposed Rule that allows for real world testing to occur in a production setting using real patient data in accordance with applicable laws as well as in an environment that mirrors a specific production environment used in a type of clinical setting for which the health IT is marketed. We have also decided to finalize the flexibility for the developer to use synthetic patient data in lieu of or in addition to real patient data in real or simulated/test scenarios executed in environments that mirror production environments where the health IT is deployed. However, we emphasize that the purpose of real world testing is to demonstrate that the Health IT Module(s) work as expected in real-life clinical settings. We note, as a point of potential interest for such consideration, that real world testing plans that meet the Program requirement might include observation or measurement of the health IT's interoperability performance while actual scenarios and use cases are executed by end users on real patient data in actual operational contexts. If a developer chooses to use synthetic data, non-production (mirrored) environments, or a combination of real and synthetic data or production and mirrored environments, to complete any portion of their annual real world testing requirements, the developer must include in their real world testing plan and results submissions a specific explanation justifying how the synthetic data, mirrored environment, or both are appropriate and adequate to meet the real world testing requirement(s) for which they will be or were used.

Comments. Several commenters sought confirmation that a product serving multiple care settings could complete a single test relevant to all settings and ask ONC to provide a list of eligible care settings for reference.

Response. The finalized real world testing Condition and Maintenance of Certification requirements include testing each criterion listed in § 170.405(a) to which any Health IT Module(s) within the product are certified, and testing in each type of setting to which it is marketed. To satisfy these Condition and Maintenance of Certification requirements as finalized, a single testing plan, protocol, or approach must address all the types of settings to which the product, with all its included Health IT Module(s), is marketed and do so with traceability to each Health IT Module of its real world performance in each type of setting for which it is marketed. We believe it is possible to construct a real world use scenario or use case that tests more than one type of setting applicable to the Health IT Module, and confirm that a developer is not required to develop unnecessarily or artificially separate scenarios or use cases across multiple types of settings to which a given developer markets its applicable Health IT Module(s). With respect to the types of settings required to be addressed by a given developer's plan, we do not believe that additional specification is necessary because we believe each developer is well situated to know for what types of settings the developer (or its authorized resellers) has marketed, is marketing, or intends to market its Health IT Modules. For purposes of this Condition and Maintenance of Certification requirement as finalized, there is no exclusion for settings or health care provider types based on their inclusion or lack of inclusion in, or eligibility or ineligibility for, and particular Federal health care program or initiative. Therefore, the types of settings eligible to be addressed in a developer's real world testing plan for a given year include all those to which product(s) including one or more Health IT Modules certified to one or more of the criteria listed at § 170.405(a) as of August 31 of the year in which that specific annual real world testing plan is due have been or are marketed when the real world testing plan is submitted, and/or the types of settings for which the developer anticipates marketing such product(s) in time to include them in a specific year's real world testing activities.

Comments. Several commenters requested ONC ensure that real world testing requirements do not create infrastructure for testing of public health transactions without public health involvement. Several commenters noted that public health organizations and many public health agencies already offer resources and processes used in onboarding processes for public health reporting connections and suggested these resources and processes could be used more broadly to test health IT's real world performance on public health interoperability criteria rather than requiring creation of new or different tools.

Response. We would tend to agree that relying for specific use cases on testing infrastructures developed without appropriate involvement of key participants in the use case would not be an optimal approach. Also, we reiterate that we encourage developers to consider a variety of options and approaches before finalizing their annual real world testing plans. We would encourage developers to consider the real world testing potential of resources, tooling, and infrastructure already offered by public health organizations and agencies before embarking on efforts to develop additional tooling. We also note that, for the interoperability-focused public health criteria, alternatives that would avoid both overuse of simulation environments and asking public health agencies to engage in work unique to developers' real world testing plans might include structured observation and measurement of interoperability performance in actual public health data reporting/exchange as well as the testing ordinarily conducted for onboarding/confirming connectivity of newly deployed/upgraded implementations to public health data exchange infrastructures.

Comments. A number of commenters expressed support of requiring the use of metrics/measurements for real world testing. One commenter stated that ONC should not allow just one measurement to suffice for real world testing of interoperability of a Health IT Module. Several commenters recommended ONC include a description of ''measurement,'' provide clarity on the role of measurement, and provide a ''sample'' or suggested set of metrics/measurements to help foster alignment of reporting around meaningful common metrics/measurements across developers. Some commenters recommended ONC identify a core set of metrics/measures that developers would be required to include, or from which developers would be required to select specific metrics/measures to include, in their real world testing plans. Other commenters advocated against developers being required to submit testing results for a minimum ''core'' set of general metrics, providing the rationale that not all metrics will be available to all systems uniformly and suggesting that many metrics are retained in the provider's locally integrated production systems and unavailable to the developer of any given Module(s) without considerable effort to retrieve the data. One commenter recommended requiring that each developer's real world test plan include measures addressing all of the domains of the NQF report:

Measurement Framework to Assess Nationwide Progress Related to Interoperable Health Information Exchange to Support the National Quality Strategy.[110]

Response. The comments on real world testing did not show clear, widespread support for any specific subset of available metrics as a ''core'' set or catalog that a significant portion of the affected communities (health IT developers, health care providers, and public health agencies) would generally agree should be consistently used across all developers' real world testing plans. Thus, we have finalized the real world testing plan requirements (see § 170.405(b)(1)(iii) and real world testing results reporting requirements (see § 170.405(b)(2)(ii)) without identifying a minimum set of measures that must be used or a catalog of suggested measures from which a developer would be expected to choose in constructing its real world testing plans. We reiterate that each developer must choose a measurement approach, including at least one measurement/metric per applicable criterion, for use in each year's real world testing and explain the selection and relevance of its selected measures/metrics within its justification for its real world testing approach in that year's plan and results report.

Comments. Comments were received on the frequency and timing of real world testing. One commenter stated the policy should not require annual testing if the capability certified for a given criterion remains unchanged year to year, offering the example that if a Health IT Module is certified for both § 170.315(b)(1) and (b)(2) and the developer is planning to release material updates to the capabilities specific to § 170.315(b)(1), but not make any material changes specific to the Module's certification to § 170.315(b)(2), this commenter would prefer that the Health IT Module would need to submit a testing plan and subsequent results addressing only the § 170.315(b)(1) criterion for the year the change is made. Another commenter expressed skepticism regarding the value of annual real world testing requirements, expressing a preference for an approach that developers would, after an initial cycle of post-certification real world testing of a Health IT Module, be required to re-test only when updating to National Coordinator-approved newer versions of adopted standards included in applicable criteria or when making major functional updates to the certified Health IT Module. One commenter who was overall not supportive of the real world testing requirement stated that developers would need a two-year cycle instead of a one-year cycle in order to adequately demonstrate compliance with full functionality testing. One commenter specifically expressed support for the annual frequency and timing of required real world testing results reporting.

Response. We thank the commenters for their feedback regarding the frequency and timing of real world testing. We have finalized the requirement for annual testing in § 170.405(b)(1). Ongoing annual testing is needed to ensure that Health IT Module(s) continue to perform as intended in the types of settings where patients and health care providers continue to rely on it to meet their interoperability needs.

Comments. Several commenters expressed support of the proposed real world testing plan requirements and requested we strengthen this provision to require that developers test their products within each clinical specialty to which the technology would be marketed. One commenter requested that we define with more particularity what is expected of developers during the testing to account for the differing conditions under which Health IT Modules are deployed, and how for example, the system works particular conditions like server degradation. Several other commenters suggested we provide a standardized template for use in developing test plans. Commenters described a template would include all required testing elements and promote greater consistency in the way the test plans are written by the various developers.

Response. For reasons stated in the Proposed Rule (84 FR 7496) and above, we do not believe a centrally developed or standardized approach for real world testing plans is the most appropriate solution at this time. By centrally mandating or endorsing a single template in the interest of consistently formatted documentation, we are concerned that we might inadvertently discourage innovation in both testing approaches and their communication to the customer community. What the plan must include or address for each applicable criterion to which the developer's Health IT Module(s) are certified is outlined in § 170.405(b)(1)(iii), as finalized by this rule. We believe the plan requirements finalized in the plan requirements in § 170.405(b) are specific enough to ensure the plans can be completed by developers and effectively reviewed for completeness by ONC–ACBs, and that both the substance and clarity or efficacy of presentation can both be examined and considered by any interested parties—from health care providers to informatics and interoperability researchers. Because individual circumstances and needs may vary even within the same type of setting or clinician specialty, it would be not be possible at this time to define a real world testing regime that eliminated all of the variability developers may have in implementing their real world testing plans.

Comments. One commenter sought clarification on the total minimum number of metrics required for a developer's real world testing plan to be considered complete and in compliance with the requirement.

Response. A developer's real world testing plan must include at least one metric for each applicable certification criteria. To ensure that we are providing clear guidance, we offer the following illustrative example: A developer with one Health IT Module that is certified to five criteria would need to include in its real world testing plan at least one specific measurement/metric associated with the real world testing for each of those five criteria. Depending on the specific criteria and the developer's real world testing approach, this could call for up to five different measurements/metrics, or could be addressed with fewer different measurements/metrics but a specific measurement/metric would need to be identified/attributed within the plan to each of the applicable certification criteria.

Comments. A few commenters stated concerns regarding our mandatory focus on scenario- and use case-focused testing. One commenter expressed a view that this would be expensive and time consuming, stating that this expense limits scenario- and use case-focused testing in the number of settings that can realistically be tested in any given year. One commenter noted that as more settings are tested, fewer scenarios can be run per setting. Two commenters sought more information on the mandatory scenario- and use case-focused testing that will be required, recommending that Health Information Service Providers (HISPs) be able to attest to the relevant use cases and provide the proper evidence of testing associated to those scenarios.

Response. In light of comments received, we can see how our use of terms that are also used in the context of ONC–ATL laboratory or ONC–ACB surveillance testing, and our reference in one instance to in-the-field

[110] *https://www.qualityforum.org/Projects/i-m/Interoperability_2016–2017/Key_Informant_Summary_Report.aspx* (last accessed 12/17/2019).

surveillance, could have led to an inference that our use of these terms implied we would expect to see the same or similar testing protocols used in real world testing. However, we did not propose that real world testing would require developers to set up and execute artificial scenarios or activities solely for purposes of testing. In fact, we do *not* encourage use of the laboratory testing or ONC–ACB in-the-field surveillance protocols to conduct real world testing, as those particular test methods, tools, and surveillance protocols were not designed and should not be relied upon for real world testing. The testing methods/methodologies need to address realistic scenarios, use cases, and workflows associated with interoperability, and we do expect developers to consider such factors as the size of the organization that production systems support, the type of organization and setting, the number of patient records and users, system components and integrations, and the volume and types of data exchange in planning for real world testing.

Comments. One commenter expressed agreement that the developer is best situated to determine the most effective real world testing plan for their products. One commenter requested developers be allowed to work together with their customers to define what real world tests are.

Response. The requirements we proposed and finalized provide developers the opportunity to identify, potentially in partnership with their customers, the real-life scenarios, use cases, and work flows applicable to the customer's day-to-day use of the Health IT Module(s) to meet their interoperability needs in their production environments.

d. Submission Dates

We proposed that a health IT developer must submit an annual real world testing plan to its ONC–ACB via a publicly accessible hyperlink for availability to ONC and the public no later than December 15, of each calendar year, and that the plan must address all of its Health IT Modules certified to the 2015 Edition certification criteria listed in proposed in § 170.405(a) and (84 FR 7496). We proposed requiring that prior to submission to the ONC–ACB, the plan will need to be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information. We proposed that the plan due in any given year will need to include all health IT certified to the 2015 Edition through August 31 of that year (in other words, the August 31 that immediately preceded the December 15 due date).

We further proposed that a health IT developer would submit annual real world testing results to their ONC–ACBs via a publicly accessible hyperlink no later than January 31 of each calendar year for the real world testing conducted in the preceding calendar year (84 FR 7497). We proposed that real world testing results for each certification criterion listed in § 170.405(a) would be required to address the elements required in the previous year's testing plan, describe the outcomes of real world testing with any challenges encountered, and provide at least one measurement or metric associated with the real world testing.

Comments. Some commenters expressed concerns that the annual real world testing plan due date falls in December, noting that in addition to multiple holidays widely celebrated in the U.S., December can be a busy time for many health IT developers due to various year-end requirements and necessary preparations to support customers' quality measurement data submissions for CMS programs.

Response. We understand the commenters' concern that the proposed real world testing plan publication due date falls in the preparatory run-up to year-end deadlines, including for many developers completing preparations to support their customers' successful clinical quality measurement data submission during CMS program windows that typically open on the first Federal business day in January. In consideration of comments received, we have made edits to the phrasing of the CFR text in § 170.405(b) to convey with more precise clarity that under the policy we have finalized, the developer is required to submit its real world testing plans so that the ONC–ACB can conduct its completeness review and publish the plan hyperlink on CHPL no later than December 15 of each year. This allows for the ONC–ACB and developer to identify and agree on the date by which the developer will actually submit its plan to the ONC–ACB, which could be well in advance of December. One practical implication of the single-deadline feature of the policy as proposed is that in order for the plans to be submitted to ONC and made publicly available by the single deadline, the ONC–ACB's requirement to review plans for completeness per Program requirements will in many cases mean that the ONC–ACB will need the developer to submit the plan to the ONC–ACB in advance of the single deadline. We have finalized the December 15 due date for real world testing plan publication on CHPL as proposed. We have also made clarifying edits to the finalized regulation text (see § 170.405(b)(1)) in comparison to the proposed text to more explicitly recognize the practical implication that the developers' and ONC–ACBs' responsibility for a single publication date for the plans means that the plan must be submitted by the developer to the ONC–ACB on a date agreed between them that allows for publication by the deadline. We encourage developers and ONC–ACBs to consider allowing at least one calendar month so that the December 15 due date for ONC–ACBs' publication of real world testing plans will be consistently met. We also note that nothing in § 170.405 as finalized precludes a developer and ONC–ACB from agreeing on the developer submitting its annual real world testing plan to the ONC–ACB more than one month prior to December 15. We have finalized the single plan publication deadline as proposed.

We did not receive comments specific to August 31 as the annual date when a Health IT Module must be certified by in order to be required to be included in the real world testing plan due that year. We have finalized this aspect of our policy as proposed in § 170.405(b)(1)(ii). Thus, developers can submit their real world testing plans as early as September 1 and on a rolling basis thereafter for products in scope for the following year, which also addresses commenter concerns.

We did not receive comments specific to this point, but have removed from § 170.405(b) as finalized the language that would have specifically required the initial submission of the plan to the ONC–ACB by the developer must be by a publicly accessible hyperlink. While this remains an option, and could be the most efficient one for developers and ONC–ACBs in many instances, we believe this is an unnecessarily limiting specification of the manner of interaction between developers and ONC–ACBs in these instances. The URL or hyperlink in CHPL will not be published on CHPL until the ONC–ACB takes action to publish it, and the ONC–ACB is required to review the plan and ensure it is complete before publishing the plan link on CHPL.

Comments. We received some comments that appeared to construe our intent to be that real world testing for all Health IT Modules certified as of August 31 of a given year would need to be planned, conducted, and reported within five months of that date. Comments that appeared to be based on this interpretation also expressed

concern that this would be too much to accomplish on such an annual schedule.

Response. We proposed that each developer's annual real world testing plan required to be published by December 15 of a given year would need to address all of the developer's Health IT Modules certified to criteria listed in § 170.405(a) as of August 31 of that year (84 FR 7496). We also proposed that this annual real world testing plan would pertain to real world testing activities to be conducted in the year following the December 15 plan publication due date. In light of comments received, we can see how we might have been more precise in how we stated that the annual results report would be due early in the year following the year in which the testing it reported was conducted. The full cycle of real world testing for a given year was never specifically proposed to be contained within a single year, considering that the plan is due in the year prior and the results report was proposed to be due in the year following the one in which a given annual round of real world testing activity occurs.

Comments. Comments raised concerns that the January 31 publication deadline might not leave enough time for developers who do not or cannot complete their annual testing activities until late in the testing year to submit their results reports, and ONC–ACBs complete their required reviews, prior to the publication deadline. One commenter raised a specific concern that the proposed January 31 due date for real world testing results falls in the submission window for several CMS programs for which developers' customers need to submit their clinical quality measurement data for the preceding year. One commenter recommended leveraging the existing quarterly update attestation process and asking developers to conduct real world testing on those items identified as major changes.

Response. As with the plan due date, the practical implication of this proposal is that each developer will need to submit their results reports to their ONC–ACB sufficiently in advance of the due date for publication for the ONC–ACB to be able to complete its pre-publication responsibilities for all of the results reports and still publish no later than that due date. In theory, this means that in some cases developers could complete their real world testing relatively early in a given testing year and submit their results report for that year before the CMS submission window for that year's measurement data even opens for the developer's customers. However, considering the comments received, we do recognize it is possible developers may for various reasons not be able to complete their annual real world testing activities until fairly late in any given testing (calendar) year. We also recognize that the data submission window for CMS programs can be a busy time for developers, and would not wish to disadvantage newer or smaller developers who may not have separate resources available to finalize a report of real world testing not concluded until late in the testing year while simultaneously supporting customers' data submissions. In light of these comments, we have decided to finalize a deadline for publication on the CHPL of the publicly accessible hyperlink to developers' report of real world testing conducted in the prior year at March 15 of each year (see § 170.405(b)(2)(ii)). This finalized date gives an additional six weeks for finalization and submission by developers compared to the date originally proposed. It also implements a single deadline, to which the developers and ONC–ACBs are mutually accountable, in parallel to the annual real world testing plan submission requirement in § 170.405(b)(1). We believe this strikes an appropriate balance between timely availability of annual real world testing results and recognition that some developers may need to devote a substantial amount of focus to the CMS quality measures data submission windows at the beginning of each year. Although we have opted not to mandate developers submit their results reports to their ONC–ACBs by a date providing a minimum required lead time for ONC–ACBs' required review of the report, we would suggest that ONC–ACBs and developers consider the potential merits of allowing at least one calendar month between the developer's initial submission of their real world testing results report to the ONC–ACB and the March 15 publication deadline.

e. Real World Testing Pilot Year

We acknowledged in the Proposed Rule that a subsequent final rule for that may not provide sufficient time for health IT developers to develop and submit plans for a full year of real world testing in 2020 (84 FR 7497). Therefore, we indicated in the Proposed Rule that we expected to provide an appropriate period of time for developers to submit their plans, and potentially treat 2020 as a ''pilot'' year for real world testing. We expected that the pilot testing of real world testing would match up to the fullest extent practicable with our proposed real world testing requirements (*e.g.,* same criteria but for a shorter duration and without the same consequences for noncompliance). We welcomed comments on this potential approach.

Comments. The majority of comments specifically addressing this point were in support of 2020 being treated as a pilot year. One commenter agreed that deferring the implementation or constructing a pilot year for the Program would be appropriate and stated their belief that 2020 may be too early even to conduct a pilot.

Response. We thank commenters for their thoughts on potential piloting of real world testing and the timing of initiating real world testing requirements. In consideration of the timing of the final rule, we have decided not to finalize 2020 as a pilot year since developers will now have the majority of calendar year 2020 to develop a prospective plan for real world testing that would begin in 2021. However, we recognize that this first ''performance'' year of real world testing in 2021 presents unique challenges with respect to the development of initial plans, and we fully intend to approach both the submission of initial plans and submission of retrospective testing results for those plans (*i.e.,* 2021 real world testing results) as learning experiences for developers that can be used to inform future iterations of real world test plans. As noted in the proposed rule (84 FR 7497), the due date for the first annual real world testing plan would be finalized based in part on the timing of the final rule. Because this final rule is publishing well in advance of the December 15 annual due date for publication of developers' plans of real world testing activities to be conducted in the following year, we have concluded it is reasonable to require the first annual real world testing plan be published via a publicly accessible hyperlink on the CHPL no later than December 15, 2020. This initial real world testing plan must address any and all of the developer's Health IT Modules that hold a current, valid certificate under the Program as of August 31, 2020. The real world testing plan due to be published in December 2020, will need to address the real world testing activities that will occur during calendar year 2021. The report of results for this initial (2021) annual real world test cycle will be due to be published on the CHPL no later than March 15, 2022.

f. Health IT Modules Certified But Not Yet Deployed

We proposed (84 FR 7497) that even if a health IT developer does not have customers or has not deployed their

certified Health IT Module(s) at the time the real world testing plan is due, the health IT developer would still need to submit a plan that prospectively addresses its plans for real world testing that would occur in the coming year for those Health IT Modules that had been certified on or before August 31 of the calendar year in which the plan is due (the calendar year immediately preceding the calendar year during which testing addressed by any given annual real world testing plan will take place). If a health IT developer has not yet deployed their certified Health IT Module to any real world users when the annual real world testing results are due for that module, we proposed that the developer would need to report as such to meet the proposed Maintenance of Certification requirement.

Comments. We received no comments on this proposal.

Response. We have finalized this proposal. Any Health IT Module certified to at least one criterion within the scope of real world testing as of August 31 of a given year must be addressed by its developer's real world testing plan for the subsequent year that must be published via publicly accessible hyperlink on the CHPL by the December 15 due date (see § 170.405(a)). This requirement applies regardless of whether that Health IT Module is in actual real world use prior to December 15 (or the earlier date by which the developer and ONC–ACB agree the developer will submit its annual real world testing plan to the ONC–ACB to ensure the developer and ONC–ACB meet single, December 15, deadline for the plan to have been reviewed for completeness and published on CHPL). To ensure precise clarity about the effect of the August 31 reference date for purposes of real world testing requirements, we reiterate that if a developer has at least one Health IT Module certified to at least any one criterion within the real world testing scope of applicability as of August 31 of a given year, the real world testing Condition and Maintenance of Certification requirements apply to that developer and the developer must submit an annual real world testing plan for that year, addressing each of their Health IT Module(s) certified to any (one or more) criteria listed in § 170.405(a) and that plan must meet the requirements in § 170.405(b)(1)(iii) for each module and criterion. Only developers who have no Health IT Module(s) certified to any criterion within the real world testing scope of applicability as of August 31 of a given year need not submit a real world testing plan that year and would not be required to perform real world testing in the subsequent year.

g. Standards Version Advancement Process (SVAP)

As discussed in the Proposed Rule (84 FR 7497), as newer versions [111] become available for adopted standards and implementation specifications included in the certification criteria subject to the real world testing Condition and Maintenance of Certification requirements, we believe that a health IT developer's ability to conduct ongoing maintenance on its certified Health IT Module(s) to incorporate these newer versions of Secretary-adopted standards and implementation specifications (''standards'') is essential to support interoperability in the real world. Updated versions of standards reflect insights gained from real-world implementation and use. They also reflect industry stakeholders' interests to improve the capacity, capability, and clarity of such standards to meet new, innovative business needs, which earlier standards versions cannot support. Therefore, as part of the real world testing Condition of Certification, we proposed a Maintenance of Certification flexibility that we refer to as the Standards Version Advancement Process (SVAP).[112] This flexibility would permit health IT developers to voluntarily use in their certified Health IT Modules newer versions of adopted standards so long as certain conditions are met. As we stated in the Proposed Rule, these conditions are not limited to but notably include successful real world testing of the Health IT Module using the new version(s) subsequent to the inclusion of these newer standards and implementation specification versions in the Health IT Module's certification. We proposed to establish the SVAP not only to meet the Cures Act's goals for interoperability, but also in response to the continuous stakeholder feedback that ONC has received through prior rulemakings and engagements, which requested that ONC establish a predictable and timely approach within the Program to keep pace with the industry's standards development efforts.

The SVAP we proposed, with corresponding proposed revisions for §§ 170.500 and 170.555, introduces two types of administrative flexibility for health IT developers participating in the Program (84 FR 7498). First, for those health IT developers with existing certified Health IT Module(s), such Health IT Modules could be upgraded to a new version of an adopted standard within the scope of the certification and have support for that updated version of the standard reflected on the Health IT Module's certificate so long as: Such version was approved by the National Coordinator for use in the Program; and the developer satisfied all requirements of the SVAP including demonstration of conformance through an acceptable means (84 FR 7498 through 7500). For purposes of the SVAP as applied to updates to Health IT Modules with certificates to criteria listed in § 170.405(a) that include prior version(s) [113] of the standards, acceptable means of demonstrating conformance include but are not necessarily limited to self-declaration of conformance, as proposed in 84 FR 7499 and finalized in this final rule. Second, for those health IT developers presenting health IT for certification to a criterion listed in § 170.405(a), a National Coordinator-approved newer version of a standard included in one of these criteria could be used in lieu of or in addition to the version of that standard incorporated by reference in § 170.299 (84 FR 7498). However, for purposes of the SVAP as applied to health IT that is presented for certification to any criterion listed in § 170.405(a), developer self-declaration is an acceptable means of demonstrating conformance *only* where there is not yet another conformance method available that can be validly used for that version of that standard (84 FR 7499 through 7500). The regulation text codifying requirements for health IT developers to avail themselves of each of the proposed types of administrative flexibility was proposed (84 FR 7595 through 7596) in § 170.405(b)(5). Corresponding revisions to § 170.550 and § 170.555 were proposed in 84 FR 7598.

We proposed that the SVAP would be available only for National Coordinator-approved newer versions of standards and implementation specifications (''standards'') that have already been

[111] We note that standards developing organizations and consensus standards bodies use various nomenclature, such as ''versions'' or ''releases,'' to identify updates to standards and implementation specifications.

[112] Regulation text implementing the real world testing Condition and Maintenance of Certification requirement was proposed in § 170.405, including but not limited to SVAP-specific provisions proposed in § 170.405(b)(5). The SVAP-specific provisions have now been finalized in § 170.405(b)(8) and (9) (see section VII.B.5.g of this final rule).

[113] Prior versions for this purpose could include those incorporated by reference in § 170.299, National Coordinator approved newer versions, or a mix of such versions for any or all of the standards adopted by the Secretary in subpart B of part 170 that are included in a given criterion.

adopted into the Program by the Secretary through rulemaking in accordance with applicable law including the Administrative Procedures Act (5 U.S.C. 553) and sections 3001 and 3004 of the Public Health Service Act (PHSA) (42 U.S.C. 300jj–1 and 42 U.S.C. 300jj–11) (84 FR 7498). We have finalized this aspect of the standards version advancement flexibility as proposed. Under current law and the finalized SVAP flexibility, a standard must be initially *adopted* by the Secretary through rulemaking before the National Coordinator can *approve* the use of newer updated versions of that standard in the Program.

We also proposed that a health IT developer would be able to choose which of the updated standards versions approved by the National Coordinator for use in certification to include in its updated certified Health IT Module and would be able to do so on an itemized basis (84 FR 7499).

We stated in the Proposed Rule that we welcomed comments on any and all aspects of our proposed SVAP as an option available to developers through maintenance requirements as part of the real world testing Condition and Maintenance of Certification requirements (84 FR 7500). We also invited comments on our proposal to allow in conjunction with this maintenance flexibility the opportunity for developers to elect to present health IT for initial testing and certification either to more advanced versions or to the prior adopted versions of the standards included in regulatory text as of the date the Health IT Modules are presented for certification.

Comments. Comments were strongly supportive of the SVAP. Several commenters recommended the description of this process include recognition of the fact that developers and systems might need to maintain operational support for previously adopted versions of standards to avoid potential adverse effects on data access, exchange, and use.

Response. We have finalized the SVAP in § 170.405(b)(8) and (9) to provide the flexibility for which stakeholders' comments expressed support. This flexibility includes the option for a Health IT Module to be certified to the standards versions incorporated by reference in § 170.299 and/or one or more National Coordinator-approved updated versions of standards included in the criteria listed in § 170.405(a). Thus, once the National Coordinator has approved for use in the Program more advanced version(s) of any standard(s) applicable to any of the criteria listed in § 170.405(a), a health IT developer will have flexibility to choose on an itemized basis which of the National Coordinator-approved updated standards versions they wish to have included in their Health IT Module certification(s). Using the SVAP flexibility does not require a developer cease supporting prior version releases of standards referenced by applicable certification criteria.

Comments. Several commenters expressed concerns about the effect of an uneven pace of advanced version implementation across health IT developers and products within and outside the Program. Several of these commenters recommended that, as developers voluntarily seek to support newer versions of standards and specifications through the SVAP, they also be required to maintain support for the adopted version of the standard listed in the Code of Federal Regulations (45 CFR part 170, subpart B) for the applicable criteria until HHS conducts rulemaking that would require all certified health IT upgrade to the newer version of the standard and sunset older versions of the standard from the Program on a mandatory, coordinated timeline.

Response. We do recognize the importance of ensuring that updated versions of standards are approved and available for use in the Program only when such use is consistent with the Program's purposes. We do not anticipate that the National Coordinator would approve a newer version of a standard for use in the Program where that is inconsistent with the Program's purposes, notably including the maintenance and advancement of interoperability. Moreover, we believe there is substantial value in allowing for the market to, in effect, sunset obsolete standards versions at its own pace unless a hard cutover (or other highly coordinated nationwide timeline for abandoning older versions) would be necessary to sustain functional interoperability. The SVAP flexibility simply allows for a developer to choose to work with their ONC–ACB to obtain certification, or to modify the scope of the of Health IT Module's certification, to reflect that the Health IT Module as certified includes: The version of each adopted standard that is incorporated by reference in § 170.299; or a specific National Coordinator-approved updated version of each applicable standard; or a National Coordinator-approved updated version for each of one or more applicable standard(s); or multiple version(s) of any one or more adopted standard(s). Previously, developers were free to upgrade certified Health IT Modules to support newer versions of adopted standards, but only in addition to the version(s) of those standards incorporated by reference in § 170.299. In our experience, newer versions render prior versions obsolete on a more rapid pace for some standards than for others and more rapidly than the versions incorporated by reference in regulations could be updated. Prior feedback had indicated that being required to maintain support for the version of a standard that is incorporated by reference in § 170.299 solely for the purpose of maintaining regulatory compliance under the Program represented a burden without commensurate value in cases where customers' operational interoperability needs could be met only by use of newer version(s) of particular adopted standards than the versions listed in the regulations. The SVAP is designed to eliminate that burden and simultaneously provide, through inclusion of support for advanced standards versions within a Health IT Module's certification, enhanced assurance to users that Health IT Modules supporting National Coordinator-approved newer versions of standards under the SVAP flexibility continue to meet all of the requirements of the criteria to which the Health IT Module is certified.

Comments. A number of commenters requested clarification on how the proposed Standards Version Advancement Process would align with expansion of the USCDI, or whether the USCDI will be versioned through the SVAP. Some commenters expressed an opinion that the USCDI expansion process should not be executed or allowed via the SVAP and instead require rulemaking.

Response. As discussed in section IV.B.1, we have adopted the USCDI as a standard in § 170.213 and incorporated USCDI v1 by reference in § 170.299(n)(5). For purposes of the SVAP, the USCDI will be treated like any other standard. This means that health IT when presented for certification to any one or more criteria referencing § 170.213 will be required to support USCDI v1 or a later version, with SVAP providing flexibility for developers to choose whether to support later versions of USCDI that the National Coordinator may approve for use in the Program in lieu of or in complement to USCDI v1. Developers and will not be required to support newer versions of the USCDI standard instead of USCDI v1 until such time as § 170.213 and § 170.299 are updated. However, developers may voluntary choose to use the SVAP flexibility to voluntarily upgrade certified Health IT

Modules, or to seek certification of their health IT, to newer version release(s) of the USCDI if such release(s) have been approved by the National Coordinator for use under the Program. As with any other standard relevant to the SVAP flexibility, we would anticipate that the National Coordinator would not approve for voluntary use under the Program an updated version of any standard that would render Health IT Module(s) using it incapable of exchanging EHI with other technology certified under the Program to other version(s) of the standard. We also note that, although HHS is the steward of the USCDI standard, we have not at this time foreclosed the possibility that we could publish a newer update of the USCDI that the National Coordinator would not immediately approve for developers' voluntary use under the Program via the SVAP flexibility. We recognize a potential that expanding the USCDI to include additional data classes in future versions could lead to Health IT Modules certified to these more advanced versions of USCDI being able to access, use, and exchange more data classes than Health IT Modules certified only to earlier versions of the USCDI. However, the technology certified to National Coordinator-approved newer versions of the USCDI would be capable of exchanging the data classes included in prior version(s) of the standard. Thus, the flexibility maintains interoperability while allowing those who need additional data classes to be fully supported by certified health IT in their access, exchange, and use of these additional data classes and not forcing other users of certified health IT (who do not yet need to access, exchange, or use such additional data classes) to update their health IT. We therefore believe that allowing for expansion of data for which certified Health IT Modules can support interoperability at a pace driven by the market's progress in standards development and demand for interoperability is an important benefit of the SVAP flexibility.

Comments. One commenter stated the SVAP would be more effective for electronic prescribing if it could be used to allow voluntary adoption of a new version of the NCPDP SCRIPT standard by prescribers, pharmacies, and Part D prescription drug plans without CMS rulemaking.

Response. CMS is solely responsible for Medicare Part D program regulations and other policies, including its required e-prescribing standards and standards versions. In the future, the SVAP flexibility could enable developers to have the certifications of their Health IT Modules to e-prescribing criteria updated to reflect conformance of the Health IT Modules to newer versions of adopted standards that might be required by CMS Part D program or other HHS regulatory requirements before we could update the version(s) of e-prescribing standards incorporated by reference in § 170.299. This approach would avoid the need for CMS or ONC to go through joint rulemaking in order maintain programmatic alignment.

h. Updating Already Certified Health IT Leveraging SVAP Flexibility

We proposed that in instances where a health IT developer has certified a Health IT Module, including but not limited to instances where its customers are already using the certified Health IT Module, if the developer intends to update pursuant to the SVAP election, the developer will be required to provide advance notice to all affected customers and its ONC–ACB: (a) Expressing its intent to update the software to newer versions of the standard approved by the National Coordinator through the SVAP; (b) the developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world; and (c) whether the developer intends to continue to support the certificate for the existing Health IT Module version for some period of time and how long, or if the existing version of the Health IT Module certified to prior version(s) of applicable standards will be deprecated (*e.g.,* that the developer will stop supporting the earlier version of the module and request to have the certificate withdrawn) (84 FR 7498). The notice would be required to be provided sufficiently in advance of the developer establishing its planned timeframe for implementation of the upgrade to the more advanced standard(s) version(s) in order to offer customers reasonable opportunity to ask questions and plan for the update. We requested public comment on the minimum time prior to an anticipated implementation of an updated standard or implementation specification version update that should be considered reasonable for purposes of allowing customers, especially health care providers using the Health IT Module in their health care delivery operations, to adequately plan for potential implications of the update for their operations and their exchange relationships. We also requested comments on specific certification criteria, standards, characteristics of the certified Health IT Module or its implementation (such as locally hosted by the customer using it versus software-as-a-service type of implementation), or specific types or characteristics of customers that could affect the minimum advance notice that should be considered reasonable across variations in these factors (84 FR 7499).

Comments. Only a few commenters offered thoughts specifically on the minimum time prior to an anticipated implementation of an updated standard or implementation specification version update that should be considered reasonable. Several of these commenters noted that different market segments and provider types vary in their willingness or ability to upgrade to new software versions. One comment submission indicated two months would be a reasonable minimum time prior to implementation of an updated standard for their customers to be notified. Another commenter observed that the minimum timeframe prior to an anticipated implementation of an updated standard is two to four years.

Response. The comments received comport with our prior understanding that the minimum advance notice needed to offer customers reasonable opportunity to ask questions and plan for the update or modification of Health IT Modules the customers are using or have purchased and scheduled for deployment varies across different circumstances. We have, therefore, decided to finalize the advance notice requirement as proposed. The regulation text for this requirement is finalized in § 170.405(b)(8)(i). Thus, a developer choosing to take advantage of the SVAP flexibility must provide notice to its customers sufficiently in advance of the developer's anticipated timeframe for implementation of the update to the newer version(s) of applicable standard(s) to offer customers reasonable opportunity to ask questions and plan for the update. We note for clarity that we intend to apply a reasonableness standard to evaluating adequacy of advance notice timeframes for particular version updates in their specific factual contexts, prioritizing the perspective of a reasonable person in the situation of the developer's customers because this requirement is intended to protect the interests of those customers. We would anticipate that proactive engagement between the developers and their customers would result in mutually agreeable timeframes and obviate the need for us to assess reasonableness in at least the vast majority, and ideally the totality, of instances where developers choose to use the SVAP flexibility.

i. Health IT Modules Presented for Certification Leveraging SVAP Flexibility

In instances where a health IT developer presents health IT for certification to a criterion listed in § 170.405(a) to which the health IT is not already certified, we proposed that the health IT developer would be permitted to use National Coordinator-approved newer versions of any or all of the standards included in the criterion, instead of or in combination with the versions of these standards incorporated by reference in § 170.299. In such circumstances, a health IT developer would be able to choose which National Coordinator-approved standard version(s) it seeks to include in a new or updated certified Health IT Module and would be able to do so on an itemized basis. To enable this flexibility for developers seeking certification, we proposed to amend ONC–ACB Principles of Proper Conduct (PoPC) to require ONC–ACBs offer certification to National Coordinator-approved newer versions of standards and provide the ability for ONC–ACBs to accept a developer self-declaration of conformity as to the use, implementation, and conformance to a newer version of a standard (including but not limited to implementation specifications) as sufficient demonstration of conformance in circumstances where the National Coordinator has approved a version update of a standard for use in certification but no testing tool is yet available to test to the newer version (84 FR 7501).

Comments. Commenters supported the proposal to allow for both updates to existing certifications of Health IT Modules and newly sought certifications to applicable criteria to follow a process of self-declaration where approved test tools are not yet available to support conformance validation of the pertinent National Coordinator-approved newer version of a standard. A few commenters requested we clarify how developers can demonstrate conformance when a newer version of a standard is available for use under this process but does not yet have testing tools available under the Program.

Response. We proposed (84 FR 7456) and have finalized modifications in § 170.523(h) to permit ONC–ACBs to certify Health IT Modules that the ONC–ACB has evaluated for conformance with certification criteria without first passing through an ONC–ATL. As finalized, § 170.523(h)(2) provides that an ONC–ACB may certify a Health IT Module that has been evaluated by it for compliance with a conformance method approved by the National Coordinator. This provides flexibility for the National Coordinator to approve a conformance method other than ONC–ATL testing, for evaluating conformance where the National Coordinator has approved a version update of a standard for use in certification but an associated testing tool is not yet updated to test to the newer version. We have also made edits to the text in § 170.405(b) as finalized in comparison to the text included in the Proposed Rule to make more immediately clear which specific requirements apply when developers choose to take advantage of the SVAP flexibility for updating Health IT Modules already certified to a criterion listed in § 170.405(a) and which specific requirements apply when developers choose to leverage the flexibility when presenting Health IT Modules for certification to a criterion listed in § 170.405(a).

Comments. Commenters recommended HHS give health IT developers' flexibility to choose which standards to advance through this process and not obligate them to update to all possible standards at once.

Response. In the Proposed Rule, we noted (84 FR 7497) that a health IT developer would be able to choose which National Coordinator-approved standard version(s) it seeks to include in a new or updated certified Health IT Module and would be able to do so on an itemized basis. Under the finalized SVAP flexibility in § 170.405(b)(9), health IT developers are permitted to choose to use National Coordinator-approved version(s) or the version incorporated by reference in § 170.299 or both for any standard(s) included in applicable criteria it seeks to use in its certified Health IT Module(s) on an itemized, standard-by-standard basis at the developer's discretion.

In the Proposed Rule, the regulation text for all SVAP requirements was proposed to be codified in § 170.405(b)(5). The SVAP requirements, as finalized, are codified in § 170.405(b)(8) and (9). We decided to codify the finalized SVAP requirements in separate paragraphs because it complements other wording changes to the finalized regulation text that we made to make more immediately clear on the face of the regulation which specific requirements (§ 170.405(b)(8)) apply when developers choose to take advantage of the SVAP flexibility for updating Health IT Modules already certified to a criterion listed in § 170.405(a) and which specific requirements (§ 170.405(b)(9)) apply when developers choose to leverage the flexibility when presenting Health IT Modules for certification to a criterion listed in § 170.405(a).

j. Requirements Associated With All Health IT Modules Certified Leveraging SVAP

As outlined in the Proposed Rule (84 FR 7499), in all cases, regardless of whether a health IT developer is updating an existing certified Health IT Module or presenting a new Health IT Module for certification to new versions of adopted standards approved by the National Coordinator through the Standards Version Advancement Process, we proposed that any developer choosing to take advantage of the proposed flexibility would need to:

- Ensure its mandatory disclosures in § 170.523(k)(1) appropriately reflect its use of any National Coordinator-approved newer versions of adopted standards; and
- Address and adhere to all Program requirements—including but not limited to Conditions of Certification and Maintenance of Certification requirements—that are applicable to its certified Health IT Modules regardless of whether those Health IT Modules were certified to the adopted standards found in 45 CFR part 170 or National Coordinator-approved newer version(s) of the adopted standard(s).

For example, as we proposed, a developer would need to ensure that its real world testing plan and actual real world testing include the National Coordinator-approved newer versions of standards to which it is claiming conformance, beginning with the plan for and real world testing conducted in the year immediately following the first year the developer's applicable Health IT Module(s) were, as of August 31, certified to the National Coordinator-approved newer versions of standards.

Under the policies outlined in the Proposed Rule, developers would be held accountable for maintaining all applicable certified Health IT Modules in conformance with any National Coordinator-approved newer versions of standards and implementation specifications that they voluntarily elect to use in their certified health IT under the real world testing Condition and Maintenance of Certification requirements proposed in § 170.405, the attestations Condition and Maintenance of Certification requirements proposed in § 170.406, and through ONC–ACB surveillance applying to certificates that include National Coordinator-approved updated versions as it does to those that do not. We also included discussion indicating our intent that developers would be accountable for correcting

non-conformities with certification criteria that were discovered in real world testing of a Health IT Module certified using National Coordinator-approved newer versions. Under the proposed policies, prompt corrective action would be required by a developer discovering such non-conformity through real world testing, in similar manner as a developer would be accountable for correcting non-conformities discovered through real world testing of Health IT Modules certified using only the versions of Secretary-adopted standards that are incorporated by reference in § 170.299, or through other Program means.

Comments. We did not receive specific comments on these general requirements and details of the relationship between the proposed SVAP and other proposed Program enhancements or existing accountability mechanisms.

Response. We have finalized these details of our SVAP policies as proposed.

We stated in the Proposed Rule that we anticipate providing ONC–ACBs (and/or health IT developers) with a means to attribute information on Health IT Modules' support for National Coordinator-approved updated versions of standards to the listings on the CHPL for the Health IT Modules the ONC–ACB has certified, and proposed to require in the PoPC for ONC–ACBs that they are ultimately responsible for this information being made publicly available on the CHPL (84 FR 7501). We requested public comment on any additional information about updated standards versions that may be beneficial to have listed with certified Health IT Modules on the CHPL.

Comments. One commenter recommended ONC provide a method on the ONC CHPL for documenting the dot version/release associated with the new standard version implementation and clarify the ONC–ACBs reporting timeline for these types of standard version updates.

Response. We thank the commenter for the feedback, which will help to inform our internal deliberations about future operational planning.

k. Advanced Version Approval for SVAP

The Proposed Rule (84 FR 7500) included discussion of how, after a standard has been adopted through notice and comment rulemaking, ONC anticipated undertaking an open and transparent process to timely ascertain whether a more recent version of any standard or implementation specification that the Secretary as adopted in part 170 should be approved for developers' voluntary use under the Program. We requested commenters' input on our anticipated approach to standards and implementation specification advanced version approval as outlined in the Proposed Rule.

Comments. Some commenters expressed concerns that appeared to suggest an understanding that the SVAP would be used to adopt new standards into the Program.

Response. As stated in the Proposed Rule, the SVAP flexibility can only be used for newer (sometimes known as ''updated'') versions of standards and implementation specifications that the Secretary has already adopted through notice-and-comment rulemaking.[114]

Comments. One commenter urged that in order to be considered for approval for voluntary use under the Program the full details of a version of a standard should be required to be publicly available online by the start of opportunity for public review and discussion of the list of versions under consideration.

Response. We appreciate the feedback. Although specifics of operational processes are outside the scope of this rule, we wish to reassure all stakeholders that we do appreciate the value of ensuring public dialogue around such matters as consideration of standards versions for potential voluntary use in the program is appropriately supported by availability of relevant information. As we operationalize support for finalized policies including the SVAP, we plan to provide ample public outreach and communications through channels familiar to affected stakeholders—including but not limited to ONC's *HealthIT.gov* website.

Comments. Several commenters suggested various potential features or processes that could be used in ascertaining whether a more recent version of any standard or implementation specification that the Secretary as adopted in part 170 should be approved by the National Coordinator for developers' voluntary use under the Program. We also received several comments regarding potential uses of information from the standards review and approval processes or the SVAP flexibility itself to inform assessments of various aspects of the health IT ecosystem such as the maturity and uptake of specific standards versions.

Response. Although addressing their substance is outside the scope of this final rule, we appreciate these responses to our call for comments. This information will help to inform our deliberations about future program policies and operations.

l. Real World Testing Principles of Proper Conduct for ONC–ACBs

We proposed to include a new PoPC for ONC–ACBs in § 170.523(p) that would require ONC–ACBs to review and confirm that applicable health IT developers submit real world testing plans and results in accordance with our proposals (84 FR 7501). The proposed requirement was that the ONC–ACBs review the plans for completeness. Once completeness is confirmed, we proposed that ONC–ACBs would provide the plans to ONC and make them publicly available by December 15 of each year (see § 170.523(p)(1) and (3) in 84 FR 7598). We proposed that for the reasons discussed above in context of developer requirements, we have finalized (in § 170.405(b)(1)) December 15 of each year as the due date for the annual real world testing plans. We proposed in § 170.523(p)(2) that the ONC–ACB would ''review and confirm that applicable health IT developers submit real world testing results in accordance with § 70.405(b)(2).'' And in § 170.523(p)(3) we proposed that the ONC–ACBs would be required to submit real world testing results by April 1 of each year to ONC for public availability (84 FR 7598).

Comments. The only comments received relevant to these PoPC proposals were about due dates, and were summarized above in context of the § 170.405 requirements applicable to developers (see section VII.B.5.d *Submission Dates,* in this final rule).

Response. We thank commenters again for their feedback on this proposal and have finalized the PoPC (170.523(p)(1)–(3)) as proposed, with the exception of having adjusted in § 170.523(p)(3) the annual due date for publication of developers' real world testing results reports on CHPL from the proposed April 1 to the finalized March 15 date.

Because we proposed to allow health IT developers to implement National Coordinator-approved newer versions of adopted standards and implementation specifications in certified Health IT

[114] As also noted in the Proposed Rule, this policy considers the substance of a standard and not whether its name or version naming and identification track remains unchanged over time, as standards developing organizations and processes may apply different naming or identification methods from one version to another of the same standards or implementation specifications. For more information on version naming and identification tracks for standards and implementation specifications, please see the Proposed Rule (84 FR 7500).

Modules, we proposed two requirements to ensure the public has knowledge and ONC–ACBs can maintain appropriate oversight and surveillance of the version of a standard that certified health IT meets. First, we proposed to revise the PoPCs in § 170.523(m) to add subparagraph (4) requiring ONC–ACBs to aggregate, no less than quarterly, all updates successfully made to use newer versions of adopted standards in certified health IT per the requirements for developers choosing to take advantage of the SVAP flexibility. This would ensure that ONC is aware of the version of a standard that certified health IT meets for the purposes of Program administration. Second, we proposed, that a developer that chooses to avail itself of the SVAP flexibility must address its use of newer versions of adopted standards in its real world testing plans and results.

We sought comment on the proposed additions to the PoPC for ONC–ACBs. More specifically, we sought comment on whether ONC–ACBs should be required to perform an evaluation beyond a completeness check for the real world testing plans and results and the value versus the burden of such an endeavor.

Comments. We did not receive any comments on this proposal.

Response. The substance of the requirement is finalized as proposed, though, we have made clarifying edits to the way in which the PoPC amendments are organized and phrased. The requirement proposed in § 170.523(m)(4) (84 FR 7599) has been re-designated in § 170.523(m)(5). In the finalized § 170.523(m)(5), we have revised the citation to the SVAP requirements because they were proposed in § 170.405(b)(5) but are finalized in § 170.405(b)(8) and (9). The wording of requirement finalized in § 170.523(m)(5) was modified in comparison to that proposed in 84 FR 7599 to make clear that ONC–ACBs are required to report on all certifications of Health IT Modules to National Coordinator-approved newer versions of Secretary-adopted standards, both those updated to include newer versions of adopted standards and those of Health IT Modules first presented for certification using newer versions of adopted standards. Another modification to the finalized regulation text in § 170.523(m)(5) in comparison with that proposed clarifies that ONC–ACBs are permitted to obtain the quarterly record of successful use in certified Health IT Modules of newer versions of adopted standards from the ONC–ACB's records of certification activity. We believe this clarification is important to ensure the regulation text finalized in § 170.523(m)(5) cannot be misconstrued as precluding use of such records as the data source for this requirement.

In complement to the above requirements to ensure transparency for the public and end users, we proposed in § 170.523(t) a new PoPC for ONC–ACBs requiring them to ensure that developers seeking to take advantage of the SVAP flexibility in § 170.405(b) comply with the applicable requirements, and that the ONC–ACB both retain records of the timing and content of developers' required [115] notices and ensure each notice is timely and publicly accessible, and easily located via the CHPL through attribution of the notice to the certified Health IT Modules to which it applies.[116]

We note that in the proposed regulation text in § 170.523(t) as published in 84 FR 7598, there was an editorial error. The editorial error was in title in § 170.523(t) as published in 84 FR 7598, which read ''Standards Voluntary Advancement Process'' instead of ''Standards Version Advancement Process,'' although the proposed introductory text correctly referenced ''Standards Version Advancement Process.''

Comments. We did not receive public comment on the proposed paragraph (t) or its addition to § 170.523.

Response. We have finalized § 170.523(t) with a revised title more consistent with the finalized titles of paragraphs (8) and (9) in § 170.405(b), and a revised citation to § 170.405. The citation to § 170.405 was revised because the SVAP requirements 170.523(t) references were proposed in § 170.405(b)(5) but have been finalized in § 170.405(b)(8) and (9). The substance of the PoPC requirement in § 170.523(t) is finalized as proposed.

m. Health IT Module Certification & Certification to Newer Versions of Certain Standards

We proposed to add in § 170.550, Health IT Module certification, a new paragraph (e), which would require that ONC–ACBs must provide an option for certification of Health IT Modules to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification through the Standards Version Advancement Process (84 FR 7598).

Comments. We received no public comments on this proposed addition to § 170.550 to accommodate the SVAP flexibility.

Response. We have finalized the substance of § 170.550(e) as proposed. We have modified the regulatory text finalized in § 170.550(e) in comparison with that proposed in 84 FR 7598 by adding a header. The finalized paragraph reads: ''*Standards Updates.* ONC–ACBs must provide an option for certification of Health IT Modules to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification.''

We proposed to revise § 170.555(b)(1) to accommodate the SVAP flexibility. The revised text in § 170.555(b)(1) as proposed (84 FR 7598) read: ONC–ACBs are not required to certify Complete EHRs and/or Health IT Module(s) according to newer versions of standards adopted and named in subpart B of this part, unless: (i) The National Coordinator identifies a newer version through the Standards Version Advancement Process and a health IT developer voluntarily elects to seek certification of its health IT in accordance with § 170.405(b)(5); or (ii) The new version is incorporated by reference in § 170.299.

Comments. We did not receive public comments on revising paragraph (b)(1) of § 170.555 to accommodate the SVAP flexibility.

Response. We have finalized the substance of this revision as proposed. However, we have struck ''Complete EHRs and/or'' from the text finalized in § 170.555(b)(1) consistent with our finalizing the removal from 45 CFR part 170 of references to ''Complete EHRs'' in conjunction with the removal of the 2014 Edition (as discussed in section III.B.2 of this final rule). We have clarified the text in § 170.555(b)(1) as finalized to use the word ''approves'' in place of ''identifies,'' consistent with our phrasing and terminology throughout the preamble of this final rule and finalized regulation text implementing the SVAP flexibility. We have replaced ''under the Standards Version Advancement Process'' with ''for use in certification'' because we

[115] The advance notice requirement that was proposed in § 170.405(b)(5)(i) and that is now finalized in § 170.405(b)(8)(i) remains specific to developers leveraging SVAP flexibility to update Health IT Modules with existing certifications.

[116] We note for clarity that whether a copy of the content is hosted on CHPL, made available via a publicly accessible hyperlink provided by the developer, or another mechanism or method that may emerge as a more advanced and efficient technical approach to achieving this same goal is an operational detail and does not need to be defined in rulemaking.

believe this wording prevents potential confusion about whether the term ''Standards Version Advancement Process'' refers to the administrative flexibility established in § 170.405(b)(8) and (9) or to the National Coordinator's approach to approving versions for use in the Program. We have also revised the citation to § 170.405(b) in the finalized text in § 170.555 because the SVAP provisions proposed in § 170.405(b)(5) have been finalized in § 170.405(b)(8) and (9).

6. Attestations

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification requirement under the Program, provide to the Secretary an attestation to all of the Conditions of Certification requirements specified in PHSA § 3001(c)(5)(D), except for the ''EHR reporting criteria submission'' Condition of Certification requirement in § 3001(c)(5)(D)(vii). We proposed to implement the Cures Act by requiring health IT developers to attest, as applicable, to compliance with the Conditions and Maintenance of Certification requirements proposed in §§ 170.401 through 170.405.

We proposed that, as a Maintenance of Certification requirement for the ''attestations'' Condition of Certification requirement under § 170.406(b), health IT developers would need to submit their attestations every 6 months (*i.e.,* semiannually). We proposed to provide a 14-day attestation period twice a year. For health IT developers presenting Health IT Modules for certification for the first time under the Program, we proposed that they would be required to submit an attestation at the time of certification and also comply with the semiannual attestation periods. As stated in the Proposed Rule, we would publicize and prompt developers to complete their attestation during the required attestation periods. We also proposed to provide a method for health IT developers to indicate their compliance, noncompliance with, or the inapplicability of each Condition and Maintenance of Certification requirement as it applies to all of their health IT certified under the Program for each attestation period. Last, we proposed to provide health IT developers the flexibility to specify noncompliance per certified Health IT Module, if necessary. We noted, however, that any noncompliance with the proposed Conditions and Maintenance of Certification requirements, including the ''attestations'' Conditions and Maintenance of Certification requirements, would be subject to ONC direct review, corrective action, and enforcement procedures under the Program.

We welcomed comments on the proposed attestations Condition and Maintenance of Certification requirements, including the appropriate frequency and timing of attestations. We also welcomed comments on the proposed responsibilities for ONC–ACBs related to the attestations of Condition and Maintenance of Certification requirements.

Comments. We received many comments supporting the ''attestations'' Condition and Maintenance of Certification requirements. Commenters generally agreed that health IT developers should attest that they are complying with all the required Conditions and Maintenance of Certification requirements. A few commenters were concerned that the Condition of Certification requirements set up unreasonable expectations that health IT developers attest to statements that are subject to interpretation and are ambiguous, and that developers should be able to articulate how their software and businesses meet the expectations.

We also received comments suggesting ways to reduce burden for health IT developers. Some commenters suggested less frequent attestation periods ranging from once a year to every two years as a means for reducing burden on health IT developers. Another commenter suggested that we send reminders to health IT developers when an attestation(s) needs renewal. One commenter recommended that we include a specific deadline at the middle and end of each year for attestations in lieu of the proposed predefined 14-day attestation window. Another commenter recommended that attestations should only be sent electronically as any other process of reporting (*e.g.,* written letter) would be onerous on all parties.

Response. We thank commenters for their support and have adopted in § 170.406 the ''attestations'' Conditions and Maintenance of Certification requirement with revisions discussed below. These revisions should both provide clarity for compliance and reduce burden.

Health IT developers will be attesting to the Conditions of Certification that are statutory requirements under section 4002 of the Cures Act. This final rule also addresses concerns of ambiguity and interpretation by revising the Conditions and Maintenance of Certification requirements and the information blocking provision, which is a Condition of Certification in § 170.401. We have also revised § 170.406 to provide further clarity on the applicability of each of the Conditions and Maintenance of Certification requirements to health IT developers for the purposes of attestation. For example, all health IT developers under the Program would attest to the ''information blocking'' Condition of Certification requirement (§ 170.401), while only health IT developers that have health IT certified to the ''API'' certification criteria (§ 170.315(g)(7)–(10)) would be required to attest to the ''API'' Condition of Certification and Maintenance requirements (§ 170.404). We have also revised the ''attestations'' Conditions and Maintenance of Certification requirements in § 170.406 to clearly reflect that all attestations must be approved and submitted by an officer, employee, or other representative the health IT developer has authorized to make a binding attestation(s) on behalf of the health IT developer. This provides regulatory clarity for health IT developers as to their responsibility under the attestation provisions (§ 170.406).

A requirement of attestation every 6 months properly balances the need to support enforcement actions with the attestation burden placed on developers. In this regard, allegations of inappropriate actions and non-compliance by health IT developers with Program requirements and the information blocking provision can be more readily cross-referenced against their attestations for enforcement purposes comparative to a one-year or two-year attestation period. Based on the efficient methods we are establishing for attestation as described below, we believe that we have implemented this statutory requirement for health IT developers in ways that will reduce the compliance burden for them. We also refer readers to section VII.D of this preamble for discussion of ONC direct review, corrective action, and enforcement procedures for the Conditions and Maintenance of Certification requirements under the Program.

We recognize comments expressing concerns on the potential burden placed on health IT developers to attest semiannually. The process we plan to implement for providing attestations should minimize burden on health IT developers. To further minimize potential burden on health IT developers, we have revised the proposed 14-day attestation window to extend the window to 30 days. In other words, health IT developers will be able to submit their attestations within a

designated 30-day window twice a year for purposes of compliance. To note, in accordance with § 170.406(b), the first attestation window will begin April 1, 2021. This attestation period will cover the time period from the effective date of the final rule through March 31, 2021. This irregular time period is due to the publication of the final rule. Subsequently, a regular 6-month period will commence with the attestation window for the 6-month period opening on October 1, 2021 (attesting for the period of April 1 through September 30). We have also revised the Conditions and Maintenance of Certification requirements to reflect that all health IT developers under the Program would adhere to a similar semiannual attestation schedule, rather than new health IT developers also attesting at the time of certification. We believe this is more practical, less burdensome for health IT developers and ONC–ACBs, and creates less confusion as to what actions and statements a health IT developer is attesting to (*i.e.,* for past actions under the Program).

As stated in the Proposed Rule, we plan to implement several other means to minimize burden. First, we plan to publicize and prompt developers to complete their attestation during the required attestation periods. Second, as proposed in the Proposed Rule, we will provide a method for health IT developers to indicate their compliance, noncompliance, or the inapplicability of each Condition and Maintenance of Certification requirement as it applies to all or each of their Health IT Modules certified under the Program for each attestation period. Third, to clarify our proposal and respond to the comment recommending electronic submission, we note ONC–ACBs have discretion to specify the format and may choose to require electronic submission. In addition, to support electronic submission, we will provide a web-based form and method for health IT developers to submit attestations in an efficient manner for ONC–ACBs' review.

ONC–ACB Responsibilities

We proposed that attestations would be submitted to ONC–ACBs and reviewed in accordance with § 170.523(q) as a means for ONC–ACBs to monitor health IT developers for compliance with Program requirements. ONC–ACBs would be required to share the attestations with ONC. ONC would then make the attestations publicly available through the CHPL. The other responsibility we proposed in § 170.550(l) was that before issuing a certification, an ONC–ACB would need to ensure that the health IT developer of the Health IT Module has met its responsibilities related to the Conditions and Maintenance of Certification requirements as solely evidenced by its attestation. For example, if a health IT developer with an active certification under the Program provided noncompliant designations in their attestation but was already participating in a corrective action plan (CAP) under ONC direct review to resolve the noncompliance, certification would be able to proceed while the issue is being resolved.

Comments. One commenter requested clarification on the specific responsibilities of ONC–ACBs when collecting and submitting attestations to ONC, including instances of an attestation indicating non-conformity and the lack of a submission of an attestation by a health IT developer.

Response. We thank commenters for their input and have finalized as proposed. We refer readers to section VII.D for further discussion of ONC direct review, corrective action, and enforcement procedures for the Conditions and Maintenance of Certification requirements under the Program, including the roles of ONC–ACBs in enforcement of the Conditions and Maintenance of Certification requirements.

7. EHR Reporting Criteria Submission

As stated in the Proposed Rule, the Cures Act specifies that health IT developers shall be required, as a Condition and Maintenance of Certification requirement under the Program, to submit certain information to satisfy the reporting criteria on certified health IT in accordance with the EHR Reporting Program requirements established under section 3009A of the PHSA, as added by section 4002 of the Cures Act. We have not yet established an EHR Reporting Program. Once ONC establishes such an EHR Reporting Program, we will undertake future rulemaking to propose and implement the associated Condition and Maintenance of Certification requirement(s) for health IT developers.

C. Compliance

The Maintenance of Certification requirements discussed above do not necessarily define all the outcomes necessary to meet the Conditions of Certification. Rather, they provide preliminary or baseline evidence toward measuring whether a Condition of Certification requirement is being met. Thus, ONC could determine that a Condition of Certification requirement is not being met through reasons other than the Maintenance of Certification requirements. For example, meeting the Maintenance of Certification requirement that requires a health IT developer to not establish or enforce any contract or agreement that contravenes the Communications Condition of Certification requirement does not excuse a health IT developer from meeting all the requirements specified in the Communications Condition of Certification requirement. This is analogous to clarifications ONC has previously provided about certification criteria requirements whereby testing prior to certification sometimes only tests a subset of the full criterion's intended functions and scope. However, for compliance and surveillance purposes, we have stated that ONC and its ONC–ACBs will examine whether the certified health IT meets the full scope of the certification criterion rather than the subset of functions it was tested against (80 FR 62709 and 62710).

Comments. We did not receive any comments specific to compliance with Maintenance of Certification requirements as related to meeting Conditions of Certification requirements.

Response. We continue to maintain our position that Maintenance of Certification requirements do not define all of the outcomes necessary to meet the Conditions of Certification requirements. Thus, while complying with Maintenance of Certification requirements will provide evidence toward measuring whether a Condition of Certification requirement is being met, reasons beyond the Maintenance of Certification requirements could result in ONC determining that a Condition of Certification requirement has not been met.

D. Enforcement

The Cures Act affirms ONC's role in using certification to improve health IT's capabilities for the access, use, and exchange of EHI. The Cures Act provides this affirmation through expanded certification authority for ONC to establish Conditions and Maintenance of Certification requirements for health IT developers that go beyond the certified health IT itself. The new Conditions and Maintenance of Certification requirements in section 4002 of the Cures Act focus on the actions and business practices of health IT developers (*e.g.,* information blocking and appropriate access, use, and exchange of electronic health information) as well as technical interoperability of health IT (*e.g.,* APIs and real world testing). Furthermore

and equally important, section 4002 of the Cures Act provides that the Secretary of HHS may encourage compliance with the Conditions and Maintenance of Certification requirements and take action to discourage noncompliance. Given these considerations, we proposed a general enforcement framework outlining a corrective action process for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement has not been or is not being met by a health IT developer under the Program, including the requirement for a health IT developer to attest to meeting the Conditions and Maintenance of Certification requirements.

1. ONC Direct Review of the Conditions and Maintenance of Certification Requirements

Historically we utilized the processes previously established for ONC direct review of certified health IT in the ONC Health IT Certification Program: Enhanced Oversight and Accountability Act (EOA) final rule (81 FR 72404), and as codified in §§ 170.580 and 170.581, to address non-conformities with Program requirements. For multiple reasons, we proposed in 84 FR 7503 to utilize substantially the same processes for the enforcement of the Conditions and Maintenance of Certification requirements. First, these processes were designed to address non-conformities with Program requirements. Conditions and Maintenance of Certification requirements have been adopted as Program requirements and, as such, any noncompliance with the Conditions and Maintenance of Certification requirements constitutes a Program non-conformity. Second, health IT developers are familiar with the ONC direct review provisions as they were established by the EOA final rule in October 2016. Third, §§ 170.580 and 170.581 have provided thorough and transparent processes for working with health IT developers through notice and corrective action to remedy Program non-conformities. Last, the direct review framework has provided equitable opportunities for health IT developers to respond to ONC actions and appeal certain ONC determinations.

As further discussed below, we have finalized our proposed approach to utilize the processes previously established and codified in §§ 170.580 and 170.581 for ONC direct review of certified health IT for the enforcement of the Conditions and Maintenance of Certification requirements, along with our proposed revisions to these processes in order to properly incorporate enforcement of these requirements. We note that the Information Blocking Condition of Certification (§ 170.401) and the related Assurances Condition of Certification requirement (§ 170.402(a)(1)) have a delayed enforcement date of 6 months after date of publication of the final rule.

2. Review and Enforcement Only by ONC

We proposed in 84 FR 7503 to retain use of the term ''direct review'' as previously adopted in the EOA final rule to continue to distinguish actions ONC takes to directly review certified health IT or health IT developers' actions from actions taken by an ONC–ACB to review certified health IT under surveillance. We proposed, however, that ONC would be the sole party responsible for enforcing compliance with the Conditions and Maintenance of Certification requirements.

Comments. We received comments requesting clarification that ONC–ACBs are not responsible for enforcement of the Conditions and Maintenance of Certification requirements.

Response. We have finalized this review and enforcement approach in §§ 170.580(a)(1) and 170.580(a)(2)(iii) as proposed above. We clarify that ONC–ACBs are not responsible for enforcement of the Conditions and Maintenance of Certification requirements. Under finalized § 170.523(s), and as further discussed later in this section, ONC–ACBs must report any information that could inform whether ONC should exercise direct review of noncompliance with the Conditions and Maintenance of Certification requirements to ONC. ONC–ACBs also address non-conformities with technical and other Program requirements through surveillance and by working with health IT developers through corrective action plans.

3. Review Processes

As discussed above, we proposed to utilize the processes previously established and codified in §§ 170.580 and 170.581 for ONC's direct review and enforcement of the Conditions and Maintenance of Certification requirements, along with certain proposed revisions and additions to these processes to properly incorporate enforcement of these requirements and effectuate congressional intent conveyed through the Cures Act.

a. Initiating Review and Health IT Developer Notice

We proposed in 84 FR 7503 to fully incorporate the review of compliance with the Conditions and Maintenance of Certification requirements into the provisions of § 170.580(a) and (b). We proposed in § 170.580(a)(2)(iii) that if ONC has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement, then it may initiate direct review. Similarly, we proposed in § 170.580(b)(1) and (2) that ONC may issue the health IT developer a notice of potential non-conformity or notice of non-conformity and provide the health IT developer an opportunity to respond with an explanation and written documentation, including any information ONC requests.

Comments. We received one comment that ONC should communicate with a representative sample of users of a health IT product when enforcing the Conditions and Maintenance of Certification requirements.

Response. We appreciate this comment. We are committed to consistent and thorough enforcement of the Conditions and Maintenance of Certification requirements and review of complaints of noncompliance. Our goal is to work with developers to remedy any noncompliance in a timely manner. During the course of our review of a potential noncompliance, we may communicate with users of the health IT, as appropriate. We have finalized this approach regarding initiation of review and health IT developer notice in §§ 170.580(a)(2)(iii) and 170.580(b) as proposed.

i. Complaint Resolution

In the Proposed Rule, we noted and recommended in 84 FR 7503 that customers and end users first work with their health IT developers to resolve any issues of potential noncompliance with the Conditions and Maintenance of Certification requirements. We proposed that if the issue cannot be resolved, the end user should contact the ONC–ACB for assessment. However, as discussed above and in section VII.D.5 below, the ONC–ACB purview for certified health IT generally applies to certified capabilities and limited requirements of developer business practices. We proposed that if neither of these pathways resolves the issue, end users may want to provide feedback to ONC via the Health IT Feedback Form.

Comments. We received one comment recommending that we require complaints regarding developer compliance with Conditions and

Maintenance of Certification requirements go directly to ONC rather than to an ONC–ACB. Another commenter requested that we provide guidance regarding how to report issues related to developer compliance.

Response. We have finalized in § 170.580 our proposed approach regarding complaint resolution as described above, which is guided by prior Program experience.

Comments. One commenter recommended that we adopt a self-disclosure mechanism for health IT developers to report any non-conformity with the Program and enable such self-disclosure to offer health IT developers regulatory protection.

Response. We appreciate the comment and strongly encourage self-disclosure by developers, which health IT developers currently do under the Program. We note that currently there are methods by which health IT developers may communicate with ONC–ACBs and/or ONC, and it is our longstanding policy to work with health IT developers to correct non-conformities. While we believe this approach works well, consistent with Executive Order 13892, we are considering whether it would be appropriate to adopt additional procedures that further encourage self-reporting of non-conformities and voluntary information sharing, as well as procedures to provide pre-enforcement rulings to health IT developers who make inquiries regarding their compliance with regulatory requirements.

ii. Method of Correspondence With Health IT Developers

Section 170.505 states that correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. We noted in the Proposed Rule in 84 FR 7503 that in the EOA final rule we signaled our intent to send notices of potential non-conformity, non-conformity, suspension, proposed termination, and termination via certified mail (81 FR 72429). However, we proposed to follow § 170.505 for correspondence regarding direct review of noncompliance with the Conditions and Maintenance of Certification requirements.

As discussed in the Proposed Rule, the type and extent of review by ONC could vary significantly based on the complexity and severity of each fact pattern. For instance, ONC may be able to address certain noncompliance with the Conditions and Maintenance of Certification requirements quickly and with minimal effort (*e.g.,* failure to make public a documentation hyperlink), while other situations may be more complex and require additional time and effort (*e.g.,* violation of API fee prohibitions). Considering this wide range of potential noncompliance with the Conditions and Maintenance of Certification requirements, we proposed that ONC retain discretion to decide, on a case-by-case basis, when to go beyond the provisions of § 170.505 to use means other than email in providing notices and correspondence for noncompliance with the Conditions and Maintenance of Certification requirements.

We solicited comment on the nature and types of noncompliance with the Conditions and Maintenance of Certification requirements that ONC should consider in determining the method of correspondence. We also solicited comment on whether the type of notice should determine the method of correspondence. More specifically, we solicited comment on whether certain types of notices under direct review should be considered more critical than others, thus requiring a specific method of correspondence.

Comments. We received several comments regarding the proposed method of correspondence with health IT developers. Some commenters stressed that time-sensitive notifications should not be sent via email, with one commenter noting that ONC should use certified mail, with a copy to a designated notice recipient, for notices of potential noncompliance and noncompliance with the Conditions and Maintenance of Certification requirements. Other commenters suggested that ONC should use both email and certified mail for notices regarding initiation of direct review, potential non-conformity, non-conformity, suspension, proposed termination, and termination. One commenter recommended ONC acknowledge receipt of communications received.

Response. We appreciate commenters' support of our proposals, as well as the constructive suggestions. We have finalized our proposal to use the provisions in § 170.505 for correspondence regarding noncompliance with the Conditions and Maintenance of Certification requirements, with minor revisions. While we agree with commenters that there may be situations when sending notice only via email would not be adequate, such situations would be contingent on the circumstances as described in the Proposed Rule. Therefore, we have revised the regulation text of § 170.505 to specify some of those considerations. These considerations include, but are not limited to, whether: The party requests use of correspondence beyond email; the party has responded via email to our communications; we have sufficient information from the party to ensure appropriate delivery of such notice; and, importantly, the alleged violation of a Condition or Maintenance of Certification requirement or other Program requirement within ONC's purview under § 170.580 indicates a serious violation of the Program with potential consequences of suspension, certification termination, or a certification ban.

We did not propose any requirements regarding acknowledgment of receipt, and we have finalized our proposed approach to utilize the processes previously established and codified in §§ 170.580 and 170.581 for ONC direct review of certified health IT for the enforcement of the Conditions and Maintenance of Certification requirements, which include response requirements already codified in §§ 170.580 and 170.581.

Comments. One commenter requested clarification on ONC's timeframe for responding to health IT developers during direct review. Another commenter requested clarity on investigation timelines generally.

Response. We have finalized our proposed approach to utilize the processes previously established and currently codified in §§ 170.580 and 170.581 for ONC's direct review and enforcement of the Conditions and Maintenance of Certification requirements, which include specific response timeframes throughout the direct review process. We refer commenters to §§ 170.580 and 170.581 for the timeframes applicable to the various steps in the direct review process. We also clarify that proposed termination and suspension are excluded from ONC's direct review process for the Conditions and Maintenance of Certification requirements, so any timeframes related to proposed termination and suspension do not apply.

b. Relationship With ONC–ACBs and ONC–ATLs

Section 170.580(a)(3) outlines ONC direct review in relation to the roles of ONC–ACBs and ONC–ATLs, which we proposed to revise to incorporate the Conditions and Maintenance of Certification requirements. In the Proposed Rule in 84 FR 7507, we provided situational examples in section VII.D.5 ''Effect on Existing Program Requirements and Processes''

regarding ONC direct review and the role of an ONC–ACB. As finalized in the EOA final rule and per § 170.580(a)(3)(v), we stressed that ONC may refer the applicable part of its review of certified health IT to the relevant ONC–ACB(s) if ONC determines this would serve the effective administration or oversight of the Program (81 FR 72427 and 72428).

We did not receive comments on this specific aspect of the proposed rule and have finalized the relationship with ONC–ACBs and ONC–ATLs in § 170.580(a)(3) as proposed.

c. Records Access

We proposed in 84 FR 7504 to revise § 170.580(b)(3) to ensure that ONC, or third parties acting on its behalf, have access to the information necessary to enforce the Conditions and Maintenance of Certification requirements. As specified in § 170.580(b)(1)(ii)(A)(*2*), (b)(2)(ii)(A)(*2*) and (b)(3), in response to a notice of potential non-conformity or notice of non-conformity, ONC must be granted access to, and have the ability to share within HHS, with other Federal agencies, and with appropriate entities, all of a health IT developers' records and technology related to the development, testing, certification, implementation, maintenance, and use of its certified health IT, and any complaint records related to the certified health IT. ''Complaint records'' include, but are not limited to issue logs and help desk tickets (81 FR 72431). We proposed in 84 FR 7504 to supplement these requirements with a requirement that a health IT developer make available to ONC, and third parties acting on its behalf, records related to marketing and distribution, communications, contracts, and any other information relevant to compliance with any of the Conditions and Maintenance of Certification requirements or other Program requirements. If ONC determined that a health IT developer was not cooperative with the fact-finding process, we proposed ONC would have the ability to issue a certification ban and/or terminate a certificate (see § 170.581 discussed below and § 170.580(f)(1)(iii)(A)(*1*)).

We proposed in 84 FR 7504 that ONC would implement appropriate safeguards to ensure, to the extent permissible with Federal law, that any proprietary business information or trade secrets ONC may encounter by accessing the health IT developer's records, other information, or technology, would be kept confidential by ONC or any third parties working on behalf of ONC.

Comments. We received one comment recommending that ONC detail the procedural and technical safeguards in place to protect information submitted to ONC by a developer as part of direct review of compliance with a Conditions or Maintenance of Certification requirement.

Response. As we stated above, in the Proposed Rule, and in the EOA final rule (81 FR 72429), we will implement appropriate safeguards to ensure, to the extent permissible with Federal law, that any proprietary business information or trade secrets ONC may encounter by accessing the health IT developer's records, other information, or technology, will be kept confidential by ONC or any third parties working on behalf of ONC. We have finalized in § 170.580(b)(3) our approach regarding records access as proposed. Additionally, we have finalized our recommendation, stated in 84 FR 7504 in the Proposed Rule and the EOA final rule, that health IT developers clearly mark, as described in HHS Freedom of Information Act regulations at 45 CFR 5.65(c), any information they regard as trade secret or confidential prior to disclosing the information to ONC (81 FR 72431).

d. Corrective Action

We proposed in 84 FR 7504 that if ONC determines that a health IT developer is noncompliant with a Condition or Maintenance of Certification requirement (*i.e.,* a non-conformity), ONC would work with the health IT developer to establish a corrective action plan (CAP) to remedy the issue through the processes specified in § 170.580(b)(2)(ii)(A)(*4*) and (c). We noted that a health IT developer may be in noncompliance with more than one Condition or Maintenance of Certification requirement. In such cases, we proposed that ONC would follow the proposed compliance enforcement process for each Condition or Maintenance of Certification requirement accordingly, but may also require the health IT developer to address all violations in one CAP for efficiency of process. We also proposed, as we currently do with CAPs for certified health IT, to list health IT developers under a CAP on ONC's website.

We did not receive any comments on this aspect of the Proposed Rule, and in § 170.580(c) we have finalized our proposals regarding corrective action as proposed (84 FR 7504).

e. Certification Ban and Termination

We proposed in 84 FR 7504 that if a health IT developer under ONC direct review for noncompliance with a Condition or Maintenance of Certification requirement failed to work with ONC or was otherwise noncompliant with the requirements of the CAP and/or CAP process, ONC could issue a certification ban for the health IT developer (and its subsidiaries and successors). A certification ban, as it currently does for other matters under § 170.581, would prohibit future health IT by the health IT developer from being certified.

We proposed in 84 FR 7504 that ONC would also consider termination of the certificate(s) of the affected Health IT Module(s) should the health IT developer fail to work with ONC or is otherwise noncompliant with the requirements of the CAP and/or CAP process. We proposed that ONC may consider termination if there is a nexus between the developer's actions or business practices in relation to the Conditions and Maintenance of Certification requirements and the functionality of the affected certified Health IT Module(s). For example, as discussed in the Proposed Rule, ONC may determine that a health IT developer is violating a Condition of Certification requirement due to a clause in its contracts that prevents its users from sharing or discussing technological impediments to information exchange. In this example, the health IT developer's conduct would violate the Communications Condition of Certification requirement that we have finalized in § 170.403. If the same conduct were also found to impair the functionality of the certified Health IT Module (such as by preventing the proper use of certified capabilities for the exchange of EHI), ONC may determine that a nexus exists between the developer's business practices and the functionality of the certified Health IT Module, and may consider termination of the certificate(s) of that particular Health IT Module under the proposed approach.

We proposed this approach, which allows ONC to initiate a certification ban and/or certificate termination under certain circumstances, to ensure that health IT developers are acting in accordance with the Conditions and Maintenance of Certification requirements. However, we stressed that our first and foremost priority is to work with health IT developers to remedy any noncompliance with Conditions and Maintenance of Certification requirements through a corrective action process before taking further action. This emphasizes ONC's desire to promote and support health IT developer compliance with the

Conditions and Maintenance of Certification requirements, and ensure that certified health IT is compliant with Program requirements, in order to foster an environment where EHI is exchanged in an interoperable way.

We proposed in 84 FR 7505 that in considering whether termination of a Health IT Module's certificate(s) and/or a certification ban is appropriate, ONC would consider factors including, but not limited to: Whether the health IT developer has previously been found in noncompliance with the Conditions and Maintenance of Certification or other Program requirements; the severity and pervasiveness of the noncompliance, including the effect of the noncompliance on widespread interoperability and health information exchange; the extent to which the health IT developer cooperates with ONC to review the noncompliance; the extent of potential negative impact on providers who may seek to use the certified health IT to participate in CMS programs; and whether termination and/or a certification ban is necessary to ensure the integrity of the certification process.

In the Proposed Rule, we noted in 84 FR 7505 that, as found in § 170.580(f)(2), ONC would provide notice of the termination to the health IT developer, including providing an explanation for, information supporting, and consequences of, the termination, as well as instructions for appealing the termination. We proposed to add substantially similar notice provisions to § 170.581 for certification bans issued under ONC direct review for noncompliance with the Conditions and Maintenance of Certification requirements. These provisions would also include instructions for requesting reinstatement. In this regard, in 84 FR 7505 we proposed to apply the current reinstatement procedures under § 170.581 to certification bans resulting from noncompliance with the Conditions and Maintenance of Certification requirements, but with an additional requirement that the health IT developer has resolved the noncompliance with the Condition or Maintenance of Certification requirement. In sum, we proposed that a health IT developer could seek ONC's approval to re-enter the Program and have the certification ban lifted if it demonstrates that it has resolved the noncompliance with the Condition or Maintenance of Certification requirement, and ONC is satisfied that all affected customers have been provided appropriate remediation. We sought comment on whether ONC should impose a minimum time period for a certification ban, such as when a health IT developer is noncompliant with a Condition or Maintenance of Certification requirement more than once (*e.g.,* a minimum six months for two instances, a minimum of one year for three instances). We also sought comment on whether additional factors should be considered for a certification ban and/or termination of a health IT developer's certified health IT.

Comments. We received several comments regarding a minimum ban length for repeat offenders. A couple of the commenters recommended ONC establish a minimum ban and agreed with ONC's examples listed above. Other commenters stated that a minimum ban would not be appropriate, with one commenter stating that a minimum ban could have unintended consequences and another commenter stating that it would be better if the length of the ban was determined situationally.

Response. We have finalized the provisions regarding termination and certification ban in §§ 170.580 and 170.581 as proposed. We have not established a minimum ban length for repeat offenders, as a reinstatement process has been established in § 170.581(d) that affords ONC the discretion to determine whether a developer has demonstrated appropriate remediation to all customers affected by the certificate termination, certificate withdrawal, or noncompliance with a Condition or Maintenance of Certification requirement. Section 170.581(d)(4) allows ONC to grant reinstatement into the Program if ONC is satisfied with a health IT developer's demonstration of appropriate remediation, and ONC may consider any and all factors, including past bans, that may affect ONC's decision to grant reinstatement into the Program.

Comments. We received several comments expressing concern for how physicians using products whose developer has been banned would be impacted with respect to payment programs.

Response. We appreciate these comments and clarify that the health IT products of a health IT developer under a certification ban (not certificate termination) would still be considered certified. This means that those products would still be available for use by providers participating in programs requiring the use of certified health IT. However, while under a ban, a health IT developer could not make updates to the certification of those products. This means that access to new certified functionalities within a health IT developer's products would be limited. If the certification status of a product may impact health care providers that are users of that product for HHS program participation, ONC would continue to support HHS and other Federal and State partners, such as CMS, to help identify and make available appropriate remedies for users of terminated certified health IT. This would include supporting policies to mitigate negative impacts on providers, such as the availability of hardship exceptions for the Promoting Interoperability (PI) Programs for hospitals as mandated by section 4002(b)(1)(A) and (b)(2) of the 21st Century Cures Act and finalized by CMS in the FY 2018 Inpatient Prospective Payment System final rule (80 FR 38488 through 38490).

Comments. We received one comment that ONC should add a fine as part of the enforcement of the Conditions and Maintenance of Certification requirements.

Response. We appreciate this comment, but ONC does not have the authority to add a monetary fine as part of the enforcement of the Conditions and Maintenance of Certification requirements. We note, however, that health IT developers are subject to civil monetary penalties (CMPs) if they engage in information blocking, and that a health IT developer must not take any action that constitutes information blocking as a Condition of Certification requirement (§ 170.401).

Comments. One commenter recommended that certification bans apply not only to health IT developers who are noncompliant, but also to the individual management representatives involved, and that account migration review plans be required as an aspect of enforcement in order to address issues around creation of new legal entities in response to a certification ban.

Response. We appreciate these comments and note that certification bans affect health IT developers participating in the Program, their subsidiaries, and their successors (81 FR 72443). We do not have the authority to regulate or enforce against individual management representatives, though we believe the certification ban's reach is an appropriate and sufficient incentive for health IT developers to resolve any noncompliance and meet all required conditions. As stated previously, we are utilizing processes previously established for ONC direct review of certified health IT for the enforcement of the Conditions and Maintenance of Certification requirements, which we believe are familiar to health IT developers and provide a transparent process for working with health IT

developers to remedy instances of noncompliance.

Comments. One commenter expressed concern that there is no process for measuring the severity of a finding of noncompliance, and ONC's proposed enforcement approach would allow for banning of all of a health IT developer's certified health IT based on a finding of noncompliance. The commenter requested that the final rule specify circumstances that could lead to this serious result.

Response. We appreciate the comment and clarify that, as proposed, if a health IT developer under ONC direct review for noncompliance with a Condition of Certification requirement failed to work with ONC to correct the noncompliance, or was noncompliant with the requirements of the CAP, ONC could issue a certification ban. However, we stress that our priority is to first work with health IT developers to correct any noncompliance with the Conditions and Maintenance of Certification requirements through corrective action. As stated in the Proposed Rule in 84 FR 7505, factors we would consider prior to issuing a certification ban, or termination of a Health IT Module's certificate, include whether the health IT developer has previously been found in noncompliance with the Conditions and Maintenance of Certification requirements or other Program requirements; the severity and pervasiveness of the noncompliance; cooperation on the part of the health IT developer during ONC review; potential negative impact on providers participating in CMS programs; and whether termination and/or a certification ban is necessary to ensure the integrity of the certification process.

We clarify that while under a CAP or surveillance by ONC or an ONC–ACB, in the event a health IT developer's approach to remedy a non-conformity and/or to meet Program requirements is to withdraw their current certificate(s) for replacement with a new certificate issued by the ONC–ACB to reflect a new scope, they will not be subject to a certification ban. We note that any open non-conformities will be transferred to the newly issued certificate(s) and must still be resolved by the health IT developer. Similarly, when an ONC–ACB issues a new certificate to reflect 2015 Edition changes, and must withdraw a health IT developer's current certificate to do so, the health IT developer will not be subject to a certification ban if the developer is currently under a CAP or has health IT with open non-conformities.

Comments. One commenter stated that in instances of information blocking, the termination of a Health IT Module's certificate or issuance of a certification ban should not occur until the health IT developer has had the opportunity to respond to the charge of information blocking and appeal the finding.

Response. As stated previously, we have finalized in §§ 170.580 and 170.581 our proposed approach to utilize the processes previously established for ONC direct review of certified health IT for the enforcement of the Conditions and Maintenance of Certification requirements. These processes are open and transparent, and they provide an opportunity for health IT developers to remedy instances of noncompliance through corrective action. We again stress that it is our priority to first work with health IT developers to correct any noncompliance with the Conditions and Maintenance of Certification requirements through corrective action. We believe these processes provide ample opportunity for a health IT developer to respond to and address information blocking prior to issuance of a certification ban or termination of a Health IT Module's certificate.

Comments. We received one comment stating that the final rule should provide for an emergency remedy when the blocking of information places an individual at risk of immediate harm.

Response. Our current process for direct review enables ONC to respond appropriately in the case of certified health IT that may be causing or contributing to conditions that present a serious risk to public health or safety (§§ 170.580(a)(2)(i) and 170.580(d)(1)). We also refer readers to the information blocking section in this final rule (section VIII of preamble and Part 171) for a detailed discussion regarding the information blocking provision and the exceptions to the information blocking definition, including those designed to prevent harm to patients and others.

f. Appeal

We proposed in 84 FR 7505 that a health IT developer would have an opportunity to appeal an ONC determination to issue a certification ban and/or certificate termination resulting from noncompliance with a Condition or Maintenance of Certification requirement. We proposed to follow the processes specified in § 170.580(g). As such, we proposed to revise § 170.580(g) to incorporate ONC direct review of compliance with the Conditions and Maintenance of Certification requirements.

Comments. We received a number of comments generally supporting our proposal to utilize the Appeals processes in our enforcement of compliance with the Condition or Maintenance of Certification requirements.

Response. We appreciate the comments expressing support for our proposal and have finalized our proposal and proposed revisions to § 170.580(g) to incorporate ONC direct review of compliance with the Conditions and Maintenance of Certification requirements.

g. Suspension

We proposed in 84 FR 7506 to not apply the suspension processes under § 170.580 to our review of compliance with the Conditions and Maintenance of Certification requirements. Section 170.580 includes a process for suspending the certification of a Health IT Module at any time if ONC has a reasonable belief that the certified health IT may present a serious risk to public health and safety. While this will remain the case for certified health IT under ONC direct review (*i.e.,* suspension of certification is always available under ONC direct review when the certified health IT presents a serious risk to public health and safety), we do not believe such circumstances would apply to noncompliance with the Conditions or Maintenance of Certification requirements. Further, we believe the more streamlined processes proposed for addressing noncompliance with Conditions and Maintenance of Certification requirements alleviates the need to proceed through a suspension process.

Comments. We received a number of comments generally supporting our proposal not to include Suspension in our enforcement of compliance with the Condition or Maintenance of Certification requirements.

Response. We appreciate the comments expressing support for our proposal and have finalized our proposal as proposed.

h. Proposed Termination

We proposed in 84 FR 7506 to not include an intermediate step between a developer failing to take appropriate and timely corrective action and termination of a certified Health IT Module's certificate called ''proposed termination'' (*see* § 170.580(e) and 81 FR 72437)). Rather, as discussed above, ONC may proceed directly to issuing a certification ban or notice of termination if it determines a certification ban and/or certificate termination are appropriate per the considerations

discussed above. The Conditions and Maintenance of Certification requirements focus on developer business practices and actions for which, as previously discussed, noncompliance is likely to undermine the integrity of the Program and impede widespread interoperability and information exchange. As such, we stated that it is appropriate and consistent with the Cures Act to proceed immediately to a certification ban and/or termination of the affected Health IT Module's certificate(s) if a developer does not take appropriate and timely corrective action. A certification ban and/or termination serves as an appropriate disincentive for noncompliance with the Conditions and Maintenance of Certification requirements.

Comments. We received a number of comments generally supporting our proposal not to include Proposed Termination in our enforcement of compliance with the Condition or Maintenance of Certification requirements.

Response. We appreciate the comments expressing support for our proposal and have finalized our proposal as proposed.

4. Public Listing of Certification Ban and Termination

We proposed in 84 FR 7506 to publicly list on ONC's website health IT developers and certified Health IT Modules that are subject to a certification ban and/or have been terminated, respectively, for noncompliance with a Condition or Maintenance of Certification requirement or for reasons already specified in § 170.581. We take this same approach for health IT with terminated certifications (see 81 FR 72438). Public listing serves to discourage noncompliance with Conditions and Maintenance of Certification and other Program requirements, while encouraging cooperation with ONC and ONC–ACBs and remediation of non-conformities. It also serves to provide notice to all ONC–ATLs, ONC–ACBs, public and private programs requiring the use of certified health IT, and consumers of certified health IT of the status of certified health IT and health IT developers operating under the Program. We sought comment on this proposal, including input on the appropriate period of time to list health IT developers and affected certified Health IT Modules on healthit.gov.

Comments. We received several recommendations that we should enable indefinite posting of certification bans and certificate terminations, including a comment recommending that the public listing show the start and end date of bans that were lifted. We also received one comment recommending that ONC differentiate reinstated developers on the public listing. We also received one comment that there should be an option for a ban to be lifted once the developer comes into compliance.

Response. Responsive to comments and in order to support transparency, we have decided not to set a time limit for listings on the Certified Health IT Product List (CHPL) and to also provide the start and end dates of bans that were lifted. We clarify that the CHPL provides transparency regarding certified health IT listings, including historical non-conformities assessed through surveillance, even after the non-conformity is resolved. This approach to historical transparency is applied to certification bans as well. We also clarify that a certification ban can be lifted as long as the developer has resolved the noncompliance and met all required conditions. We refer readers to § 170.581 for details about the certification ban and reinstatement processes.

5. Effect on Existing Program Requirements and Processes

The Cures Act introduced new Conditions and Maintenance of Certification requirements that encompass technical and functional requirements of health IT and new actions and business practice requirements for health IT developers, which we proposed to adopt in subpart D of Part 170. The pre-Cures Act structure and requirements of the Program provide processes to enforce compliance with technical and functional requirements of certified health IT, and to a more limited extent, requirements for the business practices of health IT developers (*see, e.g.,* 45 CFR 170.523(k)(1)) under subparts C (Certification Criteria for Health Information Technology) and E (ONC Health IT Certification Program) of Part 170. ONC–ACBs are required to perform surveillance on certified Health IT Modules and may investigate reported allegations of non-conformities with Program requirements under subparts A, B, C, and E, with the ultimate goal of working with the health IT developer to correct the non-conformity. Under certain circumstances, such as unsafe conditions or impediments to ONC–ACB oversight, ONC may directly review certified health IT to determine whether it conforms to the requirements of the Program (*see* § 170.580 and the EOA final rule at 81 FR 72404). These avenues for investigating non-conformities with certified Health IT Modules will continue to exist under the Program and generally focus on functionality and performance of certified health IT, or on more limited requirements of business practices of health IT developers found in subparts A, B, C and E of Part 170, respectively. Thus, there may be instances where one or more Condition or Maintenance of Certification requirement is not being or has not been met that also relate to certified Health IT Module non-conformities under subparts A, B, C and E. We proposed that under these situations, ONC could in parallel implement both sets of processes—existing processes to investigate Health IT Module non-conformities and the proposed process to enforce compliance with the Conditions and Maintenance of Certification requirements. We stressed, however, that under the proposed enforcement approach, only ONC would have the ability to determine whether a Condition or Maintenance of Certification requirement per subpart D has been or is being met.

We proposed to delineate the scope of an ONC–ACB's requirements to perform surveillance on certified Health IT Modules as related only to the requirements of subparts A, B, C and E of Part 170. Given our proposed approach that would authorize solely ONC to determine whether a Conditions or Maintenance of Certification requirement per subpart D has been or is being met, we proposed in 84 FR 7506 to add a new PoPC for ONC–ACBs in § 170.523(s) that would require ONC–ACBs to report to ONC, no later than a week after becoming aware, any information that could inform whether ONC should exercise direct review for noncompliance with a Condition or Maintenance of Certification requirement or any matter within the scope of ONC direct review. We did not receive specific comments on this section of the Proposed Rule and have finalized this approach regarding delineation of the review activities of ONC and ONC–ACBs in §§ 170.580 and 170.581 as proposed.

6. Coordination With the Office of the Inspector General

We clarified in the Proposed Rule in 84 FR 7507 that the enforcement approach would apply only to ONC's administration of the Conditions and Maintenance of Certification requirements and other requirements under the Program, but it would not apply to other agencies or offices that have independent authority to investigate and take enforcement action

against a health IT developer of certified health IT. Notably, section 3022(b)(1)(A)(ii) of the PHSA, as added by the Cures Act, authorizes the OIG to investigate claims that a health IT developer of certified health IT has engaged in information blocking, which is defined by section 3022(a)(1) of the PHSA as subject to reasonable and necessary activities identified by the Secretary as exceptions to the definition as proposed in part 171 (see section VIII.D of this final rule). Additionally, section 3022(b)(1)(A)(i) authorizes OIG to investigate claims that a health IT developer of certified health IT has submitted a false attestation under the Condition of Certification requirement which is described at section 3001(c)(5)(D)(vi) of the Cures Act. We emphasized that ONC's and OIG's respective authorities under the Cures Act (and in general) are independent and that either or both offices may exercise those authorities at any time.

We noted, however, that ONC and OIG may coordinate their respective information blocking activities, as appropriate, such as by sharing information about claims or suggestions of possible information blocking or false attestations (including violations of Conditions and Maintenance of Certification requirements that may indicate that a developer has falsely attested to meeting a Condition or Maintenance of Certification requirement). Therefore, we proposed in 84 FR 7507 that we may coordinate our review of a claim of information blocking with OIG or defer to OIG to lead a review of a claim of information blocking. In addition, we proposed that we may rely on OIG's findings to form the basis of a direct review action.

Comments. The majority of comments received supported the general enforcement approach proposed by ONC. We did receive one comment recommending that we use a process similar to OCR's enforcement of the HIPAA Rules and centralize enforcement of patient and provider rights with respect to privacy and access to EHI. Additionally, we received several comments seeking clarification regarding ONC's coordination with OIG and one expressing concern about the potential for a developer to be under review by both OIG and ONC for the same conduct.

Response. We welcome the many comments in support of our proposed enforcement approach. We also appreciate the comment regarding using processes similar to OCR and centralizing enforcement of privacy and access rights. We agree that it is crucial that we develop clear processes for reporting and investigating claims of potential information blocking. To that end, ONC and OIG are actively coordinating on establishing referral policies and procedures to ensure the timely and appropriate flow of information related to information blocking complaints. We also note that the information blocking section of this final rule (part 171) has a delayed compliance date of 6 months after date of publication of the final rule.

OIG and ONC are also coordinating timing of the effective date of this final rule and the start of information blocking enforcement and enforcement of the Conditions of Certification related to information blocking (§ 170.401, § 170.404(a)(1), and § 170.406(a)(1)). We are providing the following information on timing for actors regulated by the information blocking provision. Enforcement of information blocking civil monetary penalties (CMP) in section 3022(b)(2)(A) of the PHSA will not begin until established by future notice and comment rulemaking by OIG. As a result, actors would not be subject to penalties until CMP rules are final. At a minimum, the timeframe for enforcement would not begin sooner than the compliance date of the information blocking provision and will depend on when the CMP rules are final. Discretion will be exercised such that conduct that occurs before that time will not be subject to the information blocking CMPs. Individuals and entities are subject to the information blocking regulations and must comply with this rule as of the compliance date of this provision.

The Cures Act directs the National Coordinator to implement a standardized process for the public to submit reports on claims of health information blocking. ONC intends to implement and evolve this complaint process by building on existing mechanisms, including the current ONC complaint process. We requested comment in the Proposed Rule on ways to adapt our current complaint process for claims of information blocking and refer readers to section VIII.F of this final rule for a more detailed discussion of the complaint process for claims of information blocking. OIG also has the ability to receive and review complaints directly from the public. This ensures that there is no ''wrong door'' by which a complainant can submit information. OIG will provide training to allow their investigators to identify information blocking allegations as part of their other fraud and abuse investigations. Additionally, as part of their continued efforts to implement the information blocking authorities, OIG will establish policies and procedures for reviewing and triaging complaints. We will continue to work with OIG to establish coordinated and aligned procedures and reviews of information blocking complaints as envisioned by the Cures Act. We also emphasize that in order to promote effective enforcement, the information blocking provision of the Cures Act empowers OIG to investigate claims of information blocking and provides referral processes to facilitate coordination with other relevant agencies, including ONC, OCR, and the Federal Trade Commission (FTC). Future notice and comment rulemaking by OIG will provide more additional detail regarding information blocking enforcement.

We clarify that there could be situations when a health IT developer of certified health IT's practices could be reviewed by both ONC and OIG because ONC and OIG have separate and distinct enforcement authority regarding claims of information blocking. We explained in the Proposed Rule that ONC has statutory authority to enforce the Information Blocking Condition and Maintenance of Certification requirements (§ 170.401) and that ONC would enforce the Conditions of Certification requirements through the direct review process. OIG has investigatory authority for the information blocking provision (42 U.S.C. 300jj-52(b)), which may lead to the issuance of (CMPs) for information blocking conducted by health IT developers of certified health IT, health information networks, and health information exchanges. OIG may also investigate health care providers for information blocking, which could result in health care providers being subject to appropriate disincentives. In addition, OIG may investigate false attestations by health IT developers participating in the Program. Since ONC's and OIG's respective authorities with regard to information blocking under the Cures Act (and in general) are independent, it is necessary that either or both offices may exercise those authorities at any time.

However, we emphasize, as we explained above in the Proposed Rule, that we anticipate that ONC and OIG will coordinate their respective information blocking activities, as appropriate, such as by sharing information about claims or suggestions of possible information blocking or false attestations (including violations of Conditions and Maintenance of Certification requirements that may indicate that a developer has falsely attested to meeting a Condition or Maintenance of Certification

requirement). Therefore, we have finalized in § 170.580(a)(4) the proposed approach that will allow us to coordinate our review of a claim of information blocking with the OIG, or defer to OIG to lead a review of a claim of information blocking. In addition, the finalized approach will allow ONC to rely on OIG findings to form the basis of a direct review action.

7. Applicability of Conditions and Maintenance of Certification Requirements for Self-Developers

The HHS regulation that established the Program, ''Establishment of the Permanent Certification Program for Health Information Technology'' (76 FR 1261), addresses self-developers and describes the concept of ''self-developed'' as referring to a Complete EHR or EHR Health IT Module designed, created, or modified by an entity that assumed the total costs for testing and certification and that will be the primary user of the health IT (76 FR 1300 and 1301). While we proposed in 84 FR 7508 in the ''Enforcement'' section of the Proposed Rule that all general Conditions and Maintenance of Certification requirements apply to such developers, we also sought comment on which aspects of the Conditions and Maintenance of Certification requirements may not be applicable to self-developers.

Comments. We received one comment that self-developers should not be permitted to rely on the exception available under the ''Communications'' Condition of Certification requirement that allows developers to place limited restrictions on the communications of their employees who are using their products.

Response. We agree with the comment that self-developers should not be allowed to restrict the communications of users of their product who are also employees. We have revised the language of the ''Communications'' Condition of Certification requirement in § 170.403(a)(2)(ii)(A)(*2*) to clarify that the limited prohibitions developers may place on employees under the Condition of Certification requirement cannot be placed on users of the developers' products who also happen to be employees or contractors of the developer. Overall, we intend to hold self-developers to all Conditions and Maintenance of Certification requirements of health IT developers, as applicable based on the health IT certified.

VIII. Information Blocking

A. Statutory Basis

Section 4004 of the Cures Act added section 3022 of the Public Health Service Act (PHSA) (42 U.S.C. 300jj–52, ''the information blocking provision''). Section 3022(a)(1) of the PHSA defines practices that constitute information blocking when engaged in by a health care provider, or a health information technology developer, exchange, or network. Section 3022(a)(3) authorizes the Secretary to identify, through notice and comment rulemaking, reasonable and necessary activities that do not constitute information blocking for purposes of the definition set forth in section 3022(a)(1). We proposed in the Proposed Rule to establish exceptions to the information blocking definition, each of which would define certain activities that would not constitute information blocking for purposes of section 3022(a)(1) of the PHSA because they are reasonable and necessary to further the ultimate policy goals of the information blocking provision. We also proposed to interpret or define certain statutory terms and concepts that are ambiguous, incomplete, or provide the Secretary with discretion, and that we believe are necessary to carry out the Secretary's rulemaking responsibilities under section 3022(a)(3) (84 FR 7522).

B. Legislative Background and Policy Considerations

In the Proposed Rule, we outlined the purpose of the information blocking provision and related policy and practical considerations that we considered in identifying the reasonable and necessary activities that we proposed as exceptions to the information blocking definition (84 FR 7508).

1. Purpose of the Information Blocking Provision

We explained in the Proposed Rule that the information blocking provision was enacted in response to concerns that some individuals and entities are engaging in practices that unreasonably limit the availability and use of electronic health information (EHI) for authorized and permitted purposes. These practices undermine public and private sector investments in the nation's health IT infrastructure, and frustrate efforts to use modern technologies to improve health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care consumers (84 FR 7508).

We emphasized that the nature and extent of information blocking has come into sharp focus in recent years. In 2015, at the request of Congress, we submitted a Report on Health Information Blocking [117] (''Information Blocking Congressional Report''), in which we commented on the then-current state of technology and of health IT and health care markets. Notably, we observed that prevailing market conditions create incentives for some individuals and entities to exercise control over EHI in ways that limit its availability and use (84 FR 7508).

We noted that we have continued to receive complaints and reports of information blocking from patients, clinicians, health care executives, payers, app developers and other technology companies, registries and health information exchanges, professional and trade associations, and many other stakeholders. We noted that ONC has listened to and reviewed these complaints and reports, consulted with stakeholders, and solicited input from our Federal partners in order to inform our proposed information blocking policies. Stakeholders described discriminatory pricing policies that have the obvious purpose and effect of excluding competitors from the use of interoperability elements. Many industry stakeholders who shared their perspectives with us in listening sessions, including several health IT developers of certified health IT, condemned these practices and urged us to swiftly address them. We highlighted that our engagement with stakeholders confirmed that, despite significant public and private sector efforts to improve interoperability and data accessibility, adverse incentives remain and continue to undermine progress toward a more connected health system (84 FR 7508).

Based on these economic realities and our first-hand experience working with the health IT industry and stakeholders, in the Information Blocking Congressional Report, we concluded that information blocking is a serious problem, and recommended that Congress prohibit information blocking and provide penalties and enforcement mechanisms to deter these harmful practices (84 FR 7508).

We noted in the Proposed Rule that recent empirical and economic research further underscores the intractability of this problem and its harmful effects. In a national survey of health information organizations, half of respondents reported that EHR developers routinely

[117] ONC, Report to Congress on Health Information Blocking (Apr. 2015), *https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf* [hereinafter ''Information Blocking Congressional Report''].

engage in information blocking, and a quarter of respondents reported that hospitals and health systems routinely do so. The survey reported that perceived motivations for such conduct included, for EHR vendors, maximizing short-term revenue and competing for new clients, and for hospitals and health systems, strengthening their competitive position relative to other hospitals and health systems.[118] We noted that other research suggests that these practices weaken competition among health care providers by limiting patient mobility, encouraging consolidation, and creating barriers to entry for developers of new and innovative applications (also referred to as ''apps'') and technologies that enable more effective uses of clinical data to improve population health and the patient experience [119] (84 FR 7508).

We explained in the Proposed Rule that the information blocking provision provides a comprehensive response to these concerns. The information blocking provision defines and creates possible penalties and disincentives for information blocking in broad terms, while working to deter the entire spectrum of practices that unnecessarily impede the flow of EHI or its use to improve health and the delivery of care. The information blocking provision applies to the conduct of health care providers and health IT developers, exchanges, and networks, and seeks to deter information blocking through civil monetary penalties and disincentives for violations. Additionally, developers of health IT certified under the Program are prohibited from information blocking under 3001(c)(5)(D)(i) of the PHSA (84 FR 7509).

The information blocking provision authorizes the HHS Office of Inspector General (OIG) to investigate claims of information blocking and provides for referral processes to facilitate coordination among Federal agencies, including ONC, the HHS Office for Civil Rights (OCR), and the Federal Trade Commission (FTC). The information blocking provision also provides for a process for the public to submit reports on claims of information blocking as well as confidentiality protections to encourage and facilitate the reporting of information blocking. Enforcement of the information blocking provision is buttressed by section 3001(c)(5)(D)(i) and (vi) of the PHSA, which requires the Secretary to establish as a Condition and Maintenance of Certification requirement under the Program that health IT developers do not take any action that constitutes information blocking and require such developers to attest that they have not engaged in such conduct (84 FR 7509).

2. Policy Considerations and Approach to Information Blocking

We explained in the Proposed Rule that the information blocking provision encompasses a broad range of potential practices in order to ensure that individuals and entities that engage in information blocking are held accountable. However, we explained that it is possible that some activities that are innocuous, or even beneficial, could technically implicate the information blocking provision. Given the possibility of these activities, section 3022(a)(3) of the PHSA requires the Secretary, through rulemaking, to identify reasonable and necessary activities that do not constitute information blocking. We refer to such reasonable and necessary activities identified by the Secretary as ''exceptions'' to the information blocking provision. The information blocking provision also excludes from the definition of information blocking those practices that are required by law (section 3022(a)(1) of the PHSA) and clarifies certain other practices that would either not be considered information blocking or penalized (sections 3022(a)(6) and (7) of the PHSA) (84 FR 7509).

In considering potential exceptions to the information blocking provision, we strove to balance a number of policy and practical considerations. To minimize compliance and other burdens for stakeholders, we explained that we were seeking to promote clear, predictable, and administrable policies. In addition, we emphasized our intention to implement the information blocking provision in a way that would be sensitive to legitimate practical challenges that may prevent access to, exchange, or use of EHI in certain situations. We also explained our goal to accommodate practices that, while they may inhibit access, exchange, or use of EHI, are reasonable and necessary to advance other compelling policy interests, such as preventing harm to patients and others, promoting the privacy and security of EHI, and promoting competition and consumer welfare (84 FR 7509).

At the same time, we explained that we sought to provide a comprehensive response to the information blocking problem. Information blocking can occur through a variety of business, technical, and organizational practices that can be difficult to detect and that are constantly changing as technology and industry conditions evolve. The statute responds to these challenges by defining information blocking broadly and in a manner that allows for careful consideration of relevant facts and circumstances in individual cases.

Accordingly, we proposed in the Proposed Rule to establish certain defined exceptions to the information blocking provision as a way to identify reasonable and necessary activities that do not constitute information blocking as required by section 3022(a)(3) of the PHSA. We proposed that these exceptions would be subject to strict conditions and would apply three overarching policy criteria. First, each exception would be limited to certain activities that are both reasonable and necessary. These reasonable and necessary activities include: Promoting public confidence in the health IT infrastructure by supporting the privacy and security of EHI and protecting patient safety; and promoting competition and innovation in health IT and its use to provide health care services to consumers. Second, we noted that each exception addresses a significant risk that regulated individuals and entities will not engage in these reasonable and necessary activities because of uncertainty regarding the breadth or applicability of the information blocking provision. Third, we explained that each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to protect and does not extend protection to other activities or practices that could raise information blocking concerns (84 FR 7509).

3. General Comments Regarding Information Blocking Exceptions

Comments. Numerous commenters expressed support for the proposed

[118] *See, e.g.,* Julia Adler-Milstein and Eric Pfeifer, *Information Blocking: Is It Occurring And What Policy Strategies Can Address It?,* 95 Milbank Quarterly 117, 124–25 (Mar. 2017), *available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full.*

[119] *See, e.g.,* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsburg, *Making Health Care Markets Work: Competition Policy for Health Care,* 16–17 (Apr. 2017), *available at ≤https://www.brookings.edu/research/making-health-care-markets-work-competition-policy-for-health-care/*; Diego A. Martinez et al., *A Strategic Gaming Model For Health Information Exchange Markets,* Health Care Mgmt. Science (Sept. 2016). (''[S]ome healthcare provider entities may be interfering with HIE across disparate and unaffiliated providers to gain market advantage.'') Niam Yaraghi, *A Sustainable Business Model for Health Information Exchange Platforms: The Solution to Interoperability in Healthcare IT* (2015), *available at http://www.brookings.edu/research/papers/2015/01/30-sustainable-business-model-health-information-* exchange-yaraghi; Thomas C. Tsai & Ashish K. Jha, *Hospital Consolidation, Competition, and Quality: Is Bigger Necessarily Better?,* 312 J. AM. MED. ASSOC. 29, 29 (2014).

information blocking exceptions overall. Some commenters stated that information blocking is a widespread problem and perhaps the greatest barrier to interoperability, and supported our approach to addressing information blocking.

While most commenters supported our policy goals regarding information blocking, others questioned whether our policies would have detrimental consequences to the industry given the breadth of the definitions, ambiguity of the expectations, and narrowness of the proposed exceptions. Another commenter stated that the proposed information blocking exceptions are too vague and that an alternative approach is necessary to reduce confusion. The commenter stated that we should align the information blocking requirements with the certified capabilities of health IT developers, and that information blocking should be evaluated through the lens of access, exchange, and use of the USCDI. One commenter suggested that our information blocking policies be more patient-focused as offered by the Individual Health Record™ (IHR) Model.[120] A few commenters requested clarification on how each of the exceptions would be arbitrated, and requested that we provide additional examples of actions that may fall within each exception.

Response. We appreciate the support expressed by many commenters. This final rule maintains the general direction of the Proposed Rule regarding information blocking but focuses the scope of certain terms, while also addressing the reasonable and necessary activities that would qualify for an exception under the information blocking provision. As an example, we have focused the scope of the EHI and Health Information Network (HIN) definitions and have included a new exception in this final rule, the Content and Manner Exception (§ 171.301). We appreciate the comment regarding the IHR Model, but have determined that the best approach to support interoperability and the access, exchange, and use of EHI is through the policies finalized in this final rule, which are patient-focused. For instance, the Fees Exception (§ 171.302), which allows certain fees to be charged, does not apply to a fee based in any part on the electronic access (as such term is defined in § 171.302(d)) of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual. We emphasize that an actor's practice of charging an individual, their personal representative, or another person or entity designated by the individual for electronic access to the individual's EHI would be inherently suspect under an information blocking review.

We continue to receive complaints and reports alleging information blocking from a wide range of stakeholders. ONC has listened to and reviewed these complaints and reports, consulted with stakeholders, solicited input from our Federal partners, and reviewed public comments received in response to the Proposed Rule in order to inform our information blocking policies. We look forward to ongoing collaboration with public and private sector partners as we implement the information blocking provision of this final rule. To note, we have provided clarifications and additional examples throughout this final rule.

Comments. Numerous commenters expressed concern over the proposed effective date of the information blocking policies. Commenters stated that imposing stringent new mandates with an overly aggressive implementation timeframe could be counterproductive by increasing administrative and financial burdens on physician practices, threatening the security of health information, and potentially compromising patient safety. Several provider organizations requested an enforcement ''grace period'' after the new information blocking requirements take effect to allow providers sufficient time to understand the requirements and implement new procedures to be compliant before any disincentives would be applied. Specifically, commenters recommended that OIG not take any enforcement action for a period of 18 months or two years after the effective date of the final rule. Several commenters recommended a period of enforcement discretion of no less than five years during which OIG would require corrective action plans instead of imposing penalties for information blocking. One commenter also recommended that we ''grandfather'' any economic arrangements that exist two years from date of the final rule.

We did not receive any comments on the proposed § 171.101, Applicability, which stated that this part applies to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks, as those terms are defined in § 171.102.

Response. We thank commenters for their input. Taking these comments into consideration, we have delayed the compliance date of the information blocking section of this rule (45 CFR part 171). The compliance date for the information blocking section of this final rule will be six months after the publication date of this final rule in the **Federal Register**. This six-month delayed compliance date was established to provide actors with time to thoroughly read and understand the final rule and educate their workforce in order to apply the exceptions in an appropriate manner. We also note that the finalized definition of information blocking (§ 171.103)) and the new Content and Manner Exception (§ 171.301(a)) reduce the scope of the EHI definition for the first 18 months after the compliance date of the information blocking section of this final rule to the EHI identified by the data elements represented in the USCDI. Therefore, in addition to the information blocking section's compliance date being six months after publication, actors will have an additional 18 months to gain experience applying the exceptions with just the EHI identified by the data elements represented in the USCDI as compared to the full scope of EHI, which would apply thereafter.

During this combined period of 24 months, we strongly encourage actors to apply the exceptions to *all* EHI as if the scope were not limited to EHI identified by the data elements represented in the USCDI. However, given the initial scope of EHI identified in the information blocking definition in § 171.103 and the Content and Manner Exception in § 171.103, if an actor did not, in the first 24 months from this final rule's publication date, enable access, exchange, or use of data outside the USCDI, or did not appropriately apply an exception to data outside the USCDI, such practice or error would not be considered information blocking because that data would not be considered ''EHI'' during that time period.

We have also delayed the compliance date of the Information Blocking Condition of Certification requirement in § 170.401 and the Assurances Condition of Certification requirement in § 170.402(a)(1). We also note that under 45 CFR part 171, we have focused the scope of the EHI definition and have revised the seven proposed exceptions in a manner that is clear, actionable, and likely to reduce perceived burden.

OIG and ONC are coordinating timing of the compliance date of the information blocking section of this

[120] The IHR is a digital tool that provides an all-in-one record of an individual's health, enabling a person and their care team to help improve collaboration and care.

final rule (45 CFR part 171) and the start of information blocking enforcement. We are providing the following information on timing for actors. Enforcement of information blocking civil monetary penalties (CMP) in section 3022(b)(2)(A) of the PHSA will not begin until established by future notice and comment rulemaking by OIG. As a result, actors would not be subject to penalties until CMP rules are final. At a minimum, the timeframe for enforcement would not begin sooner than the compliance date of the information blocking section of this final rule (45 CFR part 171) and will depend on when the CMP rules are final. Discretion will be exercised such that conduct that occurs before that time will not be subject to information blocking CMP.

We have finalized § 171.101 with an additional paragraph to codify the compliance date for the information blocking section of this final rule (45 CFR part 171). Section 171.101(b) states that health care providers, health IT developers of certified health IT, health information exchanges, and health information networks must comply with this part on and after November 2, 2020.

Comments. Several commenters requested that we develop training and educational materials on the information blocking provision. Commenters specifically stated that we should work with other agencies (including CMS, OIG, FTC and OCR) to develop and widely disseminate comprehensive informational materials, such as sub-regulatory guidance and frequently asked questions about what constitutes information blocking. Some commenters recommended we work with OIG to ensure that enforcement focuses on education rather than penalties against non-malicious information blockers. A few commenters suggested that we offer an opportunity for stakeholders to seek advisory opinions from OIG to clarify what constitutes information blocking, or that we create a formal advisory committee on information blocking. Other commenters requested that heath care providers be provided an opportunity to cure an alleged violation and an opportunity to appeal the alleged violation.

Response. We thank commenters for their feedback, including their suggestions for establishing a formal advisory committee. While we do not plan to establish an advisory committee, we plan to engage in multiple efforts to educate stakeholders. We intend to provide educational resources such as infographics, fact sheets, webinars, and other forms of educational materials and outreach based on needs identified. We emphasize that the final rule details our information blocking policies, and these educational materials are intended to educate stakeholders on our final policies established in the final rule. We are also actively coordinating with OIG and have provided OIG with comments we received on the Proposed Rule related to information blocking investigations and enforcement. Future notice and comment rulemaking by OIG will provide additional detail regarding information blocking enforcement.

C. Relevant Statutory Terms and Provisions

In the Proposed Rule, we included regulation text to codify the definition of information blocking in § 171.103. We discussed how we proposed to interpret certain aspects of the information blocking provision that we believe are ambiguous, incomplete, or that provided the Secretary with discretion. We proposed to define or interpret certain terms or concepts that are present in the statute and, in a few instances, to establish new regulatory terms or definitions that we believe are necessary to implement the directive in section 3022(a)(3) of the PHSA to identify reasonable and necessary activities that do not constitute information blocking. We explained that our goal in interpreting the statute and defining relevant terms is to provide greater clarity concerning the types of practices that could implicate the information blocking provision and, relatedly, to more effectively communicate the applicability and scope of the exceptions (84 FR 7509).

Comments. We did not receive any comments on the codification of the proposed definition of information blocking in § 171.103.

As discussed in more detail in section VIII.C.3, we received many comments expressing concerns regarding the breadth of the proposed EHI definition and requesting flexibility in the implementation of the information blocking provision. Many commenters stated that it would be difficult for actors to provide the full scope of EHI as it was proposed to be defined, particularly as soon as the final rule was published. Some commenters opined that we were trying to do too much too fast. Commenters requested that we provide flexibility for actors to adjust to the scope of the EHI definition, as well as the exceptions. Commenters asserted that such an approach would permit them to adapt their processes, technologies, and systems to enable the access, exchange, and use of EHI as required by the Cures Act and this final rule. Some commenters suggested that EHI under the information blocking provision should be limited to ePHI as defined in 45 CFR 160.103, while others requested that ONC consider constraining the EHI covered by the information blocking provision to only the data included in the USCDI.

Response. We have finalized the proposed definition of information blocking in § 171.103 with the addition of paragraph (b). This new paragraph states that until May 2, 2022—which is 18 months after the 6-month delayed compliance date for part 171 (a total of 24 months after the publication date of this final rule)—EHI for purposes of part 171 is limited to the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard adopted in § 170.213. This addition aligns with the content condition within the Content and Manner Exception, which states that for up to May 2, 2022, an actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213 (see § 171.301(a)(1)).

This incremental expansion of the access, exchange, and use of EHI in both the information blocking definition (§ 171.103) and Content and Manner Exception (§ 171.301) responds to commenters' concerns regarding the breadth of health information actors are required to share and the concern about the pace at which we are implementing the information blocking provision. By using USCDI as the baseline of EHI for 18 months after the compliance date of the information blocking section of this final rule (45 CFR part 171),[121] we have created a transparent, predictable starting point for sharing the types of EHI that is understood by the regulated community and more readily available for access, exchange, and use. In addition, health IT that has been certified to the 2015 Edition ''CCDS'' certification criteria will be able to immediately and readily produce almost all of the data elements identified in the USCDI. Furthermore, most, if not all, of such health IT already supports recording USCDI data elements and most HIEs/HINs are routinely exchanging such data elements. Further those developers maintaining certification over the 18-month period from the compliance date of the information blocking section of this

[121] The compliance date for the information blocking section of this final rule (45 CFR part 171) is six months after the publication date of the final rule.

final rule (45 CFR part 171) will be in the process of updating their certified health IT to produce all of the data elements specified in the USCDI, including being certified to the new standardized application programming interface (API) criterion (§ 170.315(g)(10)) and API Condition of Certification (§ 170.404).

We believe the 18-month delay will provide actors with adequate time to prepare for the sharing of all EHI and sunset any non-compliant technology, while providing a clear deadline for when all EHI must be available for access, exchange, and use. During this time period, actors can gain awareness, experience, and comfort with the information blocking provision and exceptions without being required to apply the information blocking exceptions to all EHI as it is defined in § 171.102 (see section VIII.C.3). We expect actors to use this 18-month delay from the compliance date of the information blocking section of this final rule (45 CFR part 171) (in addition to the 6-month period from the publication date of this final rule to the information blocking compliance date) to practice applying the exceptions to real-life situations and to update their processes, technologies, and systems to adapt to the new information blocking requirements. We believe actors will benefit from learning how to respond to requests for all EHI and applying the exceptions during the 18-month delay.

Further, this approach will ensure that the application of the information blocking provision is equitable across actors during the 18-month time period. For instance, if we had required actors to respond to a request to access, exchange, or use EHI during this 18-month time period with all EHI that the actor is able to provide, then actors who are able to provide more EHI would carry a heavier burden than actors who were only able to provide the data elements specified in the USCDI. Nonetheless, and as discussed above, we encourage actors to respond to requests for access, exchange, or use of EHI with as much EHI as possible in order to promote interoperability and to practice applying the exceptions.

We have included language regarding this incremental expansion of the access, exchange, and use of EHI in *both* the information blocking definition (§ 171.103) and Content and Manner Exception (§ 171.301) in order to ensure that the 18-month delay is uniformly applied in the broad circumstances when requestors request access, exchange, or use of EHI as well as in situations when an actor seeks to satisfy the Content and Manner Exception by fulfilling a request to access, exchange, or use EHI in an alternative manner than the manner requested. This approach will ensure that the requisite content to be included in an actor's response to a request to access, exchange, or use EHI during the 18-month period is clear and consistent throughout our information blocking policies.

1. ''Required by Law''

With regard to the statute's exclusion of practices that are ''required by law'' from the definition of information blocking, we emphasized in the Proposed Rule that ''required by law'' refers specifically to interferences with access, exchange, or use of EHI that are explicitly required by State or Federal law. By carving out practices that are ''required by law,'' the statute acknowledged that there are laws that advance important policy interests and objectives by restricting access, exchange, and use of EHI, and that practices that follow such laws should not be considered information blocking (84 FR 7509).

We noted in the Proposed Rule that for the purpose of developing an exception for reasonable and necessary privacy-protective practices, we distinguished between interferences that are ''required by law'' and those engaged in pursuant to a privacy law, but which are not ''required by law.'' (The former does not fall within the definition of information blocking, but the latter may implicate the information blocking provision and an exception may be necessary (84 FR 7510)).

Comments. We received comments requesting additional clarity regarding the meaning and scope of ''required by law'' within the information blocking provision.

Response. We thank commenters for the feedback. We clarify that our references to Federal and State law include statutes, regulations, court orders, and binding administrative decisions or settlements, such as (at the Federal level) those from the FTC or the Equal Employment Opportunity Commission (EEOC). We further note that ''required by law'' would include tribal laws, as applicable. For a detailed discussion of the application of ''required by law'' in the context of the Privacy Exception, please see section VIII.D.1.b.

2. Health Care Providers, Health IT Developers, Exchanges, and Networks

We explained in the Proposed Rule that section 3022(a)(1) of the PHSA, in defining information blocking, refers to four classes of individuals and entities that may engage in information blocking and which include: Health care providers, health IT developers, networks, and exchanges. We proposed in the Proposed Rule to adopt definitions of these terms to provide clarity regarding the types of individuals and entities to whom the information blocking provision applies (84 FR 7510). We noted that, for convenience and to avoid repetition in the preamble, we typically refer to these individuals and entities covered by the information blocking provision as ''actors'' unless it is relevant or useful to refer to the specific type of individual or entity. That is, when the term ''actor'' appears in the preamble, it means a health care provider, health IT developer, health information exchange, or health information network. We proposed to codify this definition of ''actor'' in § 171.102.

Comments. We did not receive any comments on this general approach to use the term ''actors'' throughout the rule for clarity or the proposed definition of ''actor'' in § 171.102. We note that we did receive comments about the definitions of the four categories of actors, which are discussed below.

Response. We have finalized this approach and the definition of ''actor'' in § 171.102 as proposed.

a. Health Care Providers

We identified in the Proposed Rule that the term ''health care provider'' is defined in section 3000(3) of the PHSA (84 FR 7510). We proposed to adopt this definition for purposes of section 3022 of the PHSA (that is, for purposes of information blocking) when defining ''health care provider'' in § 171.102. We noted that the PHSA definition is different from the definition of ''health care provider'' under the HIPAA Rules. We further stated that we were considering adjusting the information blocking definition of ''health care provider'' to cover all individuals and entities covered by the HIPAA Rules ''health care provider'' definition in 45 CFR 160.103. We sought comment on whether such an approach would be justified, and encouraged commenters to specify reasons why doing so might be necessary to ensure that the information blocking provision applies to all health care providers that might engage in information blocking.

Comments. A significant number of commenters were in favor of using the definition of health care provider used in the HIPAA Rules. However, other commenters asserted that doing so would exceed the scope intended by the Cures Act. Some commenters requested exclusions or a ''phased-in'' approach

for the requirements for State agencies, institutions, public health departments, ambulatory surgical centers, and other small providers due to their limited resources or limited access to health IT. Other commenters suggested limiting the application of the information blocking provisions only to those health care providers using certified health IT though some commenters also opposed such a limitation. Some commenters suggested including additional categories such as medical device manufacturers and community-based organizations that address social determinants of health (*e.g.,* access to food, housing, and transportation).

Response. We have retained in this final rule the definition of ''health care provider'' as set forth in section 3000(3) of the PHSA as proposed. The definitions listed in section 3000 of the PHSA apply ''[i]n this title,'' which refers to Title XXX of the PHSA. Section 3022 of the PHSA is included in Title XXX. We note that the last clause of the health care provider definition in section 3000(3) of the PHSA gives the Secretary discretion to expand the definition to any other category determined to be appropriate by the Secretary. We will consider whether the definition should be expanded in the future if the scope of health care providers subject to the information blocking provision does not appear to be broad enough in practice to ensure that the information blocking provision applies to all health care providers that might engage in information blocking.

With respect to the requested exclusions or a ''phased-in'' approach for certain types of entities, we do not believe that this is necessary due to the addition of paragraph (b) within the information blocking definition in § 171.103 and the new Content and Manner Exception in § 171.310. Section 171.103(b) states that until May 2, 2022—which is 18 months after the compliance date of the information blocking section of this final rule (part 171)—EHI for purposes of part 171 is limited to the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard adopted in § 170.213 (see the discussion in section VIII.C). Similarly, the Content and Manner Exception allows actors to make available a limited set of EHI (the USCDI) during the first 18 months after the six-month delayed compliance date for part 171 (a total of 24 months after publication of this final rule). This approach, as well as the Infeasibility Exception, will address concerns about certain actors having limited resources or limited access to health IT.

The health care provider definition and resources we have made available provide clarity and examples of the types of individuals and entities covered by the definition. To this point, medical device manufacturers and community-based organizations, as described by commenters, generally would not meet the health care provider definition unless they are also a type of individual or entity identified in the definition.

b. Health IT Developers of Certified Health IT

Section 3022(a)(1)(B) of the PHSA defines information blocking, in part, by reference to the conduct of health information technology developers. In the Proposed Rule (84 FR 7510), we explained that, because title XXX of the PHSA does not define ''health information technology developer,'' we interpreted section 3022(a)(1)(B) in light of the specific authority provided to OIG in section 3022(b)(1)(A) and (b)(2). We noted that section 3022(b)(2) discusses developers, networks, and exchanges by referencing any individual or entity described in section 3022(b)(1)(A) or (C). Section 3022(b)(1)(A) states, in relevant part, that OIG may investigate any claim that a health information technology developer of certified health information technology or other entity offering certified health information technology engaged in information blocking.

We believe it is reasonable to interpret these sections together to mean that the information blocking provision extends to individuals *or* entities that develop *or* offer certified health IT. That the individual or entity must develop or offer *certified* health IT, we explained, is further supported by section 3022(a)(7) of the PHSA—which refers to developers' responsibilities to meet the requirements of certification—and section 4002 of the Cures Act—which identifies information blocking as a Condition of Certification. Consistent with this, we proposed a definition of ''health IT developer of certified health IT'' in § 171.102 (84 FR 7601) and an interpretation of the use of ''health information technology developer'' in section 3022 of the PHSA that would apply to part 171 only, and would not apply (84 FR 7511) to the implementation of any other section of the PHSA [122] or the Cures Act, such as section 4005(c)(1) of the Cures Act.

[122] Because part 171 is referenced by part 170 subpart D, the definition and interpretation are relevant to developers' obligations to meet Condition and Maintenance of Certification Requirements.

Limiting the Definition of Health IT Developer to Developers of Certified Health IT

Comments. A number of commenters suggested broadening the definition of ''health IT developers'' to include all developers of health IT, whether or not any of their products include Health IT Module(s) certified under ONC's Health IT Certification Program. Several of these commenters expressed concern that developers of only non-certified health IT would, under our proposed definition, be able to continue to block patients from accessing or directing their EHI to third parties of their choice. A majority of these commenters expressed concerns that an information blocking prohibition limited to developers who participate in the ONC Health IT Certification Program (also referred to as ''the Program'') will result in an uneven playing field for developers who participate in the Program in comparison to those who do not participate in the Program. Some commenters suggested that this could motivate developers to avoid or withdraw from the Program.

Response. We believe that ''health information technology developer'' as used in PHSA section 3022(a)(1)(B) should be interpreted in light of the specific authority provided to OIG in section 3022(b)(1)(A) and (b)(2). Section (b)(1)(A) states, in relevant part, that OIG may investigate any claim that a health information technology developer of certified health information technology or other entity offering certified health information technology engaged in information blocking. We recognize that health IT developers that are not developers of certified health IT could engage in conduct meeting the definition of information blocking in section 3022(a) of the PHSA. However, the statute places health IT developers of certified health IT on different footing than other developers of health IT with respect to information blocking enforcement. A broader definition of ''health IT developer'' in § 171.102 would not change the scope or effect of section 3022(b)(1)(A) and (b)(2) of the PHSA.

We acknowledge that the information blocking provision may change some health IT developers' assessments of whether participation in the voluntary ONC Health IT Certification Program is the right decision for their health IT products and customers. However, we believe the value certification offers to the health IT developers' customers, such as health care providers, is substantially enhanced by both the information blocking provision and the

enhancements to certification called for in PHSA section 3001(c)(5)(D). We believe the benefit that certification offers health IT developers' customers will continue to weigh in favor of the developers obtaining and maintaining certification of their products. For example, the Promoting Interoperability Programs (formerly known as the Medicare and Medicaid EHR Incentive Programs) continue to require use of Certified EHR Technology (CERHT), which makes certification important for developers seeking to market certain types of health IT (notably including, but not limited to, that within the ''Base EHR'' definition in § 170.102) to eligible clinicians, eligible hospitals, and critical access hospitals (CAHs).

Comments. Several commenters recommended alternative approaches to interpreting the Cures Act, to justify broadening the definition of ''health IT developer'' in 45 CFR 171.102 to include all developers of any products within the definition of ''health information technology'' in section 3000 of the PHSA. These commenters offered a variety of rationales, including consideration of information that would have been available to Congress at the time the Cures Act was enacted, as the basis for inferring that Congress did not intend to limit the scope of the information blocking provision to developers that participate in the voluntary ONC Health IT Certification Program. Some commenters stated the phrasing of the Cures Act's information blocking provision appeared to exclude health IT developers that do not participate in our Program and recommended that we address what some comments described as a potential enforcement gap by broadening the regulatory definition of ''health IT developer'' in 45 CFR 171.102, although they did not identify a specific statutory basis for closing what their comments described as a gap or drafting issue in the statute. One commenter asked that we work with Congress to expand the definition of health IT developer beyond those with at least one product that is or that includes at least one Health IT Module certified under the Program.

Response. As explained in the Proposed Rule and in the immediately preceding response to comments, we believe that ''health information technology developer'' as used in PHSA section 3022(a)(1)(B) should be interpreted in light of the specific authority provided to OIG in section 3022(b)(1)(A) and (b)(2). Our interpretation is that the individual or entity must develop or offer *certified* health IT to be considered a health IT developer covered by the information blocking provision, which is further supported by PHSA sections 3022(a)(7) and 3001(c)(5)(D). Section 3022(a)(7) refers to developers' responsibilities to meet the requirements of certification, and section 3001(c)(5)(D) identifies as a Condition of Certification that a health IT developer not engage in information blocking. Moreover, PHSA § 3022 does not specifically address all of the types of individuals and entities (such as health plans and claims data clearinghouses) that could or currently do engage in practices that might otherwise meet the definition of information blocking in PHSA § 3022(a).

Applicability of Information Blocking Provision to Non-Certified Health IT Products of a Developer of Certified Health IT

Comments. On the whole, the majority of comments supported defining ''health IT developer'' in a manner that includes all health IT products developed or offered by developers who have at least one Health IT Module certified under the Program. However, multiple comments, predominantly from the perspective of developers of certified health IT, recommended that we limit the definition of ''health IT developers of certified health IT'' in § 171.102 so that it would encompass only the developers' conduct specific to their certified health IT products. Commenters advocating this more limited definition stated that these developers' non-certified health IT products would be competing against similar products of developers who are not subject to the information blocking provision.

Response. The Cures Act does not prescribe that only practices involving certified health IT may implicate PHSA section 3022(a). If Congress had intended to limit the application of section 3022 of the PHSA to practices involving certified health IT, we believe PHSA section 3022 would have included language that tied enforcement of that section to the operation or performance of health IT products that include one or more Health IT Module(s) certified under the Program. Instead, PHSA section 3022(b)(1)(A) provides that the HHS Inspector General may investigate under PHSA section 3022 any claim that ''a health information technology developer of certified health information technology or other entity offering certified health information technology—submitted a false attestation under section 3001(c)(5)(D)(vii); or engaged in information blocking.'' Similarly, neither subparagraph (B) of PHSA section 3022(b)(1), specific to claims that a health care provider engaged in information blocking, nor subparagraph (C), specific to claims that health information exchanges (HIEs) or health information networks (HINs) engaged in information blocking, includes language limiting the Inspector General to investigating claims tied to these actors' use of certified health IT.

Moreover, our observation is that the customers of health IT developers of certified health IT seldom, if ever, rely solely on Health IT Modules certified under the Program to meet their needs to access, exchange, and use EHI. A developer's health IT product suite that a hospital, clinician office practice, or other health care provider uses (and colloquially references) as its ''EHR system'' will typically include a wide variety of functions, services, components, and combinations thereof. Even where such a health IT product suite meets the definition of ''Certified EHR Technology'' for purposes of participation in the Promoting Interoperability Programs, there is no guarantee that every part of the overall product suite will meet the requirements of at least one certification criterion adopted by the Secretary. In fact, typically only a subset of the functions, services, components, and combinations thereof within the overall product suite will meet the requirements of at least one certification criterion adopted by the Secretary and be Health IT Modules certified under the Program.

If we were to interpret the information blocking provision as applying only to the certified Health IT Modules within a developer's product suite(s), we are concerned the developers' customers might too easily presume, based on the developer's participation in the ONC Health IT Certification Program, that the developer will not engage in information blocking with respect to any of the EHI that the customer uses of the developer's product suite(s) to access, exchange, or use. Moreover, limiting our definition of ''health IT developer of certified health IT'' for purposes of part 171 to only the subset of an individual or entity's products that are, or that specifically include, Health IT Modules certified under our Program could encourage developers to split various functions, services, or combinations thereof into multiple products so that they could more easily or broadly avoid accountability for engaging in practices otherwise meeting the definition of information blocking in § 171.103 with respect to various pieces of their product suite(s) rather than

composing products in response to customers' needs and preferences.

We do not believe this outcome would be in the best interest of patients, health care providers, or other customers of health IT developers of certified health IT. Thus, while acknowledging that our definition of ''health IT developer of certified health IT'' in specific may, like the information blocking provision in general, change some health IT developers' assessments of whether participation in the voluntary ONC Health IT Certification Program is the right decision for their health IT products and customers, we believe the definition we have finalized offers necessary assurance to purchasers and users that a health IT developer that has chosen to participate in the Program can be held accountable under part 170 subpart D *and* under part 171 should that developer also engage in any conduct meeting the definition of information blocking in § 171.103.

Duration of Health IT Developer of Certified Health IT Status

We proposed that ''health IT developer of certified health IT'' would mean an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program. We proposed (84 FR 7511) that the term ''information blocking claim'' within this definition should be read broadly to encompass any statement of information blocking or potential information blocking. We also noted in the Proposed Rule that ''claims'' of information blocking within this definition would not be limited, in any way, to a specific form, format, or submission approach or process.

We stated in the Proposed Rule that we were also considering additional approaches to help ensure developers and offerors of certified health IT remain subject to the information blocking provision for an appropriate period of time after leaving the Program. While encouraging commenters to identify alternative approaches for identifying when a developer or offeror should, and when they should no longer, be subject to the information blocking provision, we requested comment on whether one of two specific approaches would best achieve our policy goal of ensuring that health IT developers of certified health IT will face consequences under the information blocking provision if they engage in information blocking in connection with EHI that was stored or controlled by the developer or offeror while they were participating in the Program. One such approach would have defined ''health IT developer of certified health IT'' as including developers and offerors of certified health IT that continue to store EHI that was previously stored in health IT certified in the Program. The other would have continued to define a developer or offeror of health IT as a ''health IT developer of certified health IT'' for purposes of part 171 for an appropriate period of time, such as one year, after the developer or offeror left the Program (no longer had any Health IT Modules certified under part 170).

Comments. We received several comments in support of defining ''health IT developer of certified health IT'' in a way that would include developers and offerors who have left the Program so long as they continue to store or control EHI that had been stored in or by their health IT products while the products were, or included one or more, Health IT Module(s) certified in the Program. We also received several comments recommending developers of certified health IT remain subject to the information blocking provision for a period of time after leaving the Program. A couple of commenters recommended a hybrid approach that would include individuals and entities in the definition of ''health IT developer of certified health IT'' while they continue to store EHI that had been stored in certified health IT *or* for a reasonable period of time after they ceased participating in the Program, whichever is longer.

One reason commenters stated in support of extending the definition of ''health IT developer of certified health IT'' beyond the time a developer ceased participating in the program was that in commenters' view this could help former customers access the EHI that the customers need to provide the best care for patients and that they had contracted with a developer to manage while the developer had certified health IT. Some commenters stated that the need for customers to ensure their contracts with Program-participating developers include provisions for retrieval of the EHI upon termination or conclusion of the contract would be eliminated if the period of time during which the ''health IT developer of certified health IT'' definition applied extended beyond the date a developer leaves the Program. Other comments recommended against developers remaining subject to the information blocking provision after leaving the Program, citing concerns such as burden.

Response. We thank commenters for their feedback. We have finalized in § 171.102 that a ''health IT developer of certified health IT'' for purposes of part 171 means an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj–11(c)(5) (ONC Health IT Certification Program). This definition will ensure conduct a developer or offeror engages in while it has any health IT product certified under the Program will be within the definition of ''health IT developer of certified health IT'' for purposes of part 171.

We have not extended the definition of ''health IT developer of certified health IT'' beyond the date on which a developer or offeror no longer has any health IT certified under the Program. It may be that extending duration of ''health IT developer of certified health IT'' status beyond the date on which a developer or offeror stops participating in the Program could help motivate such a developer or offeror to better support transfers of EHI in their custody if their customers choose to switch products because of the developer's withdrawal from the Program. However, we believe that ensuring continuity of access to patients' EHI is an essential consideration in the process of selecting and contracting for health IT. All transitions between different health IT products will require transfer of EHI between those products. Planning for this transfer is, as a practical matter, integral to a successful transition between products that ensures continuity of access to EHI essential to safe, well-coordinated patient care. We are not persuaded that any of the alternative approaches to duration of ''health IT developers of certified health IT'' status could eliminate the need for health care providers and other customers of ''health IT developers of certified health IT'' to ensure their health IT planning and contracting provides for appropriate transfer(s) of data at the conclusion or termination of any particular contract.

We also note that in the market for certified Health IT Modules today, many of the customers of health IT developers

or offerors are HIPAA-covered entities (such as health care providers) or HIPAA business associates (BAs) (such as health information exchanges or clinical data registries) with whom covered entities contract for particular services. In such cases, the HIPAA Rules generally require that a HIPAA covered entity (or BA) enter into a business associate agreement (BAA) that requires that the BA (or subcontractor BA) return or destroy the PHI after the termination of its service as a BA (or subcontractor BA). Because a contract for health IT products or services, and any associated BAA, could extend beyond a developer or offeror's departure from the ONC Health IT Certification Program, we believe such contracts and agreements provide an appropriate mechanism for customers to guard against a health IT developer or offeror who has left the Program refusing to relinquish EHI. We note further that limiting the definition of ''health IT developer of certified health IT'' to the time period during which the individual or entity has at least one Health IT Module certified under the Program would not require claims of information blocking to come to our attention during that same period. We have finalized the definition as proposed, with modification to its wording that is discussed below.

Comments. A commenter suggested that the definition of ''information blocking claim'' should not include any ''potential information blocking,'' but instead should be evaluated with facts and evidence necessary to support a verifiable claim.

Response. We did not propose to define in regulation ''information blocking claim.'' We did note in the preamble to the Proposed Rule that for purposes of the definition of ''health IT developer of certified health IT'' proposed in § 171.102, claims of information blocking would not be limited, in any way, to a specific form, format, or submission process (84 FR 7511). In the definition of ''health IT developer of certified health IT'' finalized in § 171.102, we have retained reference to the time at which the individual or entity that develops or offers certified health IT engages in a practice that is the subject of an information blocking claim so that it is immediately clear on the face of the regulation text that the claim need not be brought while the developer still has certified health IT. If a health IT developer of certified health IT engages in a practice that is within the definition of information blocking in § 171.103 while they remain in the Program, that health IT developer cannot avoid applicability of the information blocking provision to those practices by simply leaving the Program before any claim(s) about the practice may come to light. Our reference to claims of information blocking in the finalized definition of ''health IT developer of certified health IT'' is not intended to imply that any actor whose conduct is the subject of a claim of information blocking that is received by HHS necessarily will be found to have engaged in conduct meeting the definition of information blocking in § 171.103 or that is otherwise contrary to requirements of the ONC Health IT Certification Program (such as the Condition and Maintenance of Certification requirements established in subpart D of part 170).[123] If subject to an investigation, each practice that implicates the information blocking provision and does not meet an exception would be analyzed on a case-by-case basis to evaluate, for example, whether it rises to the level of an interference, and whether the actor acted with the requisite intent.

Developers and Offerors of Certified Health IT

We stated in the proposed rule that within the definition of ''health IT developer of certified health IT'' for purposes of part 171, we interpret an ''individual or entity that develops the certified health IT'' as the individual or entity that is legally responsible for the certification status of the health IT, which would be the individual or entity that entered into a binding agreement that resulted in the certification status of the health IT under the Program or, if such rights are transferred, the individual or entity that holds the rights to the certified health IT (84 FR 7511). We also stated that an ''individual or entity that offers certified health IT'' would include an individual or entity that under any arrangement makes certified health IT available for purchase or license. We requested comment on both of these interpretations, and whether there are particular types of arrangements under which certified health IT is ''offered'' in which the offeror should not be considered a ''health IT developer of certified health IT'' for the purposes of the information blocking provision.

Comments. Several comments questioned the inclusion of offerors of certified health IT who do not themselves develop the health IT in the definition of ''health IT developer of certified health IT.'' Some commenters recommended the exclusion of offerors who do not modify or configure the health IT in question. Some commenters advocated treating entities that include other developers' certified health IT in the health IT products or services they offer, but do not themselves develop certified health IT, as being outside the definition of ''health IT developer of certified health IT.'' Commenters stated that these offerors do not themselves develop the certified health IT and thus do not control its design. Commenters also stated that the products offered by some of these offerors (such as clinical data registries which may be certified to clinical quality measurement and measure reporting criteria) are not primary sources of patients' EHI, and that offerors of health IT that is not a primary source of EHI should be excluded from the definition of health IT developer of certified health IT. One commenter specifically recommended excluding from the definition individuals and entities that offer under their own brand, but do not modify or configure, certified health IT developed by others. These commenters suggested that this is desirable in order to hold developers accountable for information blocking conduct in the course of development.

Response. Including both developers and other offerors in the definition of ''health IT developer of certified health IT'' is consistent with the policy goal of holding all entities who could, as a developer or offeror, engage in information blocking accountable for their practices that are within the definition of information blocking in § 171.103. PHSA section 3022(b)(1)(A) expressly references both ''a health information technology developer of certified health information technology'' and ''other entity offering certified health information technology'' in the context of authority to investigate claims of information blocking. As stated in the Proposed Rule (84 FR 7510), we interpret PHSA section 3022(a)(1)(B) in light of the specific authority provided to OIG in PHSA section 3022(b)(1)(A) and (b)(2).

We interpret these sections together as the basis for applicability of the information blocking provision to individuals or entities that develop or offer certified health IT. We refer commenters concerned about holding offerors that do not develop, modify, or configure health IT accountable for the conduct of others to PHSA section 3022(a)(6), which states that the term ''information blocking,'' with respect to

[123] Section 3022(b) of the PHSA authorizes the HHS Office of the Inspector General to investigate claims of information blocking. Simultaneously, ONC has responsibility for assessing developers' compliance with requirements of the ONC Health IT Certification Program. Coordination between ONC and OIG in our respective roles is discussed in section VII.D.3 of this preamble.

an individual or entity, shall not include an act or practice other than an act or practice committed by such individual or entity. Where the individual or entity that develops health IT is different from the individual or entity that offers certified health IT, each such individual or entity would have the potential to engage in various practices within the definition of information blocking in PHSA section 3022(a) and 45 CFR 171.103, and we believe each should be accountable for their own conduct. Actors who are not primary generators of EHI or who may hold only a few data classes or elements for any given patient (as would be the case for examples specifically cited by commenters), could nevertheless engage in conduct that constitutes information blocking as defined in § 171.103 with respect to that EHI they do hold or control. We therefore see no reason to exclude them from the definition of health IT developer of certified health IT. To do so would not be consistent with the policy goal of addressing the problem of information blocking.

Comments. Several commenters recommended that public health agencies that develop and/or offer health IT products and services, such as those related to syndromic surveillance and immunization registries, be excluded from the definition of health IT developer in § 171.102.

Response. We believe the vast majority of public health agencies would remain outside of our definition of ''health IT developer of certified health IT'' finalized in § 171.102. The ''public health'' certification criteria within the ONC Health IT Certification Program are applicable to the health IT that health care providers would use to exchange information with public health information infrastructure. These criteria are not applicable to the public health information reporting or exchange infrastructure itself.

Treatment of ''Self-Developers'' of Certified Health IT

We stated in the proposed rule (84 FR 7511) that a ''self-developer'' of certified health IT, as the term has been used in the ONC Health IT Certification Program (Program) and described in section VII.D.7 of the Proposed Rule (84 FR 7507), section VII.D.7 of this preamble, and previous rulemaking,[124] would be treated as a health care provider for the purposes of information blocking because our description of a self-developer for Program purposes [125] would mean that they would not be supplying or offering their certified health IT to other entities (84 FR 7511 and 7512). We stated in the Proposed Rule that self-developers would still be subject to the proposed Conditions and Maintenance of Certification requirements because they have health IT certified under the Program (*see also* section VII.D.7 of the Proposed Rule (84 FR 7507) and section VII.D.7 of this preamble). We requested comments on our treatment of ''self-developers'' for information blocking purposes and whether there are other factors we should consider.

Comments. A number of comments expressed support of treating ''self-developer'' health care providers who do not supply or offer their certified health IT to other entities as health care providers for purposes of information blocking.

Response. We appreciate commenters' input. The definition of ''health IT developer of certified health IT'' that we have finalized in § 171.102 expressly excludes health care providers who self-develop health IT for their own use. However, we remind health care providers who may be considering or are embarking on self-development of certified Health IT Modules that ''self-developers'' *are* subject to certain Condition and Maintenance of Certification requirements finalized in subpart D of part 170. These requirements include, though they are not limited to, providing assurances and attestations that they will not, have not, and do not engage in conduct constituting information blocking.

For purposes of the definition of ''health IT developer of certified health IT,'' we interpret ''a health care provider that self-develops health IT for its own use'' to mean that the health care provider is responsible for the certification status of the Health IT Module(s) and is the primary user of the Health IT Module(s). Moreover, we interpret ''a health care provider that self-develops health IT for its own use'' to mean that the health care provider does not offer the health IT to other entities on a commercial basis or otherwise. This interpretation rests on our established concept of ''self-developed'' certified Health IT Modules. In this context, it is important to note that some use of a self-developer's health IT may be made accessible to individuals or entities other than the self-developer and its employees without that availability being interpreted as offering or supplying the health IT to other entities in a manner inconsistent with the concept of ''self-developer.'' For example, if a hospital were to self-develop an EHR system, we would not consider inclusion in that system of certain functionalities or features—such as APIs or patient portals—to be offering or supplying the hospital's self-developed health IT to other entities. We would also not interpret as offering or supplying the self-developed health IT to other entities the issuance of login credentials allowing licensed health care professionals who are in independent practice to use the hospital's EHR to furnish and document care to patients in the hospital. Keeping in the hospital's EHR a comprehensive record of a patient's care during an admission is a practice we view as reasonable and it typically requires that all the professionals who furnish care to patients in the hospital be able to use the hospital's EHR system. It is also customary practice amongst hospitals that purchase commercially marketed health IT, as well as those that self-develop their health IT, to enable health care professionals in independent practice who furnish care in the hospital to use the EHR in connection to furnishing and documenting that care. Clinician portals made available to facilitate independent licensed health care professionals furnishing and/or documenting care to patients in the hospital would also not be interpreted as negating the hospital's ''self-developer'' status. However, if a health care provider responsible for the certification status of any Health IT Module(s) were to offer or supply those Health IT Module(s), separately or integrated into a larger product or software suite, to other entities for those entities' use in their own independent operations, that would be inconsistent with the concept of the health care provider self-developing health IT for its own use.

In deciding to exclude health care providers who self-develop health IT for their own use from the definition of ''health IT developer of certified health IT'' finalized in § 171.102, we rely substantially on our Program experience that self-developed certified health IT currently represents a small, and diminishing, share of the Health IT Modules certified under our Program. We also note that we may consider amending this definition in future

[124] The final rule establishing ONC's Permanent Certification Program, ''Establishment of the Permanent Certification for Health Information'' (76 FR 1261), addresses self-developers.

[125] The language in the final rule establishing ONC's Permanent Certification Program describes the concept of ''self-developed'' as referring to a complete EHR or EHR Module designed, created, or modified by an entity that assumed the total costs for testing and certification and that will be the primary user of the health IT (76 FR 1300).

rulemaking in response to changing market conditions. For example, the market might evolve in ways that would increase risk of abuse of this exclusion of health care providers who self-develop certified health IT from the application of the § 171.103 definition of ''information blocking'' to their conduct as a developer of health IT. In such circumstances, we might contemplate appropriate revisions to the definition of ''health IT developer of certified health IT'' for purposes of part 171.

Summary of Finalized Policy: Definition of Health IT Developer of Certified Health IT

In § 171.102, we have finalized that ''*health IT developer of certified health IT*'' means an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj–11(c)(5) (ONC Health IT Certification Program). This is substantially the definition we proposed (84 FR 7601), but with minor modifications to its text.

We have added to this finalized definition ''other than a health care provider that self-develops health IT for its own use,'' so that this feature of the proposed definition which we stated in the Proposed Rule's preamble (84 FR 7511) is immediately clear on the face of the regulation text itself. We also replaced the proposed phrasing ''health information technology (one or more) certified'' (84 FR 7601) with ''one or more Health IT Modules certified'' because it is more consistent with our Program terminology. We also replaced ''under the ONC Health IT Certification Program'' from the proposed phrasing with the finalized ''under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj–11(c)(5) (ONC Health IT Certification Program).'' Currently, we keep a single Program that we refer to as the ONC Health IT Certification Program. For purposes of precision, we decided to refer to the statutory basis for the Program, and indicate parenthetically the manner in which we currently reference it.

We interpret ''individual or entity that develops'' certified health IT as the individual or entity that is legally responsible for the certification status of the health IT, which would be the individual or entity that entered into a binding agreement that resulted in the certification status of the health IT under the Program or, if such rights are transferred, the individual or entity that holds the rights to the certified health IT. As we clarified in the final rule ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' (81 FR 72404), the consequences under 45 CFR part 170 for a developer's having had one or more of its products' certification terminated apply to developers, their subsidiaries, and their successors (81 FR 72443).

For purposes of part 171 and the information blocking provision, we interpret an entity that has health IT to include not only the entity that entered into a binding agreement that resulted in the certification status of the health IT under the Program, but also its subsidiaries, and its successors. The facts and circumstances of a particular case may determine which individual(s) or entity (or entities) are culpable and whether enforcement against particular individual(s), the developer entity, a successor in rights to the health IT, the developer or successor's subsidiary, or a parent entity will be pursued. Similarly, use of the word ''individual'' in this context does not limit responsibility for practices of an entity that develops or offers health IT to the particular natural person(s) who may have signed binding agreement(s) that resulted in the certification status of the health IT under the Program. Depending on the nature of the organization, the person who signs the binding agreement that results in the certification status may be different from the person who determines the fees, the person who implements the health IT, and the person who sets the overall business strategy for the company. The facts and circumstances of each case may determine who the culpable individual or individual(s) are and whether enforcement against the entity or against specific individual(s) will be pursued.

As stated in the Proposed Rule, for purposes of this definition, a developer or offeror of a single certified health IT product that has had its certification suspended will still be considered to have certified health IT (84 FR 7511).

c. Health Information Networks and Health Information Exchanges

The terms ''network'' and ''exchange'' are not defined in the information blocking provision or in any other relevant statutory provisions. We proposed to define these terms in a way that does not assume the application or use of certain technologies and is flexible enough to apply to the full range and diversity of exchanges and networks that exist today and that may arise in the future.

We stated that in considering the most appropriate way to define these terms, we examined how they are used throughout the Cures Act and the HITECH Act. Additionally, we considered dictionary and industry definitions of ''network'' and ''exchange.'' While the terms have varied usage and meaning in different industry contexts, we noted that certain concepts are common and were incorporated into the proposed definitions.

Health Information Network

We proposed a functional definition of ''health information network'' (HIN) that focused on the role of these actors in the health information ecosystem. We stated that the defining attribute of a HIN is that it enables, facilitates, or controls the movement of information between or among different individuals or entities that are unaffiliated. Therefore, we proposed that two parties are affiliated if one has the power to control the other, or if both parties are under the common control or ownership of a common owner. We noted that a significant implication of the definition is that a health care provider or other entity that enables, facilitates, or controls the movement of EHI within its own organization, or between or among its affiliated entities, is not a HIN in connection with that movement of information for the purposes of the HIN definition.

We proposed that an actor could be considered a HIN if it performs any one or any combination of the following activities. First, the actor would be a HIN if it were to determine, oversee, administer, control, or substantially influence policies or agreements that define the business, operational, technical, or other conditions or requirements that enable or facilitate the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities. Second, an actor would be a HIN if it were to provide, manage, control, or substantially influence any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.

We noted that, typically, a HIN will influence the sharing of EHI between many unaffiliated individuals or entities. However, we did not propose to establish any minimum number of

parties or ''nodes'' beyond the requirement that there be some actual or contemplated access, exchange, or use of information between or among at least two unaffiliated individuals or entities that is enabled, facilitated, or controlled by the HIN. We stated that any further limitation would be artificial and would not capture the full range of entities that should be considered networks under the information blocking provision. We clarified that any individual or entity that enables, facilitates, or controls the access, exchange, or use of EHI between or among only itself and another unaffiliated individual or entity would not be considered a HIN in connection with the movement of that EHI (although that movement of EHI may still be regulated under the information blocking provision on the basis that the individual or entity is a health care provider or health IT developer of certified health IT). To be a HIN, we emphasized that the individual or entity would need to be enabling, facilitating, or controlling the access, exchange, or use of EHI between or among two or more *other* individuals or entities that were not affiliated with it.

We provided multiple examples to illustrate how the proposed definition would operate. An entity is established within a state for the purpose of improving the movement of EHI between the health care providers operating in that state. The entity identifies standards relating to security and offers terms and conditions to be entered into by health care providers wishing to participate in the network. The entity offering (and then overseeing and administering) the terms and conditions for participation in the network would be considered a HIN for the purpose of the information blocking provision. We noted that there is no need for a separate entity to be created in order for that entity to be considered a HIN. To illustrate, we stated that a health system that ''administers'' business and operational agreements for facilitating the exchange of EHI that are adhered to by unaffiliated family practices and specialist clinicians in order to streamline referrals between those practices and specialists would likely be considered a HIN.

We noted that the proposed definition would also encompass an individual or entity that does not directly enable, facilitate, or control the movement of information, but nonetheless exercises *control or substantial influence* over the policies, technology, or services of a network. In particular, we stated that there may be an individual or entity that relies on another entity—such as an entity specifically created for the purpose of managing a network—for policies and technology, but nevertheless dictates the movement of EHI over that network. As an example, a large health care provider could decide to lead an effort to establish a network that facilitates the movement of EHI between a group of smaller health care providers (as well as the large health care provider) and through the technology of health IT developers. To achieve this outcome, the large health care provider, together with some of the participants, could create a new entity that administers the network's policies and technology.

In this scenario, we noted that the large health care provider would come within the functional definition of a HIN and could be held accountable for the conduct of the network if the large health care provider used its control or substantial influence over the new entity—either in a legal sense, such as via its control over the governance or management of the entity, or in a less formal sense, such as if the large health care provider prescribed a policy to be adopted—to interfere with the access, exchange, or use of EHI. We clarified that the large health care provider in this example would be treated as a health care provider when utilizing the network to move EHI via the network's policies, technology, or services, but would be considered a HIN in connection with the practices of the network over which the large health care provider exercises control or substantial influence.

We sought comment on the proposed definition of a HIN. In particular, we requested comment on whether the proposed definition was broad enough (or too broad) to cover the full range of individuals and entities that could be considered HINs within the meaning of the information blocking provision. Additionally, we specifically requested comment on whether the proposed definition would effectuate our policy goal of defining this term in a way that does not assume particular technologies or arrangements and was flexible enough to accommodate changes in these and other conditions.

We note that we summarize and respond to the comments received on the HIN definition below with the comments received on the health information exchange definition (HIE) due to the overlap in the comments received and our responses.

Health Information Exchange

We proposed to define a ''health information exchange'' (HIE) as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. We noted that our research and experience in working with exchanges drove the proposed definition of this term. We stated that HIEs would include, but were not limited to, regional health information organizations (RHIOs), State health information exchanges (State HIEs), and other types of organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used between or among particular types of parties or for particular purposes. As an example, we noted an HIE might facilitate or enable the access, exchange, or use of EHI exclusively within a regional area (such as a RHIO), or for a limited scope of participants and purposes (such as a clinical data registry or an exchange established by a hospital-physician organization to facilitate Admission, Discharge, and Transfer (ADT) alerting). We further noted that HIEs may be established under Federal or State laws or regulations but may also be established for specific health care or business purposes or use cases. We also mentioned that if an HIE facilitates the access, exchange, or use of EHI for more than a narrowly defined set of purposes, then it may be both an HIE and a HIN.

We sought comment on the proposed HIE definition and encouraged commenters to consider whether the proposed definition was broad enough (or too broad) to cover the full range of individuals and entities that could be considered exchanges within the meaning of the information blocking provision, and whether the proposed definition was sufficiently flexible to accommodate changing technological and other conditions.

Comments on the HIN and HIE Definitions

As mentioned above, we received substantially similar comments on both proposed definitions. Based on those comments and our approach to the final definition for these terms, we have combined our comment summary and response for the proposed definitions.

Comments. Many commenters suggested that the definitions of HIN and HIE should be combined because confusion could arise in trying to distinguish between the two terms. Commenters asserted that these definitions are used to describe entities that perform the same or similar functions. Some commenters expressed support for the broad functional definitions of HIE and HIN, while others expressed concern that many organizations could be unintentionally

covered by the proposed definitions due to the broad scope of the definitions as proposed.

Many commenters suggested excluding certain individuals and entities from the HIE and/or HIN definitions, while other commenters noted such an approach could significantly limit the application of the information blocking provision. Proposed exclusions offered by commenters included, but were not limited to: Health plans, payers, health care providers, business associates, accountable care organizations, health care clearinghouses, public health agencies, research organizations, clinical data registries, certified health information technology providers, software developers, mobile app providers, cloud storage vendors, internet service providers, and patient or consumer focused social media.

Some commenters suggested limiting the types of activities and/or the purposes for those activities that might be necessary to be considered a HIN or HIE.

Commenters also raised concerns with particular language in the proposed HIN definition, noting that the term ''substantially influences'' was vague and that we should remove ''individual'' from the definitions as commenters could not foresee an individual acting as a HIN or HIE.

Response. The definitions of HIN and HIE in the Proposed Rule achieved a key goal which was to solicit feedback from a wide array of stakeholders that might be considered HINs or HIEs under the proposed definition, including on whether the definitions were too broad or not broad enough. We have adopted a modified definition in this final rule to address much of the feedback without expressly excluding any specific type of entity, which we believe would be unwieldy to appropriately administer and, more importantly, in conflict with our overarching approach to include any individual or entity that performs certain functional activities as outlined in the Proposed Rule.

Foremost, in this final rule, we are combining the definitions of HIN and HIE to create one functional definition that applies to both statutory terms in order to clarify the types of individuals and entities that would be covered. This approach is consistent with statements we made in the Proposed Rule noting that a HIE could also be an HIN. In addition, section 3022 of the PHSA often groups these two terms together, and as we noted previously, does not define them. This approach will also eliminate stakeholder confusion as expressed by commenters and respond to commenters who asserted the terms refer to entities performing the same function. To this point, we have found numerous associations and publications referring to entities that perform the same or similar functions that we have specified in the HIN/HIE definition as HINs, HIEs, and regional health information organizations (RHIOs).[126] We have finalized under § 171.102 that a *health information network or health information exchange* means an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI: (1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) that is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164.

In consideration of comments, we also narrowed the definition in three ways. First, the types of actions (*e.g.,* manages or facilitates) that would be necessary for an actor to meet the definition of HIN or HIE were reduced. This includes removing the ''substantially influences'' element of the proposed definition of HIN to address concerns about possible ambiguity. Second, we have revised the definition to specify that to be a HIN or HIE there must be exchange among more than two unaffiliated individuals or entities besides the HIN/HIE that are enabled to exchange with each other. This revision ensures that the definition does not unintentionally cover what are essentially bilateral exchanges in which the intermediary is simply performing a service on behalf of one entity in providing EHI to another or multiple entities and no actual exchange is taking place among all entities (*e.g.,* acting as an intermediary between two entities where the first sends non-standardized data to be converted by the intermediary into standardized data for the receiving entity). To be clear, to be enabled, the parties must have the ability and discretion to exchange with each other under the policies, agreements, technology, and/or services. Third, we focused the definition on three activities: Treatment, payment, and health care operations, as each are defined in the HIPAA Rules (45 CFR 164.501). The activities described by the terms treatment, payment and health care operations were selected for multiple reasons. Many, but not all, individuals and entities that would meet the definition of HIN/HIE for information blocking purposes will be familiar with these terms because they currently function as a covered entity or business associate under the HIPAA Rules. Last, this approach serves to ensure that certain unintended individuals and entities are not covered by the definition, which we discuss in more detail below.

Two important points about the definition require clarification. First, the reference to the three types of activities does *not* limit the application of the HIN/HIE definition to individuals or entities that are covered entities or business associates (as defined in HIPAA). For example, if three unaffiliated entities exchanging information were health care providers that were not HIPAA covered entities, their exchange of information for treatment purposes through a HIN or HIE would qualify for this element of the definition even though the HIN/HIE would not be a business associate to any of the providers. We expect such situations to be rare, but they may occur. Second, the three activities serve as elements of the definition such that if an individual or entity meets them, then the individual or entity would be considered a HIN/HIE under the information blocking regulations for any practice they conducted while functioning as a HIN/HIE. To illustrate, if a HIN/HIE was exchanging EHI on behalf of a health care provider for treatment purposes, but denied an individual access to their EHI available in the HIN/HIE, then the HIN/HIE would be considered a HIN/HIE under the circumstances for the purposes of information blocking. Having said this, the HIN/HIE may not have ''interfered

[126] *See* HIMSS FAQ, Health Information Exchange: A catch-all phrase for all health information exchange, including Regional Health Information Organizations (RHIOs), Quality Information Organizations (QIOs), Agency for Healthcare Research and Quality (AHRQ)-funded communities and private exchanges, *https://protect2.fireeye.com/url?k=7d5b6f82-210e6652-7d5b5ebd-0cc47a6a52de-fe4abdcde0e54deb&u=https://www.himss.org/library/health-information-exchange/FAQ*; AHIMA, ''An HIE is the electronic movement of health-related information among organizations according to nationally recognized standards. HIE is also sometimes referred to as a health information network (HIN)'', *http://bok.ahima.org/PdfView?oid=104129*; SHIEC Member List, SHIEC is the trade association of HIEs, called the Strategic *Health Information Exchange* collaborative, which has 17 members with ''network'' in their name, *https://protect2.fireeye.com/url?k=f84ddacd-a418d31d-f84debf2-0cc47a6a52de-8424832df6e921dc&u=https://strategichie.com/membership/member-list/*.

with'' the individual's access to their EHI depending on the terms of the HIN/HIE's business associate agreements with the participating covered entities or for other reasons such as the EHI could not be disclosed by law or the HIN/HIE met an exception under the information blocking provision. To be clear, the HIN/HIE definition is only applicable to the circumstances of an information blocking claim. For example, a health care provider that may have ownership of a HIN/HIE, would not be considered a HIN/HIE, but instead a ''health care provider'' with respect to situations that involve their behavior as a health care provider, such as denying another health care provider's ability to access, exchange, or use EHI for treatment purposes or denying an individual's access to their EHI via the health care provider's patient portal.

With respect to suggestions to exclude specific types of entities, we believe that the Cures Act goals of supporting greater interoperability, access, exchange, and use of EHI are best advanced by a functional definition without specific exclusions. We note, however, that the narrower definition of HIN/HIE in this final rule should clearly exclude entities that might have been included under the proposed definitions, such as social networks, internet service providers, and technology that solely facilitates the exchange of information among patients and family members. The definition in this final rule continues to focus on the functional activity of the individual or entity in question and not on any title or classification of the person or entity.

The reference to ''individual'' was maintained in the final rule because the Cures Act states that penalties apply to any individual or entity that is a developer, network, or exchange (see section 3022(b)(2)(A) of the PHSA).

3. Electronic Health Information

In the Proposed Rule, we noted that the information blocking definition applies to *electronic* health information (EHI) (section 3022(a)(1) of the PHSA). We further noted that while section 3000(4) of the PHSA by reference to section 1171(4) of the Social Security Act defines ''health information,'' EHI is not specifically defined in the Cures Act, PHSA, HITECH Act, or other relevant statutes. Therefore, we proposed to include the definition of EHI in § 171.102 and define it to mean (84 FR 7513):

(i) Electronic protected health information; and

(ii) any other information that—

- is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103;
- identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
- relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual (84 FR 7513).

We explained in the Proposed Rule that this definition of EHI includes, but is not limited to: Electronic protected health information and health information that is created or received by a health care provider and those operating on their behalf; health plan; health care clearinghouse; public health authority; employer; life insurer; school; or university. In addition, we clarified that under our proposed definition, EHI includes, but is not limited to, electronic protected health information (ePHI) as defined in 45 CFR 160.103. We noted that EHI may also be provided, directly from an individual, or from technology that the individual has elected to use, to an actor covered by the information blocking provisions. We also proposed that EHI does not include health information that is de-identified consistent with the requirements of 45 CFR 164.514(b) (84 FR 7513).

We clarified that the EHI definition provides for an expansive set of health information, which could include information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information (84 FR 7513).

We generally requested comment on this proposed definition as well as on whether the exclusion of health information that is de-identified consistent with the requirements of 45 CFR 164.514(b). We also sought comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking (84 FR 7513).

Comments. Some commenters were strongly supportive of the proposed EHI definition, stating that it covers the breadth of EHI that should be addressed within the regulation. Conversely, many other commenters, including health care providers and health IT developers, contended that the definition was overly broad and vague. They expressed concern about their ability to know what health information they must make available for access, exchange, and use for the purposes of complying with the information blocking provision. Some other commenters posited that they could be put in a situation of having to separate EHI from PHI for compliance purposes, noting this would be extremely burdensome. Many commenters stated simply trying to determine what constitutes EHI for compliance purposes would be extremely burdensome and costly.

Commenters offered various options for narrowing the scope of the EHI definition. Many commenters suggested that EHI should only be electronic protected health information (ePHI) as defined under the HIPAA Rules. Some of these commenters specifically recommended that the EHI definition be limited to align with the definition of a designated record set under HIPAA. A few commenters stated that EHI should be limited to observational health information as described in the Proposed Rule (84 FR 7516). Commenters also recommended that the EHI definition be limited to only standardized health information, with some commenters recommending that EHI be specifically limited to information that meets the USCDI standard.

Response. We appreciate the comments and agree that actors should not have to separate ePHI from EHI in order to comply with both the HIPAA Rules and the information blocking provision. It is also important for actors to clearly understand what health information should be available for access, exchange, and use. To address these concerns, we have focused the EHI definition at this time on terms that are used in the HIPAA Rules and that are widely understood in the health care industry as well as on a set of health information that is currently collected, maintained, and made available for access, exchange, and use by actors. By doing so, we believe we have eliminated any perceived burden and actors will be in a situation that will permit them to readily and continually comply with the information blocking provision. While we understand that some commenters supported the EHI definition as proposed or included alternative definitions in their comments, we believe that, for the above reasons, the EHI definition we have codified in regulation through this final rule will enable effective implementation.

We have defined EHI (§ 171.102) to mean electronic protected health information (ePHI) as the term is defined for HIPAA in 45 CFR 160.103 to the extent that the ePHI would be included in a designated record set as defined in 45 CFR 164.501 (other than

psychotherapy notes as defined in 45 CFR 164.501 or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding), regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103. The ePHI definition in 45 CFR 160.103 incorporates the definitions in that section for protected health information and electronic media. Although the definition of designated record set refers to records maintained by or for a covered entity, the EHI definition has been finalized to apply to groups of records (as they are included in the designated record set) regardless of whether they are maintained by or for a covered entity (*e.g.,* a developer of certified health IT, a health information network, a health information exchange, or even a health care provider that may not be a covered entity or may not be acting as a business associate of a covered entity).

We did not focus the EHI definition finalized in this final rule on observational health information (OHI) as described in the Proposed Rule (84 FR 7516) for multiple reasons. We did not and cannot not at this time define OHI concretely. The use of OHI as a definition would also not align with our above stated goals to provide alignment with the HIPAA Rules and ease of implementation for actors. We also did not focus the EHI definition solely on the data identified in the USCDI standard. We are strong supporters of interoperability and standards-based access and exchange. To this point, the ONC Health IT Certification Program (Program) supports standards-based interoperability through the adoption of standards and the certification of health IT to those standards. In this respect, we have made the USCDI a *baseline* set of data that certified health IT must be able to make available for access and exchange (see section IV.B.1 of this preamble). However, this set of EHI is too limiting in terms of what actors are capable of making available in both the near and long term as is evident by compliance with HIPAA's right of access regulatory provision in 45 CFR 164.524.

To be further responsive to commenters expressing compliance concerns about the EHI definition, we have established a new ''Content and Manner'' exception in this final rule (§ 171.301) that will provide actors time to adjust to the new information blocking paradigm and make EHI available for access, exchange, and use. The new exception permits an actor to provide, at a minimum, a limited set of EHI comprised of the data elements included in the USCDI for access, exchange, and use during the first 18 months after the compliance date of the information blocking provisions (24 months after publication of this final rule). The data elements represented in the USCDI represent an even more focused set of data than the finalized EHI definition (§ 171.102). We refer readers to section VIII.D.2.a of this final rule for further discussion of this new exception.

Comments. Commenters argued both for and against the inclusion of price information in the EHI definition. Commenters that argued for the inclusion of price information stated that it was well within the meaning of the term health information found in the PHSA. Many of these commenters argued that the availability of this type of information would be helpful to patients in selecting and obtaining health care. Commenters also contended that the availability of price information would increase competition and reduce health care costs. Conversely, other commenters made various arguments for not including price information within the definition of EHI. Some of these commenters asserted that price information was not within the scope of health information as specified in section 3022 of the PHSA because Congress did not specifically include it. Commenters also asserted that price information is too vague and lacks standardization to be clearly understood and made available for access, exchange, and use. Other commenters contended that disclosing price information would violate trade secret laws and would harm competitive pricing by health plans.

Response. The EHI definition codified through this final rule does not expressly include or exclude price information. However, to the extent that ePHI includes price information and is included in a designated record set, it would be considered EHI. This approach is intended to assure that the current scope of EHI for purposes of information blocking is aligned with the definitions of ePHI and designated record set under the HIPAA Rules, with limited exceptions.

Comments. A few commenters specifically questioned whether algorithms or processes that create EHI, or the clinical interpretation or relevancy of the results of the algorithms or processes, would be considered EHI.

Response. The EHI definition codified through this final rule does not expressly include or exclude algorithms or processes that create EHI, or the clinical interpretation or relevancy of the results of the algorithms or processes. However, any such information would be considered EHI if it was ePHI included in the designated record set (such as the inclusion of the clinical interpretation of an algorithm's results in an individual's clinical note). Like with price information, this approach is intended to ensure that the current scope of EHI for purposes of information blocking is aligned with the definitions of ePHI and designated record set under the HIPAA Rules, with limited exception.

Comments. Many commenters supported the position that health information which is de-identified in accordance with HIPAA regulations should not be considered EHI.

Response. We agree that health information that is de-identified consistent with the requirements of 45 CFR 164.514(b) should not be included in EHI. It is not, however, necessary to specifically exclude such de-identified information from the EHI definition because information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable information, so it would not be EHI (*see* 45 CFR 164.514(a)). To note, once PHI has been de-identified, it is no longer considered to be PHI. So, such information would not be considered EHI by definition (see 45 CFR 164.514 (b)).

Comments. One commenter viewed the proposed EHI definition as overly restrictive by requiring EHI to be individually identifiable.

Response. The EHI definition codified through this final rule retains the core requirement that the health information be individually identifiable in order to be consistent with HIPAA and general health care industry practice regarding use and disclosure of health information.

4. Price Information—Request for Information

In the Proposed Rule, we requested comment on the technical, operational, legal, cultural, environmental, and other challenges to creating price transparency within health care, and posed multiple specific questions for commenters to consider (84 FR 7513 and 7514).

We received over 1,000 comments regarding price information and price transparency in response to our request, which included recommendations from the HITAC. We thanks commenters for their comments and have shared this

feedback with appropriate Department partners.

5. Interests Promoted by the Information Blocking Provision

a. Access, Exchange, and Use of EHI

We stated in the Proposed Rule that the information blocking provision promotes the ability to *access, exchange, and use* EHI, consistent with the requirements of applicable law. We interpreted the terms ''access,'' ''exchange,'' and ''use'' broadly, consistent with their generally understood meaning in the health IT industry and their function and context in the information blocking provision (84 FR 7514).

We explained in the Proposed Rule that the concepts of access, exchange, and use are closely related: EHI cannot be used unless it can be accessed, and this often requires that the EHI be exchanged among different individuals or entities and through various technological means. Moreover, the technological and other means necessary to facilitate appropriate access and exchange of EHI vary significantly depending on the purpose for which the information will be used. We stated that this explanation is consistent with the way these terms are employed in the information blocking provision and in other relevant statutory provisions. Noting, for example, that section 3022(a)(2) of the PHSA contemplates a broad range of purposes for which EHI may be accessed, exchanged, and used—from treatment, care delivery, and other permitted purposes, to exporting complete information sets and transitioning between health IT systems, to supporting innovations and advancements in health information access, exchange, and use.

In addition, we stated in the Proposed Rule that we considered how the terms access, exchange, and use have been defined or used in existing regulations and other relevant health IT industry contexts. We explained that, while those definitions have specialized meanings and are not controlling for the purposes of information blocking, they are instructive insofar as they illustrate the breadth with which these terms have been understood in other contexts. We noted that the HIPAA Security Rule defines ''access'' as the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource (45 CFR 164.304). Last, we noted that the HIPAA Privacy Rule defines the term ''use,'' which includes the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains the information (45 CFR 160.103).

We stated that the types of access, exchange, and use described above would be promoted under the information blocking provision, as would other types of access, exchange, or use not specifically contemplated in these or other regulations.

We emphasized in the Proposed Rule the interrelated nature of the definitions and proposed to define these terms in § 171.102. For example, the definition of ''use'' that we proposed includes the ability to read, write, modify, manipulate, or apply EHI to accomplish a desired outcome or to achieve a desired purpose, while ''access'' is defined as the ability or means necessary to make EHI available for *use.* As such, we specified that the interference with ''access'' would include, for example, an interference that prevented a health care provider from writing EHI to its health IT or from modifying EHI stored in health IT, whether by the provider itself or by, or via, a third-party app. We encouraged comment on these definitions. In particular, we asked commenters to consider whether these definitions are broad enough to cover all of the potential purposes for which EHI may be needed and ways in which it could conceivably be used, now and in the future.

Comments. Several commenters supported our proposed definitions of ''access,'' ''exchange,'' and ''use,'' based on our broad interpretation of the definitions, which they stated supports interoperability. Several health IT developers and developer organizations stated that the definition of ''access'' was overly broad. They suggested that we clarify and narrow the scope of our proposed definition of ''access.'' One commenter specifically suggested that we clarify that ''access'' need not be provided through a direct interface. Some commenters suggested that we remove the proposed language regarding ''any and all source systems.''

Some commenters expressed concern that the proposed definition of ''exchange'' is overly broad. Other commenters requested additional clarity regarding the scope of the definition. One commenter suggested that we clarify the meaning of ''transmission'' within the definition.

Some health care providers and provider organizations stated that our proposed definition of ''use'' was overly broad. Some commenters suggested that we look to more established definitions of ''use,'' such as HIPAA. Other commenters suggested that the proposed definition would inappropriately increase administrative burden.

Response. We have revised these definitions in response to comments. These revisions do not narrow the scope of the definitions in regard to their intended interpretation and purpose in supporting interoperability and the goals of the information blocking provision. We believe, however, the revisions and their explanations below will provide the necessary clarifications for stakeholders to properly implement and comply with the terms.

Access

We have finalized the definition of ''access'' as ''the ability or means necessary to make EHI available for exchange, use, or both'' (§ 171.102). This final definition improves on the proposed definition (see 84 FR 7601) in a couple of ways. First, it makes clear that ''access'' is the ability or means necessary to make EHI available not only for ''use,'' but also for ''exchange'' or both (the proposed definition only included ''for use''). This modification will provide clarity because, as we noted in the Proposed Rule, these terms are interrelated and EHI cannot be exchanged *or* used if it is inaccessible. Second, to be responsive to comments and in order to promote additional clarity in the definition, we have removed ''including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained'' from the definition. This language was exemplary and resulted in some confusion among stakeholders. Last, we clarify that the definition of ''access'' is not limited to direct interfaces, which we believe is evident by the final definition.

Exchange

We have finalized the definition of ''exchange'' as ''the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks.'' As with the finalized ''access'' definition, we have maintained the general scope of the proposed definition while modifying the definition for clarity. First, we removed ''securely and efficiently'' as proposed descriptors of the way that EHI is to be transmitted under the definition. While we continue to advocate for and promote secure and efficient exchange, we do not think this descriptive language is necessary within the definition of ''exchange'' because ''exchange'' for the purposes of the information blocking provision can

occur regardless of whether the transaction is ''secure'' or ''efficient.'' Our intent with this definition was never to exclude unsecure or ''inefficient'' exchanges from the definition or enforcement of the information blocking provision because the exchange of EHI was not secure or ''inefficient,'' so we have removed this extraneous language. We also refer stakeholders to the information blocking exceptions included in this final rule that discuss how EHI may be transmitted and the importance of security as it relates to the access, exchange, and use of EHI.

Second, we have removed the provision at the end of the proposed definition, that in order for ''exchange'' to occur, it must be ''in a manner that allows the information to be accessed and used.'' This language was potentially confusing because the manner of transmittal is not a necessary component of the ''exchange'' definition. If EHI is exchanged but is done so in way that does not permit the use of the EHI, then that practice may implicate the information blocking provision because the ''use'' of the EHI is being prevented. Further, to be responsive to comments, we emphasize that ''transmitted'' within the definition is *not* limited to a one-way transmission, but instead is inclusive of *all* forms of transmission such as bi-directional and network-based transmission. We note this as a point of clarification, as it was always our intent that ''transmission'' would be interpreted this way.

Use

We have finalized ''use'' to mean ''the ability for EHI, once accessed or exchanged, to be understood and acted upon.'' Put another way, ''use'' is an individual or entity's ability to do something with the EHI once it has been accessed or exchanged. We believe this final definition is more concise and clear than the proposed definition—''the ability of health IT or a user of health IT to access relevant EHI; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose'' (84 FR 7602). Again, we emphasize the general scope and meaning of the definition is the same as proposed as explained below.

First, we have removed language that is more appropriately used as examples in this preamble. For instance, the use of the word ''understood'' in the final definition encompasses the ability to comprehend various things such the structure, content, and meaning of the information from the proposed definition. However, we clarify that ''understood'' just like the proposed term ''comprehend'' does not mean the ability to understand the clinical significance or relevance of the EHI. For example, if an ambulatory provider received patient EHI from a hospital that included a risk score, the concept of ''use'' does not require the hospital to provide additional resources to interpret the score nor would the tool or technology needed to interpret the information be considered an interoperability element because its sole purpose is clinical interpretation.

Similarly to ''understood,'' ''acted upon'' within the final definition encompasses the ability to read, write, modify, manipulate, or apply the information from the proposed definition. We also clarify that ''use'' is bi-directional (to note, we also clarified above in the ''exchange'' discussion that ''exchange'' is bi-directional). Thus, an actor's practice could implicate the information blocking provision not only if the actor's practice interferes with the requestor's ability to read the EHI (one-way), but also if the actor's practice interferes with the requestor's ability to write the EHI (bi-directional) back to a health IT system.

We note that the ability ''to access relevant EHI'' from the proposed definition will fall under the ''access'' definition, particularly in light of the modifications we have made to the ''access'' definition discussed above. Last, we note that we have removed the requirement from the final definition that it would only be considered ''use'' if the action were ''to accomplish a desired outcome or to achieve a desired purpose.'' We do not believe this language is necessary because the ultimate purpose of the ''use'' of the EHI is not relevant to the definition of ''use.''

We appreciate the comments suggesting that we look to more established definitions of ''use,'' such as that within the HIPAA Privacy Rule. We did consider adopting the HIPAA Privacy Rule definition, but ultimately decided that our finalized definition is more appropriate and easier to understand within the information blocking context. We also appreciate the comments suggesting that the proposed definition would inappropriately increase administrative burden; however, we do not believe there is a basis for such assertion, particularly with the clarifications we have provided and the focusing of the EHI definition.

b. Interoperability Elements

We proposed to use the term ''interoperability element'' to refer to any means by which EHI can be accessed, exchanged, or used. We proposed that the means of accessing, exchanging, and using EHI is not limited to functional elements and technical information but also encompasses technologies, services, policies, and other conditions [127] necessary to support the many potential uses of EHI. Because of the evolving nature of technology and the diversity of privacy and other laws and regulations, institutional arrangements, and policies that govern the sharing of EHI, we did not provide an exhaustive list of interoperability elements in the Proposed Rule. We requested comment on the proposed definition.

Comments. Some commenters supported the proposed definition, noting that the breadth and scope of the definition is appropriate. Some commenters requested clarifications and modifications regarding aspects of the proposed definition. A few commenters requested that we clarify whether specific functionalities and technologies, such as certified Health IT Modules and proprietary APIs, would be considered interoperability elements. A commenter requested, within the context of the Licensing Exception (§ 171.303), clarification regarding whether interoperability elements are limited to those elements to which an actor can lawfully confer rights or licenses without the agreement of a third party. A few commenters stated that the definition should exclude underlying substantive content or health facts because such content is not a potential means by which EHI may be accessed, exchanged, or used. One of those commenters also requested that we clarify that legally required data tags are excluded from the ''interoperability element'' definition. A commenter suggested that we clarify that whether a functionality is considered an interoperability element should be determined without regard to whether it can be protected under copyright or patent law. One commenter requested additional examples of interoperability elements. Another commenter requested clarification regarding the meaning of ''transmit'' within the definition.

Some commenters stated that the definition is too broad and should be narrowed. A couple of commenters

[127] *See* ONC, Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at x–xi, *https://www.healthit.gov/topic/interoperability/interoperability-roadmap* (Oct. 2015) [hereinafter ''Interoperability Roadmap''].

stated that the definition is confusing and ambiguous. A few commenters noted that we should focus the definition on specific elements that are currently certified and/or are employed to support interoperability through existing standards and requirements that enable the exchange of EHI in a usable fashion.

Response. We appreciate commenters' support of the proposed definition, as well as the comments that requested clarifications and suggested improvements to the definition. We have streamlined the definition, with the intent of maintaining a broad definition of interoperability elements, and leveraged other regulatory and industry terms to add clarity. We have finalized the definition of ''interoperability element'' to mean hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that: (1) May be necessary to access, exchange, or use EHI; and (2) is controlled by the actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of EHI.

While this definition remains broad, it is confined by changes we have made to other parts of the information blocking section. Specifically, the more focused definitions of ''electronic health information'' and ''access,'' ''exchange,'' or ''use'' will result in a smaller scope of interoperability elements, as defined above, being necessary to enable access, exchange, or use of EHI. Further, under the Content and Manner Exception (§ 171.301), we establish that an actor is not required to respond to a request to access, exchange, or use EHI in the manner requested if the actor would be required to license its IP (which could constitute an interoperability element) and cannot reach agreeable terms for the license with the requestor (§ 171.301(b)(1)(i)(B)). This means that actors who do not want to license their interoperability elements will not be required to do so if they are able to respond in an alternative manner in accordance with § 171.301(b)(2).

We believe the above definition improves on the proposed definition in multiple ways. First, while preserving the meaning described in the Proposed Rule that would constitute an interoperability element (*i.e.,* hardware, software, technical information, technology, service, license, right, privilege), we have removed descriptive language and examples from the regulation text. Such language did not add clarity, as it was not exhaustive as noted in the regulation text, which included the language: ''Any other means by which electronic health information may be accessed, exchanged, or used.'' The removal of this language makes the definition clearer and more concise. We note that we provide examples of ''interoperability elements'' in the discussion below.

Second, we leveraged the definition of ''health information technology'' from title XXX of the PHSA (specifically, section 3000(5) of the PHSA), as added by title XIII of the HITECH Act. The Cures Act amended title XXX of the PHSA to establish the information blocking provision in section 3022 of the PHSA. Section 3000(5) of the PHSA defines ''health information technology'' as ''hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.'' We emphasize that this definition includes intellectual property.

When we drafted the Proposed Rule, we chose to use the term ''interoperability element'' to describe the means necessary to access, exchange, or use EHI instead of ''health IT'' because we believed that defining a new term (interoperability element) would allow us to tailor and focus the definition to the specific issue of information blocking. However, after further reflection and review of stakeholder comments—specifically those requesting additional clarity regarding the definition of ''interoperability element''—we believe a better approach is to leverage the definition of ''health information technology'' from section 3000(5) of the PHSA because that definition provides the statutory basis for the types of technology, services, functionality necessary to support interoperability, including the access, exchange, and use of EHI. We believe this approach of leveraging an established, statutory definition will promote transparency and clarify ONC's expectations for regulated actors.

As such, we have added ''integrated technologies,'' ''intellectual property,'' and ''upgrades'' from the PHSA definition into our definition of interoperability element. These additions will strengthen the ''interoperability element'' definition by explicitly identifying types of interoperability elements that *would have been covered* by our proposed definition, but were not called out in the proposed definition (these types of interoperability elements would have been covered by the provision in the proposed definition that an interoperability element could be any other means by which EHI may be accessed, exchanged, or used). We chose not to substitute the PHSA health information technology definition in its entirety for the ''interoperability element'' definition in this final rule because some aspects do not fit within the ''interoperability element'' definition. For instance, the concept of ''packaged solutions'' is undefined and would not add clarity to the interoperability element definition. Thus, we believe this approach will achieve our goal of establishing a definition of interoperability element that is tailored for the information blocking context.

Last, we have clarified within the definition that a requisite component of an interoperability element is that it is *controlled by the actor.* As used in the interoperability element definition, controlled by the actor includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of EHI. In order to make this point clear, we have added and finalized paragraph (2) within the interoperability element definition (see § 171.102). Thus, if an actor could not confer a right or authorization necessary to use the interoperability element to enable the access, exchange, or use of electronic health information, (*e.g.,* by way of sub-license or assignment), the actor would not have the requisite ''control'' under the ''interoperability element'' definition. This clarification reinforces our position that our rule does not require or encourage actors to infringe on IP rights.

We appreciate the comments that asked that we specify whether specific functionalities and technologies, such as certified Health IT Modules and proprietary APIs, would be considered interoperability elements. We clarify that most certified Health IT Modules and proprietary APIs would be considered interoperability elements under the interoperability element definition. We also clarify that the underlying substantive content or health facts are not considered interoperability elements because substantive content and health facts are not a *means* by which EHI is accessed, exchanged, or used. Regarding legally required data tags, we would need additional information concerning the specific data tag to determine whether it could constitute an interoperability element.

Generally, data tags would likely be considered technical information under the ''interoperability element'' definition, but such data tags would need to be necessary to access, exchange, or use EHI to be considered an interoperability element.

A determination regarding whether a functionality is considered an interoperability element will be determined without regard to whether it is protected under copyright or patent law. In fact, the finalized definition of interoperability element includes ''licenses'' and ''intellectual property.'' We have also established an exception to information blocking that supports the licensing of intellectual property. Thus, we make clear that functionalities generally covered by copyright, patent, or other such laws can be interoperability elements.

In response to the commenter who requested additional examples of interoperability elements, we provide the following non-exhaustive list of examples:

- Functional elements of health IT that could be used to access, exchange, or use EHI for any purpose, including information exchanged or maintained in disparate media, information systems, or by HINs/HIEs;
- Technical information that describes the functional elements of technology, such as a standard, specification, protocol, data model, or schema, that would be required to use a functional element of a certain technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements;
- System resources, technical infrastructure, or HIN/HIE elements that are required to enable the use of a compatible technology in production environments; or
- Licenses, rights, or privileges that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.

We appreciate the comments requesting that we clarify and narrow the ''interoperability element'' definition. As discussed above, we believe the revised definition addresses commenters' concerns regarding the clarity of the definition. Responsive to commenters, the final definition is also narrower than the proposed definition, as we have removed the proposed provision that an interoperability element could be *any other means* by which EHI may be accessed, exchanged, or used (see 84 FR 7602).

We have decided not to focus the definition on certified elements or existing standards or requirements because such a narrowed focus would unduly limit the definition, interoperability, and the access, exchange, and use of EHI. The finalized definition reflects that there are countless means by which EHI may be accessed, exchanged, or used that are not certified or standardized. We note that the new Content and Manner Exception (§ 171.301) supports certified and standards-based exchange as suggested by the commenter. We refer readers to VIII.D.2.a of this preamble for a discussion of that exception.

We note that we have removed the term ''transmit'' from the regulatory text because it no longer fit in the context of other changes made to the definition.

6. Practices That May Implicate the Information Blocking Provision

To meet the definition of information blocking under section 3022(a) of the PHSA, a practice must be *likely to interfere with, prevent, or materially discourage* the access, exchange, or use of EHI. In this section and elsewhere in the Proposed Rule, we discussed various types of hypothetical practices that *could* implicate the information blocking provision. We did this to illustrate the scope of the information blocking provision and to explain our interpretation of various statutory concepts. However, we stressed that the types of practices discussed in the preamble of the Proposed Rule are illustrative and not exhaustive and that many other types of practices could also implicate the provision. We emphasized that the fact that we did not identify or discuss a particular type of practice did not imply that it is less serious than those that were discussed in the preamble. Indeed, we explained in the Proposed Rule that because information blocking may take many forms, it is not possible to anticipate or catalog all potential types of practices that may raise information blocking concerns.

We emphasized that any analysis of information blocking necessarily requires a careful consideration of the individual facts and circumstances, including whether the practice was required by law, whether the actor had the requisite knowledge, and whether an exception applies. A practice that seemingly meets the statutory definition of information blocking would not be information blocking if it was required by law, if one or more elements of the definition were not met, or if it was covered by one of the exceptions for reasonable and necessary activities.

In accordance with section 3022(a)(3) of the PHSA, we proposed in the Proposed Rule to establish exceptions to the information blocking provision for certain reasonable and necessary activities. We proposed that if an actor can establish that an exception applies to each practice for which a claim of information blocking has been made, including that the actor satisfied all applicable conditions of the exception at all relevant times, then the practice would not constitute information blocking.

Comments. There was broad support from commenters regarding the categories of practices identified in the Proposed Rule that may implicate the information blocking provision, as well as the non-exhaustive list of specific examples provided in the Proposed Rule to assist with compliance. Commenters noted that the illustrative examples provided were helpful in providing further clarity on the scope of the information blocking provision. Many commenters noted that considerable barriers continue to obstruct both provider and patient access to patient data and our approach to the information blocking provision can increase access to this data.

Several commenters suggested the need for a comprehensive inventory or repository of examples, including examples of information blocking conduct that have been submitted to ONC. Many commenters suggested specific clarifications and modifications to the examples provided in the Proposed Rule in the sections below, as well as additional examples for inclusion in the final rule, such as additional examples applicable to specific contexts (*e.g.,* imaging providers, and pharmacies) or specific practices (*e.g.,* practices involving clinical data registries and pharmacogenomics).

Response. We thank commenters for their support and feedback. We have not revised the examples provided in the Proposed Rule because we believe they are clear, accurate, and helpful to readers. To be responsive to commenters who requested additional examples be added to the final rule, we have added examples in the discussion of ''Limiting or Restricting the Interoperability of Health IT'' in section VIII.C.6.c.ii. as well as additional examples within the preamble discussion for the exceptions. We used commenters' suggestions to help inform these examples and highlight important use cases and circumstances that required additional clarification. We emphasize that these listed examples are illustrative, but not exhaustive.

We also clarify that when we say that the actor must satisfy all applicable conditions of the exception at *all*

relevant times to meet each exception, *all relevant times* means any time when an actor's practice relates to the access, exchange, or use of EHI.

a. Prevention, Material Discouragement, and Other Interference

We explained in the Proposed Rule that the information blocking provision and its enforcement subsection do not define the terms ''interfere with,'' ''prevent,'' and ''materially discourage,'' and use these terms collectively and without differentiation. Based on our interpretation of the information blocking provision and the ordinary meanings of these terms in the context of EHI, we interpreted these terms to not be mutually exclusive. Instead, prevention and material discouragement may be understood as types of interference, and that use of these terms in the statute to define information blocking illustrates the desire to reach all practices that an actor knows, or should know, are likely to prevent, materially discourage, or otherwise interfere with the access, exchange, or use of EHI. Consistent with this understanding, we used the terms ''interfere with'' and ''interference'' as inclusive of prevention and material discouragement.

We explained that interference could take many forms. In addition to the prevention or material discouragement of access, exchange, or use, we stated that interference could include practices that increase the cost, complexity, or other burdens associated with accessing, exchanging, or using EHI. Interference could also include practices that limit the utility, efficacy, or value of EHI that is accessed, exchanged, or used, such as by diminishing the integrity, quality, completeness, or timeliness of the data. Relatedly, to avoid potential ambiguity and clearly communicate the full range of potential practices that could implicate the information blocking provision, we proposed to codify a definition of ''interfere with'' in § 171.102, consistent with our interpretation set forth above (84 FR 7516).

Comments. We did not receive comments on our proposed definition of ''interfere with.''

Response. We have finalized the definition of ''interfere with'' (also referred to as ''interference'') in § 171.102 as proposed, but with a modification to remove the phrase ''access, exchange, or use of electronic health information'' from the definition. We removed this language because it was not necessary in the definition, and to avoid duplication, as we often say in the preamble of this final rule that ''a practice interferes with access, exchange or use of EHI.'' We also note that we received many comments requesting clarification of whether certain practices would constitute interference with the access, exchange, and use of EHI, and thus implicate the information blocking provision. We address these comments in section VIII.C.6.c (Examples of Practices Likely to Interfere with the Access, Exchange or Use of EHI) below.

b. Likelihood of Interference

We noted in the Proposed Rule that the information blocking provision is preventative in nature. That is, the information blocking provision proscribes practices that are *likely* to interfere with (including preventing or materially discouraging) access, exchange, or use of EHI—whether or not such harm materializes. By including both the likely and the actual effects of a practice, the information blocking provision encourages individuals and entities to avoid engaging in practices that undermine interoperability, and to proactively promote access, exchange, and use of EHI.

We explained that a practice would satisfy the information blocking provision's ''likelihood'' requirement if, under the circumstances, there is a reasonably foreseeable risk that the practice will interfere with access, exchange, or use of EHI. We explained that a policy or practice that limits timely access to information in an appropriate electronic format creates a reasonably foreseeable likelihood of interfering with the use of the information.

We noted that whether the risk of interference is reasonably foreseeable will depend on the particular facts and circumstances attending the practice or practices at issue. Because of the number and diversity of potential practices, and the fact that different practices will present varying risks of interfering with access, exchange, or use of EHI, we did not attempt to anticipate all of the potential ways in which the information blocking provision could be implicated. Nevertheless, to assist with compliance, we clarified certain circumstances in which, based on our experience, a practice will almost always be likely to interfere with access, exchange, or use of EHI. We cautioned that the situations listed are not exhaustive and that other circumstances may also give rise to a very high likelihood of interference under the information blocking provision. We noted that in each case, the totality of the circumstances should be evaluated as to whether a practice is likely to constitute information blocking.

In the Proposed Rule, we stated that we believe that information blocking concerns are especially pronounced when the conduct at issue has the potential to interfere with the access, exchange, or use of EHI that is created or maintained during the practice of medicine or the delivery of health care services to patients, which we referred to collectively as ''observational health information'' (84 FR 7516 and7517). We received a few comments seeking clarification regarding our use of the term ''observational health information'' or that we provide a regulatory definition for the term.

Comments. We received some comments requesting clarification regarding the meaning of ''timely'' access in the discussion in the Proposed Rule.

Response. We have not established a set timeframe for what ''timely'' access means because there is so much variability regarding what ''timely'' will mean based on the specific facts and circumstances, and particularly with regard to the broad scope of health IT being discussed. We emphasize that whether access is considered timely will be determined based on the specific facts and circumstances. We refer readers to the discussion in section VIII.C.6.c. on ''Limiting or Restricting the Interoperability of Health IT'' where we discuss how slowing or delaying access, exchange, or use of EHI could be considered information blocking.

Comments. We did not receive any additional comments regarding out interpretation of the information blocking provision's ''likelihood'' requirement discussed above.

Response. We have finalized our interpretation as described above.

Comments. We received comments requesting clarification regarding the meaning of ''observational health information'' as used in the Proposed Rule.

Response. As discussed earlier in section VIII.C.3, after consideration of concerns raised by commenters, we have not finalized the definition of EHI as proposed. Instead, we have finalized a more focused definition of EHI. Because we have finalized a definition of EHI with a more focused scope than proposed, we no longer believe our proposed approach regarding observational health information is necessary. Accordingly, we are not using the term ''observational health information'' in this final rule. We refer readers to section VIII.C.3. for further discussion of the definition of EHI.

i. Purposes for Which Information May Be Needed

We explained in the Proposed Rule that the information blocking provision will almost always be implicated when a practice interferes with access, exchange, or use of EHI for certain purposes, including but not limited to:

- Providing patients with access to their EHI and the ability to exchange and use it without special effort (*see* section VII.B.4).
- Ensuring that health care professionals, care givers, and other authorized persons have the EHI they need, when and where they need it, to make treatment decisions and effectively coordinate and manage patient care and can use the EHI they may receive from other sources.
- Ensuring that payers and other entities that purchase health care services can obtain the information they need to effectively assess clinical value and promote transparency concerning the quality and costs of health care services.
- Ensuring that health care providers can access, exchange, and use EHI for quality improvement and population health management activities.
- Supporting access, exchange, and use of EHI for patient safety and public health purposes.

We emphasized that the need to ensure that EHI is readily available and usable for these purposes is paramount. Therefore, practices that increase the cost, difficulty, or other burdens of accessing, exchanging, or using EHI for these purposes would almost always implicate the information blocking provision. We stressed that individuals and entities that develop health IT or have a role in making these technologies and services available should consider the impact of their actions and take steps to support interoperability and avoid impeding the availability or use of EHI (84 FR 7517).

Comments. We did not receive comments of the discussion above.

Response. Consistent with the Proposed Rule, in this final rule we continue to emphasize that practices that interfere with the access, exchange, or use of EHI for the purposes listed in this section and that do not meet any of the final exceptions will almost always implicate the information blocking provision and will be inherently suspect. These practices may jeopardize the core functions of the health care system that require the access, exchange, or use of EHI. We believe there are few, if any, legitimate reasons for an actor to interfere with the use of EHI in the context of these purposes.

We specifically emphasize that practices that involve an actor charging an individual a fee to access, exchange, or use their EHI would be inherently suspect, as discussed in more detail in the Fees Exception (section VIII.D.2.b), as there are few, if any, legitimate reasons for an actor to charge an individual for access to their EHI.

ii. Control Over Essential Interoperability Elements; Other Circumstances of Reliance or Dependence

We explained in the Proposed Rule that an actor may have substantial control over one or more interoperability elements that provide the only reasonable means of accessing, exchanging, or using EHI for a particular purpose. We noted that, in these circumstances, any practice by the actor that could impede the use of the interoperability elements—or that could unnecessarily increase the cost or other burden of using the elements—would almost always implicate the information blocking provision.

We explained that the situation described above is most likely when customers or users are dependent on an actor's technology or services, which can occur for any number of reasons. For example, technological dependence may arise from legal or commercial relations, such as a health care provider's reliance on its EHR developer to ensure that EHI managed on its behalf is accessible and usable when it is needed. Relatedly, most EHI is currently stored in EHRs and other source systems that use proprietary data models or formats. Knowledge of the data models, formats, or other relevant technical information (*e.g.,* proprietary APIs) is necessary to understand the data and make efficient use of it in other applications and technologies. Because this information is routinely treated as confidential or proprietary, the developer's cooperation is required to enable uses of the EHI that go beyond the capabilities provided by the developer's technology. This includes the capability to export complete information sets and to migrate data in the event that a user decides to switch to a different technology.

We noted that separate from these contractual and intellectual property issues, users may become ''locked in'' to a particular technology, HIE, or HIN for financial or business reasons. For example, many health care providers have invested significant resources to adopt EHR technologies—including costs for deployment, customization, data migration, and training—and have tightly integrated these technologies into their information management strategies, clinical workflows, and business operations. As a result, they may be reluctant to switch to other technologies due to the significant cost and disruption this would entail.

We explained that another important driver of technological dependence is the ''network effects'' of health IT adoption, which are amplified by reliance on technologies and approaches that are not standardized and do not enable seamless interoperability. Consequently, health care providers and other health IT users may gravitate towards and become reliant on the proprietary technologies, HIEs, or HINs that have been adopted by other individuals and entities with whom they have the greatest need to exchange EHI. We noted that these effects may be especially pronounced within particular products or geographic areas. For example, a HIN that facilitates certain types of exchange or transactions may be so widely adopted that it is a *de facto* industry standard. A similar phenomenon may occur within a particular geographic area once a critical mass of hospitals, physicians, or other providers adopt a particular EHR technology, HIE, or HIN.

We emphasized that in these and other analogous circumstances of reliance or dependence, there is a heightened risk that an actor's conduct will interfere with access, exchange, or use of EHI. To assist with compliance, we highlighted the following common scenarios, based on our outreach to stakeholders, in which actors exercise control over key interoperability elements.[128]

Health IT developers of certified health IT that provide EHR systems or other technologies used to capture EHI at the point of care are in a unique position to control subsequent access to and use of that information.

- HINs and HIEs may be in a unique position to control the flow of information among particular persons or for particular purposes, especially if the HIN or HIE has achieved significant adoption in a particular geographic area or for a particular type of health information use case.
- Similar control over EHI may be exercised by other entities, such as health IT developers of certified health IT, that supply or control proprietary technologies, platforms, or services that are widely adopted by a class of users or that are a ''de facto standard'' for

[128] As an important clarification, we note that control over interoperability elements may exist with or without the actor's ability to manipulate the price of the interoperability elements in the market.

certain types of EHI exchanges or transactions.

• Health care providers within health systems and other entities that provide health IT platforms, infrastructure, or information sharing policies may have a degree of control over interoperability or the movement of data within a geographic area that is functionally equivalent to the control exercised by a dominant health IT developer, HIN, or HIE.

To avoid engaging in conduct that may be considered information blocking, actors with control over interoperability elements should be careful not to engage in practices that exclude persons from the use of those elements or create artificial costs or other impediments to their use.

We encouraged comment on these and other circumstances that may present an especially high likelihood that a practice will interfere with access, exchange, or use of EHI within the meaning of the information blocking provision.

Comments. A few commenters appreciated the examples provided and ONC's acknowledgement in the Proposed Rule that certain parties are in a unique position to control access, exchange, and use of EHI. Other commenters urged ONC to only hold accountable those parties that actually have control of the EHI or control of interoperability elements necessary to access, exchange, or use the EHI in question.

Response. We thank commenters for their support. We stress that any analysis of whether an actor's practices constitute information blocking will depend on the particular facts and circumstances of the case, which may include an assessment of the actor's control over the EHI or interoperability elements necessary to access, exchange, or use the EHI in question, as applicable. A key element of information blocking is that the actor's practice is likely to interfere with an individual or entity's ability to access, exchange, or use EHI. Thus, we look at accountability through the lens of whether the actor is the individual or entity engaging in the practice.

Regarding the comment that we should only hold accountable those parties that actually have control of the EHI or interoperability elements necessary to access, exchange, or use the EHI, we note that we have addressed this issue within preamble discussion concerning the definition of ''interoperability element'' (VIII.C.5.b), Infeasibility Exception (VIII.D.1.d), and Content and Manner Exception (VIII.D.2.a). We refer readers to those discussions.

c. Examples of Practices Likely To Interfere With Access, Exchange, or Use of EHI

To further clarify the scope of the information blocking provision, we described in the Proposed Rule several types of practices that would be likely to interfere with access, exchange, or use of EHI. Those examples clarified and expanded on those set forth in section 3022(a)(2) of the PHSA.

Because information blocking can take many forms, we emphasized that the categories of practices described in the Proposed Rule were illustrative only and did not provide an exhaustive list or comprehensive description of practices that may implicate the information blocking provision and its penalties. We also reiterated that each case will turn on its unique facts. We noted that, for the categories of practices described in the Proposed Rule, we did not consider the applicability of any exceptions. We reiterate that the examples provided in the Proposed Rule were designed to provide greater clarity on the various types of hypothetical practices that could implicate the information blocking provision.

Comments. We received comments requesting that we revise or clarify examples provided in the Proposed Rule in the following sections.

Response. We have not revised or clarified the majority of the examples for purposes of this final rule, and we believe the *majority* of the examples are still applicable. We note in the discussion below necessary clarifications concerning concepts expressed in some of the proposed examples. We refer readers to the Proposed Rule (84 FR 7518 through 7521) for a complete listing of the examples provided for each category of practices below.

i. Restrictions on Access, Exchange, or Use

We explained in the Proposed Rule that the information blocking provision establishes penalties, including civil monetary penalties, or requires appropriate disincentives, for practices that restrict access, exchange, or use of EHI for permissible purposes. We noted that one means by which actors may restrict access, exchange, or use of EHI is through formal restrictions. These may be expressed in contract or license terms, EHI sharing policies, organizational policies or procedures, or other instruments or documents that set forth requirements related to EHI or health IT. Additionally, in the absence of an express contractual restriction, an actor may achieve the same result by exercising intellectual property or other rights in ways that restrict access, exchange, or use (84 FR 7518).

We explained that access, exchange, or use of EHI can also be restricted in less formal ways. The information blocking provision may be implicated, for example, where an actor simply refuses to exchange or to facilitate the access or use of EHI, either as a general practice or in isolated instances. The refusal may be expressly stated or it may be implied from the actor's conduct, such as where the actor ignores requests to share EHI or provide interoperability elements; gives implausible reasons for not doing so; or insists on terms or conditions that are so objectively unreasonable that they amount to a refusal to provide access, exchange, or use of the EHI (84 FR 7518).

We emphasized that restrictions on access, exchange, or use that are required by law would not implicate the information blocking provision. Moreover, we recognized that some restrictions, while not required by law, may be reasonable and necessary for the privacy and security of individuals' EHI and noted that such practices may qualify for protection under an exception (84 FR 7519).

Comments. Commenters requested that we clarify the types of contract and agreement terms that could implicate the information blocking provision beyond terms specifying fees and the licensing of intellectual property rights. Some commenters stated that ''legacy EHR platforms'' impede real time data flow between EHRs and the clinical workflow, including the use of third-party clinical decision support applications, through various contract terms. Many commenters also indicated that EHR developers place onerous contract terms on developers of applications that enable patient access to EHI through APIs. A few commenters asserted that a business associate (BA), as defined under the HIPAA Privacy Rule, should not be liable under the information blocking provision (or there should be an exception for information blocking) for not responding to or fulfilling requests for access, exchange, or use of EHI if such access, exchange, or use of EHI would violate the BA's business associate agreement (BAA).

Response. We first clarify that all of the scenarios provided by the commenters might implicate the information blocking provision. We offer specific situations as follows where there might be an implication. As a first example, an actor (*e.g.,* a health care provider that is a covered entity

under HIPAA) may want to engage an entity for services (*e.g.,* use of a clinical decision support application (''CDS App Developer'')) that require the CDS App Developer to enter into a BAA with the health care provider and, in order to gain access and use of the EHI held by another BA of the health care provider (*e.g.,* EHR developer of certified health IT), the CDS App Developer is required by the EHR developer of certified health IT to enter into a contract to access its EHR technology. As a second example, an entity may offer an application that facilitates patients' access to their EHI through an API maintained by an actor (*e.g.,* EHR developer of certified health IT) that is a BA of a health care provider that is a covered entity under HIPAA. As a third example, a health care provider may request EHI from an actor that is a BA of another health care provider under HIPAA, such as an EHR developer of certified health IT or HIN, that is contracted to make EHI available for treatment purposes.

In response to comments and for the situations described above, we clarify that contracts and agreements can interfere with the access, exchange, and use of EHI through terms besides those that specify unreasonable fees and commercially unreasonable licensing terms (see sections VIII.D.2.b (Fees) and VIII.D.2.c (Licensing) for further discussion of unreasonable fees and commercially unreasonable licensing terms and associated exceptions to the information blocking provision). For instance, a contract may implicate the information blocking provision if it included unconscionable terms for the access, exchange, or use of EHI or licensing of an interoperability element, which could include, but not be limited to, requiring a software company that produced a patient access application to relinquish all IP rights to the actor or agreeing to indemnify the actor for acts beyond standard practice, such as gross negligence on part of the actor. Such terms may be problematic with regard to information blocking in situations involving unequal bargaining power related to accessing, exchanging, and using EHI.

Business Associate Agreements (BAAs)

We designed the final rule to operate in a manner consistent with the framework of the HIPAA Privacy Rule and other laws providing privacy rights for patients. Foremost, we do not require the disclosure of EHI in any way that would not already be permitted under the HIPAA Privacy Rule (or other Federal or State law). However, if an actor is *permitted* to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the information blocking provision would require that the actor provide that access, exchange, or use of EHI so long as the actor is not prohibited by law from doing so (assuming that no exception is available to the actor).

Under the HIPAA Privacy Rule, a BAA must contain the elements specified in 45 CFR 164.504(e), including a description of the permitted and required uses of PHI by the business associate, and provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law.[129] While the information blocking provision does not require actors to violate these agreements, a BAA or its associated service level agreements must not be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule. For example, a BAA entered into by one or more actors that permits access, exchange, or use of EHI by certain health care providers for treatment should generally not prohibit or limit the access, exchange, or use of the EHI for treatment by other health care providers of a patient.

To be clear, both the health care provider(s) who initiated the BAA and the BA who may be an actor under the information blocking provision (*e.g.,* a health IT developer of certified health IT) would be subject to the information blocking provision in the instance described above. To illustrate the potential culpability of a BA, a BA with significant market power may have contractually prohibited or made it difficult for its covered entity customers to exchange EHI, maintained by the BA, with health care providers that use an EHR system of one of the BA's competitors. To determine whether there is information blocking, the actions and processes (*e.g.,* negotiations) of the actors in reaching the BAA and associated service level agreements would need to be reviewed to determine whether there was any action taken by an actor that was likely to interfere with the access, exchange, or use of EHI, and whether the actor had the requisite intent. We further note that if the BA has an agreement with the covered entity to provide EHI to a third party that requests it and the BA refuses to provide the access, exchange, or use of EHI to a requestor in response to the request received by the CE, then the BA (who is also an actor under the information blocking provision) may have violated the information blocking provision unless an exception applied.

Successors to Contractors and Agreements

We note that there may be circumstances in which there is a successor to a contract or agreement when, for example, an actor goes out of business, a provider leaves a practice, or an actor engages in a merger or adopts a new corporate structure. If not handled appropriately, it is possible that information blocking could occur.

ii. Limiting or Restricting the Interoperability of Health IT

We explained in the Proposed Rule that the information blocking provision includes practices that restrict the access, exchange, or use of EHI in various ways (see section 3022(a)(2) of the PHSA). These practices could include, for example, disabling or restricting the use of a capability that enables users to share EHI with users of other systems or to provide access to EHI to certain types of persons or for certain purposes that are legally permissible. In addition, the information blocking provision may be implicated where an actor configures or otherwise implements technology in ways that limit the types of data elements that can be exported or used from the technology. We noted that other practices that would be suspect include configuring capabilities in a way that removes important context, structure, or meaning from the EHI, or that makes the data less accurate, complete, or usable for important purposes for which it may be needed. Likewise, implementing capabilities in ways that create unnecessary delays or response times, or that otherwise limit the timeliness of EHI accessed or exchanged, may interfere with the access, exchange, and use of that information and therefore implicate the information blocking provision. We noted that any conclusions regarding such interference would be based on fact-finding specific to each case and would need to consider the applicability of the exceptions.

We explained that the information blocking provision would be implicated if an actor were to deploy technological measures that limit or restrict the ability to reverse engineer the functional

[129] 45 CFR 164.514(e)(3) limits the use and disclosure of a limited data set (LDS) to only the purposes of research, public health or health care operations. Some of the other restrictions on use and disclosure by a party that receives LDS Recipient are similar to those imposed by the HIPAA Rules on business associates so the discussion that follows generally applies to recipients of LDS and their data use agreements as well as to business associates (and their business associate agreements) to the extent of such similar provisions.

aspects of technology in order to develop means for extracting and using EHI maintained in the technology. We noted that this may include, for example, employing technological protection measures that, if circumvented, would trigger liability under the Digital Millennium Copyright Act (see 17 U.S.C. 1201) or other laws.

Additional Examples

In the context of ONC's certification rules, including certification criteria and Conditions and Maintenance of Certification requirements, we provide the following more explicit examples of actions by actors that would likely constitute information blocking.

The first example of a technical interference that restricts the interoperability of health IT relates to the publication of ''FHIR service base URLs'' (sometimes also referred to as ''FHIR endpoints''). As discussed in the API Condition of Certification preamble (section VII.B.4), an API User needs to know a certified API technology's FHIR service base URL to interact with the certified API technology. This knowledge is foundational for the use of certified API technology without special effort. Therefore, a FHIR service base URL cannot be withheld by an actor as it (just like many other technical interfaces) is necessary to enable the access, exchange, and use of EHI. Notably, in the case of patients seeking access to their EHI, the public availability of FHIR service base URLs is an absolute necessity and without which the access, exchange, and use of EHI would be prevented. Thus, any action by an actor to restrict the public availability of URLs in support of patient access would be more than just likely to interfere with the access, exchange, or use of EHI; it would prevent such access, exchange, and use. Accordingly, as noted in § 170.404(b)(2), a Certified API Developer must publish FHIR service base URLs for certified API technology that can be used by patients to access their electronic health information.

Consistent with this example, the above interpretation means that API Information Sources (*i.e.,* health care providers) who locally manage their FHIR servers without Certified API Developer assistance cannot refuse to provide to Certified API Developers the FHIR service base URL(s) that is/are necessary for patients to use to access their EHI. Equally, pursuant to the Maintenance of Certification requirement finalized for Certified API Developers in § 170.404, they would be required to publish the FHIR service base URLs they centrally manage on behalf of API Information Sources. We also clarify that the public availability of FHIR service base URLs is a requirement that is scoped specifically to the context of patients' access to their EHI and is not intended to be interpreted as requiring all FHIR service base URLs to be made publicly available (*i.e.,* FHIR service base URLs that are created and used among business partners would not need to be made publicly available).

Along the same lines discussed in the example directly above, for a patient to be able to use an application of their choice with certified API technology, the software application will need to be ''registered.'' In that regard, as a second example, an actor's refusal to register a software application that enables a patient to access their EHI would effectively prevent its use given that registration is a technical prerequisite for software applications to be able to connect to certified API technology. As a result, such refusals in the context of patient access unless otherwise addressed in this rule would be highly suspect and likely to implicate information blocking. We note, however, for the first and second example that neither app registration nor the public availability of a FHIR service base URL means that an application will be able to access any EHI. On the contrary, the application would be unable to do so unless a patient authenticates themselves via an appropriate workflow or, in the case of a health care provider, the application is appropriately configured to work within the provider's IT infrastructure.

As a third example, there is often specific information that may be necessary for certain actors, in this case health care providers, to effectively access, exchange, and use EHI via their Certified EHR Technology and certified Health IT Modules. A health care provider's ''direct address'' is an example of this kind of information. If this information were not made known to a health care provider upon request, were inaccessible or hidden in a way that a health care provider could not identify (or find out) their own direct address, or were refused to be provided to a health care provider by a health IT developer with certified health IT, we would consider all such actions to be information blocking because knowledge of a direct address is necessary to fully engage in the exchange of EHI.

As a last example, we note that, to the extent that a legal transfer of IP to an individual or entity that is not an actor is intended to facilitate circumvention of the information blocking provision, the *transfer itself* by an actor could be considered an interference with the access, exchange, or use of EHI.

We note that we have added definitions of ''API Information Source,'' ''API User,'' ''Certified API Developer,'' and ''certified API technology'' to § 171.102. Each of those terms is defined as they are in § 170.404(c). We note that ''API Information Source'' replaced the proposed definition of ''API Data Provider'' and ''Certified API Developer'' replaced the proposed definition of ''API Technology Supplier'' in order to align with the terms used in § 170.404(c) (see the proposed terms in 84 FR 7601).

Comments. A few commenters requested that we provide further clarity on whether slowing or delaying access, exchange, or use of EHI could be considered information blocking.

Response. We clarify that slowing or delaying access, exchange, or use of EHI could constitute an ''interference'' and implicate the information blocking provision. We understand that some delays may be legitimate and inevitable due to factors such as limited legal, project management, and technical resources. Notwithstanding such understandable challenges, we are aware that some actors use and embellish legitimate challenges to create extended and unnecessary delays. For instance, an actor could have legitimate technical scoping and architecture questions regarding data integrations that require attention and take time to address. However, these scoping and architecture questions could constitute interference and implicate the information blocking provision if they are not necessary to enable access, exchange, or use of EHI and are being utilized as a delay tactic. When assessing such practices, facts indicating that an actor created extended or unnecessary delays may be evidence of an actor's intent. We expect actors to make good faith efforts to work through common and understandable challenges and limitations to enable requestors to access, exchange, and use EHI as quickly and efficiently as possible.

iii. Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

We explained in the Proposed Rule that the information blocking provision encompasses practices that create impediments to innovations and advancements to the access, exchange, and use of EHI, including care delivery enabled by health IT (section 3022(a)(2)(C)(ii) of the PHSA). Importantly, the information blocking provision may be implicated and

penalties or appropriate disincentives may apply if an actor were to engage in exclusionary, discriminatory, or other practices that impede the development, dissemination, or use of interoperable technologies and services that enhance access, exchange, or use of EHI.

We emphasized that, most acutely, the information blocking provision may be implicated if an actor were to refuse to license or allow the disclosure of interoperability elements to persons who require those elements to develop and provide interoperable technologies or services—including those that might complement or compete with the actor's own technology or services. The same would be true if the actor were to allow access to interoperability elements but were to restrict their use for these purposes. We provided a list of non-exhaustive examples to illustrate practices that would likely implicate the information blocking provision by interfering with access, exchange, or use of EHI (84 FR 7519 and 7520). We encourage readers to review those examples in the Proposed Rule, as they are still applicable.

We explained that, rather than restricting interoperability elements, an actor may insist on terms or conditions that are burdensome and discourage their use. These practices may implicate the information blocking provision as well. We have chosen not to include those examples in this final rule, but emphasize that they are still applicable and encourage readers to review the examples in the Proposed Rule (84 FR 7520).

We explained that the information blocking provision may also be implicated if an actor were to discourage efforts to develop or use interoperable technologies or services by exercising its influence over customers, users, or other persons, and we provided a non-exhaustive list of examples. We have chosen not to include those examples in this final rule, but emphasize that they are still applicable and encourage readers to review the examples in the Proposed Rule (84 FR 7520).We noted that similar concerns would arise were an actor to engage in discriminatory practices—such as imposing unnecessary and burdensome administrative, technical, contractual, or other requirements on certain persons or classes of persons—that interfere with access and exchange of EHI by frustrating or discouraging efforts to enable interoperability. We provided a list of non-exhaustive examples to illustrate some ways this could occur. We have chosen not to include those examples in this final rule, but emphasize that they are still applicable and encourage readers to review the examples in the Proposed Rule (84 FR 7520).

Not all instances of differential treatment would necessarily constitute a discriminatory practice that may implicate the information blocking provision. For example, we explained that different fee structures or other terms may reflect genuine differences in the cost, quality, or value of the EHI and the effort required to provide access, exchange, or use. We also noted that, in certain circumstances, it may be reasonable and necessary for an actor to restrict or impose reasonable and non-discriminatory terms or conditions on the use of interoperability elements, even though such practices could implicate the information blocking provision. For this reason, and as further explained in section VIII.D, we proposed to establish a narrow exception for licensing interoperability elements (see § 171.303) that would apply to these types of practices.

Comments. We received some recommendations to describe specific scenarios when a refusal to license would be considered information blocking.

Response. We note that for the purposes of the categories of practices described in the Proposed Rule (84 FR 7518 through 7521), we did not consider the applicability of any exceptions, and strongly encouraged readers to review the discussion of practices in this section in conjunction with the section on the exceptions (84 FR 7518). Regarding the specific comment above regarding licensing, we direct readers to our discussion of the Licensing Exception (section VIII.D.2.c.) for additional examples and a discussion of substantive conditions we have finalized for the licensing of interoperability elements under the exception.

We note one important clarification that applies to all examples in the Proposed Rule concerning the licensing of interoperability elements. As clarified in the Licensing Exception preamble discussion, an actor will not implicate the information blocking provision in circumstances where the entity requesting to license or use the interoperability element is not seeking to use the interoperability element to interoperate with either the actor or the actor's customers in order for EHI to be accessed, exchanged, or used. In other words, if there is no nexus between a requestor's need to license an interoperability element and existing EHI, an actor's refusal to license the interoperability element altogether or in accordance with § 171.303 would not constitute an interference under the information blocking provision. We refer readers to the Licensing Exception preamble discussion in section VIII.D.2.c.

Interference Versus Education When an Individual Chooses Technology To Facilitate Access

In the Proposed Rule, we stated that the information blocking provision would likely be implicated when an EHR developer of certified health IT requires third-party applications to be ''vetted'' for security before use but does not promptly conduct the vetting or conducts the vetting in a discriminatory or exclusionary manner (84 FR 7519). We also stated under the proposed ''promoting the privacy of EHI'' exception that when the consent or authorization of an individual was necessary for access, exchange, or use of EHI, to qualify for the exception, an actor must not have improperly encouraged or induced the individual to not provide the consent or authorization. We further stated that this does not mean that an actor cannot inform an individual about the advantages and disadvantages of exchanging EHI and any associated risks, so long as the information communicated is accurate and legitimate. However, we noted that an actor could not mislead an individual about the nature of the consent to be provided, dissuade individuals from providing consent in respect of disclosures to the actor's competitors, or impose onerous requirements to effectuate consent that were unnecessary and not required by law (84 FR 7531).

Overview of Comments

Commenters expressed concerns that app developers not covered by the HIPAA Rules frequently do not provide patients (individuals) with clear terms of how their EHI will be subsequently used by the app developer once patients authorize (approve) the app to receive their EHI. These commenters, many of whom would be actors under the information blocking provision, expressed these concerns in comments recited below, while also requesting clarification about what steps they may take to assist individuals in protecting the privacy and security of their EHI.

Comments. Commenters requested that we clarify the extent of vetting that would be permitted by actors for third-party apps.

Response. We first clarify that the example provided in the Proposed Rule and recited above was to illuminate practices, such as delaying access and

discriminatory behavior, which could implicate the information blocking provision. ''Vetting'' in the example's context meant a determination regarding whether the app posed a security risk to the EHR developer's API, which may be the situation with a proprietary API. For certified API technology, which includes the use of OAuth2 among other security requirements in addition to its focus on ''read-only''/responses to requests for EHI to be transmitted, there should be few, if any, security concerns about the risks posed by patient-facing apps to the disclosing actor's health IT systems (because the apps would only be permitted to receive EHI at the patient's direction). Thus, for third-party applications chosen by individuals to facilitate their access to their EHI held by actors, there would generally not be a need for ''vetting'' on security grounds and such vetting actions otherwise would be an interference. We refer readers to our discussion of ''vetting'' versus verifying an app developer's authenticity under the API Condition of Certification earlier in section VII.B.4 of this preamble. We do note, however, that actors, such as health care providers, have the ability to conduct whatever ''vetting'' they deem necessary of entities (*e.g.,* app developers) that would be their business associates under HIPAA before granting access and use of EHI to the entities. In this regard, covered entities must conduct necessary vetting in order to comply with the HIPAA Security Rule.

Comments. Several commenters stated that the information blocking proposals would open the door for third-party apps (*e.g.,* patient-facing apps) to access, exchange, and use copious amounts of patient data without providing patients with clear terms of use. Commenters stated that most individuals may be surprised when commercial application companies that are not subject to the HIPAA Rules shared health information obtained from a hospital or health plan, such as diagnoses, medications, or test results, in ways the HIPAA Rules would not permit. These commenters asserted that individuals would incorrectly blame the hospital or health plan if a third-party app developer sold their EHI or used it for marketing or other purposes. Additionally, the commenters contended that because the third-party apps and the third-party app developers are not subject to the HIPAA Rules, such developers may, through their apps' required terms of use, grant the developers the right to sell the EHI received or generated by the app without the individual's consent or could expose all of the individual's EHI without the individual's knowledge.

Response. This final rule supports an individual's ability to choose which third-party developer and app are best for receiving all or part of their EHI from a health care provider and to agree to clear and public terms of use on how that initial and ongoing engagement with the third-party developer and app occurs. As discussed in more detail below, this final rule also supports and strongly encourages providing individuals with information that will assist them in making the best choice for themselves in selecting a third-party application. We believe that allowing actors to provide additional information to individuals about apps will assist individuals as they choose apps to receive their EHI and such an approach is consistent with statements in the Proposed Rule recited above regarding informing individuals about the advantages and disadvantages of exchanging EHI and any associated risks. Individuals concerned about information privacy and security can gain a better understanding about how the third-party apps are using and storing their EHI, how individuals will be able to exercise any consent options, and more about what individuals are consenting to before they allow the app to receive their EHI.

Practices that purport to educate patients about the privacy and security practices of applications and parties to whom a patient chooses to receive their EHI may be reviewed by OIG or ONC, as applicable, if there was a claim of information blocking. However, we believe it is unlikely these practices would interfere with the access, exchange, and use of EHI if they meet certain criteria. Foremost, the information provided by actors must focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology. Second, this information must be factually accurate, unbiased, objective, and not unfair or deceptive. Finally, the information must be provided in a non-discriminatory manner. For example, all third-party apps must be treated the same way in terms of whether or not information is provided to individuals about the privacy and security practices employed. To be clear, an actor may not prevent an individual from deciding to provide its EHI to a technology developer or app despite any risks noted regarding the app itself or the third-party developer.

Comments. Several commenters requested that we require actors, including API technology suppliers, to verify the existence of a privacy notice for each application requesting registration by an API User (third-party app developer). Commenters also suggested that the privacy notices should be commensurate with ONC's Model Privacy Notice (MPN). One commenter recommended that all third-party developers should have to attest ''yes'' or ''no'' to having a privacy notice for each app it makes available for use/(for patients to use) to access EHI. The commenter asserted that requiring attestation would provide transparency about the existence or lack of privacy policies and practices and data uses and serve as a means to support enforcement of acts of deceptive or misleading conduct in relation to stated privacy policies and practices.

Response. As noted above, an actor may provide factually accurate, objective, unbiased, fair, and non-discriminatory information about the third party or third-party app that an individual chooses to use to receive EHI on their behalf. And as also noted above, we strongly encourage actors to educate patients and individuals about the risks of providing other entities or parties access to their EHI. This type of education can be designed to inform the patient about the privacy and security practices of the third party and the third-party app, including whether the third-party developer has not acted in accordance with elements of its privacy policy. In this regard, we think there are many efficient and allowable ways of providing such education without such practices being considered or creating an interference under the information blocking provision, including those similar to the one suggested by the commenter.

For example, to the commenter's specific point, actors may establish processes where they notify a patient, call to a patient's attention, or display in advance (as part of the app authorization process with certified API technology) whether the third-party developer of the app that the patient is about to authorize to receive their EHI has attested in the positive or negative whether the third party's privacy policy and practices (including security practices such as whether the app encrypts the EHI) meet certain ''best practices'' set by the market for privacy policies and practices. We note that we identify *minimum* best practices for third-party privacy policies and practices below. This notification, would enable a patient to pause, consider this educational information provided by the actor, and decide whether to proceed with approving the

app to receive their EHI or to stop mid-way in the process to do more research into the app or to pick a different app, in which case the patient would not approve the original app in question to receive their EHI. Understandably, in order for an actor to execute this kind of notification or attention grabbing process and to attribute certain app developer practices to educational insights provided to a patient in real-time, certain information may need to be collected by an actor in advance. Such information may include whether the app developer has a privacy notice, policies, or practices. Actors providing patients with educational information (a notice) could help patients better understand how their EHI may be used by the app and the third-party developer.

While the ONC 2018 MPN is a voluntary, openly available resource designed to help developers clearly convey comprehensive information about their privacy and security policies and practices to their users, the privacy notice and practices of a third-party developer's app or personal health record does not have to be identical to the ONC's 2018 MPN. There may be other privacy policies and practices (including security practices) of third-party developers and apps that accomplish the same goals and even provide more information relevant to a user. At a minimum, as it relates to the above, all third-party privacy policies and practices should adhere to the following:

(1) The privacy policy is made publicly accessible at all times, including updated versions;

(2) The privacy policy is shared with all individuals that use the technology prior to the technology's receipt of EHI from an actor;

(3) The privacy policy is written in plain language and in a manner calculated to inform the individual who uses the technology;

(4) The privacy policy includes a statement of whether and how the individual's EHI may be accessed, exchanged, or used by any other person or other entity, including whether the individual's EHI may be sold at any time (including in the future); and

(5) The privacy policy includes a requirement for express consent from the individual before the individual's EHI is accessed, exchanged, or used, including receiving the individual's express consent before the individual's EHI is sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction).

We note that the market may set different and more stringent expectations for third-party privacy notices and practices than the above minimum. As described above and in the examples below, an actor may provide information or notice to the individual whose EHI is requested from the actor that the privacy policy that applies to the technology used to make the request does or does not meet the minimum privacy policy notice and practices outlined above.

Example 1: Providing education to an individual of a third-party app developer's privacy and security policies and practices through an automated attestation and warning process.

An API User (third-party app developer) develops a software application (named ''App-Y'') and registers it with the Certified API Developer's (developer of certified health IT) authorization server. During the registration process, the Certified API Developer requests, as a business associate and on behalf of a HIPAA covered entity, that the API User attest that for App-Y, the API User follows the privacy policies and practices outlined above. Given the ''yes or no'' choice, the API User attests ''no.'' The Certified API Developer completes App-Y's registration process and provides it with a client identifier. An individual seeks to use App-Y to obtain their EHI from the health care provider (covered entity) that is a customer of the Certified API Developer. The individual then opens App-Y on their smartphone and after authenticating themselves to their health care provider (covered entity), but prior to the app receiving the EHI from the health care provider, the patient is provided with an app authorization screen controlled by the health care provider.

Using the certified API technology and the normal OAuth2 workflow the patient is asked by the health care provider via the app authorization screen whether they want to approve or reject App-Y's ability to receive their EHI via certified API technology. On the authorization screen, there is a ''warning'' from the health care provider that the application has not ''attested'' to having privacy policies and practices that adhere to the minimum policies and practices outlined above or to having other specified privacy *and security* policies. When presented with that warning, the patient has two choices: (1) Choose to ignore the warning and approve App-Y's ability to receive their EHI and App-Y receives the patient's PHI; or (2) reject App-Y's ability to receive their EHI, and the health care provider does not provide the patient's EHI to App-Y.

Example 2: Patient sending EHI using certified health IT capabilities provided by health IT developer.

An individual has made an appointment with a health care specialist for a second medical opinion. During the initial scheduling, the administrative staff requested that the individual bring all their prior health information to the specialist. The patient portal of the individual's primary care provider allows EHI to be transmitted to a third party using Direct protocol. The individual identifies a third-party app that is able to receive EHI using Direct protocol and creates an account with the app as well as obtain/create a ''Direct address.'' During the account creation process with the app, the individual reviews the ''privacy policy'' for the app. The third-party app also sends the individual a copy of the privacy policy via email once the individual completes the account creation process.

Subsequently, the individual logs into the primary care provider's portal to transmit her EHI to her direct address linked to her new account on the third-party app. Her provider uses certified health IT that is capable of sending EHI securely using Direct protocol to third-party organizations (including apps) with which they have exchanged trust anchors. It turns out, the health care provider has established prior trust with the third-party app and is able to send EHI to the application. To note, this health care provider may offer education, including a warning (notice), to the patient, as discussed above, if the provider is being directed by the patient to transmit their EHI to a recipient that is unknown to the provider.

Prior to sending the EHI, the portal provides a summary screen that provides the privacy policy ''warning'' about the third-party app. The patient reviews and accepts it. The provider's system/API technology sends EHI to her Direct address. The patient logs into her application and confirms that the EHI has been received.

Comments. Commenters stated that, given the access to personal health information that patient-directed third-party apps are expected to have and the potential privacy risks they pose, a process should be implemented by the Federal Trade Commission (FTC) to vet apps for the adequacy of the consumer disclosures which should include the privacy and security of the information and secondary uses that should be permitted. A commenter suggested that the vetting process should be at the application and application developer

level, and that the results of such vetting process should be made public in the form of an application ''safe list.''

Response. The privacy practices of developers of patient-facing health IT products and services are typically regulated by the Federal Trade Commission Act (FTC Act). The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce (15 U.S.C. 45(a)(1)), but it does not prescribe specific privacy requirements. The FTC has authority to enforce the FTC Act's prohibition on deception, for example, by challenging deceptive statements made in privacy policies, user interfaces, FAQs, or other consumer-facing materials. The FTC could also, for example, challenge a particular use or disclosure of EHI as unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition (15 U.S.C. 45(n)). We will continue to work with our Federal partners, including the FTC, to assess education opportunities for consumers and app developers about the privacy and security of EHI collected, used, or received by health apps.

Comments. A commenter recommended the development of a privacy framework regarding how health information should be shared and to empowering consumers; and it noted that it should be developed and matured in concert with the modernization of our nation's health IT infrastructure. They expressed that there are private sector and public-private examples of models that we should look to from both health care and other industries. They believed that the Proposed Rule does not, however, fully address patient and consumer privacy protections. They recommended that the Center for Medicare and Medicaid Services and ONC should work together with relevant agencies and departments and private-sector colleagues to develop a companion consumer privacy framework.

Response. We are aware of various industry initiatives regarding a ''privacy framework.'' We have previously published the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information; [130] produced, in cooperation with the FTC, FDA, and OCR, the Mobile Health Apps Interactive Tool; [131] and more recently published and developed the Privacy and Security Framework for Patient-Centered Outcomes Research (PCOR). This project developed tools and resources that address the many different types of data that can be used to conduct patient-centered outcomes research. The framework consists of two initiatives: The Legal and Ethical Architecture for PCOR Data (Architecture), which guides readers through the responsible use and protection of electronic health data for PCOR and The Patient Choice Technical Project which harmonized existing technical mechanisms to enable interoperable exchange of patient consent for basic and granular choice for research and treatment, payment, and health care operations. This project, which remains active, also identifies, tests and validates technical standards that support an individual's consent preferences.[132]

We will continue to monitor how individuals are educated about potential privacy and security risks of third-party apps and will continue to work with HHS OCR and industry stakeholders to further educate individuals as part of our implementation of section 4006 of the Cures Act. In this regard, we also encourage individuals to review consumer education materials related to protecting their EHI on our website at *healthit.gov* (''What You Can do to Protection Your Health Information''—*https://www.healthit.gov/topic/privacy-security/what-you-can-do-protect-your-health-information*; and ''Health IT: How to Keep Your Health Information Privacy and Secure: Fact Sheet''—*https://www.healthit.gov/sites/default/files/how_to_keep_your_health_information_private_and_secure.pdf).*

Comments. Commenters expressed concerns that if patients access their health data—some of which could contain family history and could be sensitive—through a smartphone, they should have a clear understanding of the potential uses of that data by third-party app suppliers.

Response. Under the HIPAA Privacy Rule, when a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual's family medical history, this information may become part of the individual's medical record (45 CFR 164.501 (definition of ''Designated Record Set''). Thus, if the family medical history becomes part of the medical record, the individual/patient may exercise the rights under the HIPAA Privacy Rule, 45 CFR 164.524, to this information in the same fashion as any other information in the medical record, including the right of access. As discussed above, actors may educate patients of the risks related to providing other persons and entities with their EHI, including the various the types of EHI (*e.g.,* family health history) that will be provided to an entity (*e.g.,* third-party app) at the patient's request.

iv. Rent-Seeking and Other Opportunistic Pricing Practices

Certain practices that artificially increase the cost and expense associated with accessing, exchanging, and using EHI may implicate the information blocking provision. We emphasized in the Proposed Rule that such practices are plainly contrary to the information blocking provision and the concerns that motivated its enactment.

We explained that an actor may seek to extract profits or capture revenue streams that would be unobtainable without control of a technology or other interoperability elements that are necessary to enable or facilitate access, exchange, or use of EHI. Most EHI is currently stored in EHRs and other source systems that use proprietary data models or formats; this puts EHR developers (and other actors that control data models or standards) in a unique position to block access to (including the export and portability of) EHI for use in competing systems or applications or to charge rents for access to the basic technical information needed to accomplish the access, exchange, or use of EHI for these purposes. We emphasized that these information blocking concerns may be compounded to the extent that EHR developers do not disclose, in advance, the fees they will charge for interfaces, data export, data portability, and other interoperability-related services (see 80 FR 62719 through 62725; 80 FR 16880 through 16881). We noted that these concerns are not limited to EHR developers. Other actors who exercise substantial control over EHI or essential interoperability elements may engage in analogous behaviors that would implicate the information blocking provision (84 FR 7520).

To illustrate, we provided a list of non-exhaustive examples that reflected some of the more common types of rent-seeking and opportunistic behaviors of which we were aware and that are likely to interfere with access, exchange, or use of EHI. Those examples are still applicable and we encourage readers to

[130] *https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.*

[131] *https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.*

[132] *See https://www.healthit.gov/topic/scientific-initiatives/pcor/privacy-and-security-framework-pcor-psp.*

review the examples in the Proposed Rule (84 FR 7520 and 7521).

The information blocking provision may be implicated by these and other practices by which an actor profits from its unreasonable control over EHI or interoperability elements without adding any efficiency to the health care system or serving any other pro-competitive purpose. However, we stressed that the reach of the information blocking provision is not limited to these types of practices. We interpreted the definition of information blocking to encompass any fee that materially discourages or otherwise imposes a material impediment to access, exchange, or use of EHI. We used the term ''fee'' in the broadest possible sense to refer to any present or future obligation to pay money or provide any other thing of value and proposed to include this definition in § 171.102. We noted that this scope may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services. Therefore, as further explained in section VIII.D, we proposed to create an exception that, subject to certain conditions, would permit the recovery of costs that are reasonably incurred to provide access, exchange, and use of EHI (84 FR 7521).

Comments. We did not receive comments specifically on our proposed definition of ''fee.''

Response. We have finalized the definition in § 171.102 as proposed.

Comments. A few commenters requested additional examples and clarity on the types of rent-seeking and opportunistic pricing practices that would be likely to implicate the information blocking provision.

Response. We refer readers to our discussion of the Fees Exception (section VIII.D.2.b.) for additional examples, as well as for a detailed discussion of fees that may and may not be charged under this exception.

v. Non-Standard Implementation Practices

We explained in the Proposed Rule that section 3022(a)(2)(B) of the PHSA states that information blocking may include implementing health IT in non-standard ways that substantially increase the complexity or burden of accessing, exchanging, or using EHI. In general, this type of interference is likely to occur when, despite the availability of generally accepted technical, policy, or other approaches that are suitable for achieving a particular implementation objective, an actor does not implement the standard, does not implement updates to the standard, or implements the standard in a way that materially deviates from its formal specifications. We noted that these practices lead to unnecessary complexity and burden, such as the additional cost and effort required to implement and maintain ''point-to-point'' connections, custom-built interfaces, and one-off trust agreements.

While each case will necessarily depend on its individual facts, and while we recognized that the development and adoption of standards across the health IT industry is an ongoing process, we explained that the information blocking provision would be implicated in at least two distinct sets of circumstances. First, we stated that information blocking may arise where an actor chooses not to adopt, or to materially deviate from, relevant standards, implementation specifications, and certification criteria adopted by the Secretary under section 3004 of the PHSA. Second, even where no federally adopted or identified standard exists, if a particular implementation approach has been broadly adopted in a relevant industry segment, deviations from that approach would be suspect unless strictly necessary to achieve substantial efficiencies.

To further illustrate these types of practices that may implicate the information blocking provision, we provided a list of non-exhaustive examples of conduct that would be likely to interfere with access, exchange, or use of EHI. We have chosen not to include those examples in this final rule, but emphasize that they are still applicable and encourage readers to review the examples in the Proposed Rule (84 FR 7521).

We explained that even where no standards exist for a particular purpose, actors should not design or implement health IT in non-standard ways that unnecessarily increase the costs, complexity, and other burdens of accessing, exchanging, or using EHI. We also noted that we were aware that some actors attribute certain non-standard implementations on legacy systems that the actor did not themselves design but which have to be integrated into the actor's health IT. We noted that such instances will be considered on a case-by-case basis.

Comments. A few commenters requested additional clarity on when non-standard based interoperability is permissible. Some commenters urged ONC to be careful and flexible in its interpretation of this information blocking practice given the complexities of health IT implementation, such as implementing newly adopted standards or requirements. One commenter highlighted the importance of being able to retain certain types of optionality, especially for specialized use cases. Other commenters expressed concern that considering non-standard implementation practices as likely to implicate the information blocking provision could have the unintended consequence of stymying innovative or novel technologies used in information exchange.

Response. We appreciate the commenters' suggestions. We emphasize that the problematic nature of non-standard design and implementation choices was identified by Congress in section 3022(a)(2)(B) of the PHSA, which states that information blocking may include implementing health IT in non-standard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI. We continue to be concerned that these practices will lead to unnecessary complexity and burden related to the access, exchange, or use of EHI, and depending on the circumstances, we maintain that such practices would be likely to interfere with access, exchange, or use of EHI. We refer readers to the discussion of this topic in the Fees Exception (section VIII.D.2.b).

We also agree, however, that we must give each case careful consideration and assess the individual facts and circumstances to determine whether such practices would be likely to interfere with access, exchange, or use of EHI.

7. Applicability of Exceptions

a. Reasonable and Necessary Activities

Section 3022(a)(3) of the PHSA requires the Secretary to identify, through notice and comment rulemaking, reasonable and necessary *activities* that do not constitute information blocking for purposes of the definition in section 3022(a)(1). Section 3022(a)(1) of the PHSA defines information blocking by referring to *practices* likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information. Based on this terminology used in the PHSA, we noted that conduct that implicates the information blocking provision and that does not fall within one of the exceptions or does not meet all conditions for an exception, would be considered a ''practice.'' Conduct that falls within an exception and meets all the applicable conditions for that exception would be considered

an ''activity.'' We noted that the challenge with this distinction is that when examining conduct that is the subject of an information blocking claim—an actor's actions that are likely to interfere with access, exchange, or use of EHI—it can be illusory to distinguish, on its face, conduct that is a *practice* and conduct that is an *activity.* Indeed, conduct that implicates the information blocking provision but falls within an exception could nonetheless be considered information blocking if the actor has not satisfied the conditions applicable to that exception.

Acknowledging the terminology used in the PHSA, we proposed to define ''practice'' in § 171.102 as one or more related acts or omissions by an actor.

We also proposed to use the term ''practice'' throughout the Proposed Rule when we described conduct that is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, and clarify when describing the conduct at issue whether it is a practice that is information blocking, a practice that implicates the information blocking provision, or a practice that is reasonable and necessary and not information blocking (84 FR 7522). We stated that adopting the terminology of ''activity'' to describe conduct that may or may not be information blocking would be confusing and obfuscate our intent in certain circumstances. Consistent with this approach, when describing the exceptions in the final rule, we describe *practices* that, if all the applicable conditions are met, are reasonable and necessary and not information blocking.

Comments. We received no comments specifically on the distinction between ''activities'' and ''practices'' and our proposed definition and use of the term ''practice.''

Response. We have finalized the definition of ''practice'' in § 171.102 as ''an act or omission by an actor.'' This definition is a modification of the proposed definition, which was ''one or more related acts or omissions by an actor.'' We finalized this definition of ''practice'' in order to clarify that a practice need only be a single act or omission. This modification does not substantively change the proposed definition, as we included in the proposed definition that a ''practice'' *could* be one act or omission.

We have finalized the use of the term ''practice,'' rather than the term ''activity,'' to describe conduct that is likely to interfere with, prevent or materially discourage the access, exchange, or use of EHI. We have also finalized our approach that when identifying exceptions, we describe *practices* that, if all the applicable conditions are met, are reasonable and necessary and not information blocking.

b. Treatment of Different Types of Actors

We explained in the Proposed Rule that the proposed exceptions would apply to health care providers, health IT developers of certified health IT, HIEs, and HINs who engage in certain practices covered by an exception, provided that all applicable conditions of the exception are satisfied at all relevant times and for each practice for which the exception is sought. We noted that the exceptions are generally applicable to all actors. However, in some instances, we proposed conditions within an exception that apply to a particular type of actor.

Comments. Several commenters agreed that the exceptions should apply to all actors. A few commenters requested that ONC identify exceptions that apply to all actors and identify exceptions that only apply to select actors.

Response. We appreciate the support for our approach to the exceptions, as well as the suggestion to restructure the exceptions. We continue to believe that the clearest and most equitable approach to the exceptions is to make all of the exceptions apply to all actors, as proposed. We have addressed the commenters' concerns by creating conditions within certain exceptions that apply to one or a subset of actors, as applicable.

c. Establishing That Practices Meet the Conditions of an Exception

We proposed that, in the event of an investigation of an information blocking complaint, an actor must demonstrate that an exception is applicable and that the actor met all relevant conditions of the exception at all relevant times and for each practice for which the exception is sought (84 FR 7522). We considered this allocation of proof to be a substantive condition of the proposed exceptions. As a practical matter, we proposed that actors are in the best position to demonstrate compliance with the conditions of the exceptions and to produce the detailed evidence necessary to demonstrate that compliance. We requested comment about the types of documentation and/or standardized methods that an actor may use to demonstrate compliance with the exception conditions.

Comments. Many commenters requested clarification regarding the type and amount of documentation required to demonstrate that they have met an exception. In particular, many commenters noted that meeting the exceptions will substantially increase documentation burden and other administrative costs for actors. Commenters also noted that organizations may need to update, develop and/or implement policies and procedures focused on documenting compliance with information blocking exceptions. Many commenters requested that ONC develop and provide examples, templates, and guidance on the type of documentation that would be acceptable to support the conditions for each information blocking exception. Several commenters noted that the supporting documentation should clearly demonstrate why the actor qualifies for the exception, why the exception is required, and how all conditions of the exception are fulfilled. One commenter asked that we provide guidance on the appropriate storage method for this documentation, as this information may not be appropriate for the clinical record.

Response. We thank commenters for these thoughtful comments and suggestions. We have tailored the exceptions and provided significant detail within each exception to clearly explain what an actor must do to meet each exception. For each exception, we have proposed and finalized conditions that we believe can be consistently applied across a range of actors and practices and also further the goals of the information blocking provision. For some exceptions, this includes a writing or documentation requirement to demonstrate that the practice precisely meets all of the conditions to afford an actor the enhanced assurance an exception offers. Many of these conditions are related to other existing regulatory requirements that have similar documentation standards. For example, an actor's practice may meet the Security Exception at § 171.203 if it is consistent with an organizational security policy and that policy meets several requirements. We expect that many actors have existing organizational security policies based on the ''Policy and procedures and documentation requirements'' in the HIPAA Security Rule at 45 CFR 164.316. Consequently, the burden associated with meeting the documentation requirement in the Security Exception should be less if actors are already complying with the HIPAA Security Rule.

We encourage actors to voluntarily comply with an exception so that their practices do not meet the definition of information blocking and are not subject

to information blocking enforcement. However, failure to meet an exception does not necessarily mean a practice meets the definition of information blocking. If subject to an investigation, each practice that implicates the information blocking provision and does not meet an exception would be analyzed on a case-by-case basis to evaluate, for example, whether it rises to the level of an interference, and whether the actor acted with the requisite intent.

D. Exceptions to the Information Blocking Definition

We proposed to establish seven exceptions to the information blocking provision. The exceptions would apply to certain practices that may technically meet the definition of information blocking but that are reasonable and necessary to further the underlying public policies of the information blocking provision. We appreciate that most actors will want to meet an exception to guarantee that their practice or practices do not meet the definition of information blocking and be subject to enforcement. The statute defines information blocking broadly and in a manner that allows for careful consideration of relevant facts and circumstances in individual cases, which includes analysis of an actor's intent and whether it meets the requisite knowledge standard.

The proposed exceptions were based on three related policy considerations. First, each exception was limited to certain activities that clearly advance the aims of the information blocking provision. These reasonable and necessary activities included providing appropriate protections to prevent harm to patients and others; promoting the privacy and security of EHI; promoting competition and innovation in health IT and its use to provide health care services to consumers, and to develop more efficient means of health care delivery; and allowing system downtime to implement upgrades, repairs, and other changes to health IT. Second, each proposed exception addressed a significant risk that regulated actors will not engage in these beneficial activities because of uncertainty concerning the breadth or applicability of the information blocking provision. Finally, each exception was subject to strict conditions to ensure that it was limited to activities that are reasonable and necessary.

We explained that the first three exceptions extended to certain activities that are reasonable and necessary to prevent harm to patients and others; promote the privacy of EHI; and promote the security of EHI, subject to strict conditions to prevent the exceptions from being misused. We discussed that without these exceptions, actors may be reluctant to engage in the reasonable and necessary activities and that this could erode trust in the health IT ecosystem and undermine efforts to provide access and facilitate the exchange and use of EHI for important purposes. We stressed that such a result would be contrary to the purpose of the information blocking provision and the broader policies of the Cures Act.

We explained that the next three exceptions addressed activities that are reasonable and necessary to promote competition and consumer welfare. First, we proposed to permit the recovery of certain types of reasonable costs incurred to provide technology and services that enable access to EHI and facilitate the exchange and use of that information, provided certain conditions are met. Second, we proposed to permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, subject to a duty to provide a reasonable alternative. And third, we proposed an exception that would permit an actor to license interoperability elements on reasonable and non-discriminatory terms. We emphasized that the exceptions would be subject to strict conditions to ensure that they do not extend protection to practices that raise information blocking concerns.

The last exception recognized that it may be reasonable and necessary for actors to make health IT temporarily unavailable for the benefit of the overall performance of health IT. This exception would permit an actor to make the operation of health IT unavailable to implement upgrades, repairs, and other changes.

As context for the proposed exceptions, we noted that addressing information blocking is critical for promoting competition and innovation in health IT and for the delivery of health care services to consumers. We noted that the information blocking provision itself expressly addresses practices that impede innovation and advancement in health information access, exchange, and use, including care delivery enabled by health IT (section 3022(a)(2)(C)(ii) of the PHSA). We also noted that health IT developers of certified health IT, HIEs, HINs, and, in some instances, health care providers, may exploit their control over interoperability elements to create barriers to entry for competing technologies and services that offer greater value for health IT customers and users, provide new or improved capabilities, and enable more robust access, exchange, and use of EHI.[133] More than this, we emphasized that information blocking may harm competition not just in health IT markets, but also in markets for health care services.[134] Dominant providers in these markets may leverage their control over technology to limit patient mobility and choice.[135] They may also pressure independent providers to adopt expensive, hospital-centric technologies that do not suit their workflows, limit their ability to share information with unaffiliated providers, and make it difficult to adopt or use alternative technologies that could offer greater efficiency and other benefits.[136] The technological dependence resulting from these practices can be a barrier to entry by would-be competitors. It can also make independent providers vulnerable to acquisition or induce them into exclusive arrangements that enhance the market power of incumbent providers while preventing the formation of clinically-integrated products and networks that offer more choice and better value to consumers and purchasers of health care services.

We noted in the Proposed Rule that section 3022(a)(5) of the PHSA provides that the Secretary may consult with the Federal Trade Commission (FTC) in defining practices that do not constitute information blocking because they are necessary to promote competition and consumer welfare. We expressed appreciation for the expertise and informal technical assistance of FTC staff, which we took into consideration in developing the exceptions for recovering costs reasonably incurred, responding to requests that are infeasible, and licensing of interoperability elements on reasonable and non-discriminatory terms. We noted that the language in the Cures Act regarding information blocking is substantively and substantially different

[133] *See also* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, *Making Health Care Markets Work: Competition Policy for Health Care,* 16–17 (Apr. 2017), available at *http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930.*

[134] *See, e.g.,* Keynote Address of FTC Chairwoman Edith Ramirez, Antitrust in Healthcare Conference Arlington, VA (May 12, 2016), available at *https://www.ftc.gov/system/files/documents/public_statements/950143/160519antitrusthealthcarekeynote.pdf.*

[135] *See, e.g.,* Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, *Making Health Care Markets Work: Competition Policy for Health Care,* 16–17 (Apr. 2017), available at *http://heinz.cmu.edu/news/news-detail/index.aspx?nid=3930.*

[136] *See, e.g., Healthcare Research Firm Toughens Survey Standards as More CIOs Reap the Profits of Reselling Vendor Software,* Black Book, available at *http://www.prweb.com/releases/2015/02/prweb12530856.htm*; Arthur Allen, *Connecticut Law Bans EHR-linked Information Blocking,* Politico.com (Oct. 29, 2015).

from the language and goals in the antitrust laws enforced by the FTC. We explained that we view the Cures Act as addressing conduct that may be considered permissible under the antitrust laws. On this basis, the Proposed Rule required that actors who control interoperability elements cooperate with individuals and entities that require those elements for the purpose of developing, disseminating, and enabling technologies and services that can interoperate with the actor's technology.

We emphasized that ONC took this approach because we view patients as having an overwhelming interest in EHI about themselves. As such, access to EHI, and the EHI itself, should not be traded or sold by those actors who are custodians of EHI or who control its access, exchange, or use. We emphasized that such actors should not be able to charge fees for providing electronic access, exchange, or use of patients' EHI. We explained that the information blocking provision prohibits actors from interfering with the access, exchange, or use of EHI unless they are required to do so under an existing law or are covered by one of the exceptions detailed in this preamble. In addition, we explained that any remedy sought or action taken by HHS under the information blocking provision would be independent of the antitrust laws and would not prevent FTC or DOJ from taking action with regard to the same actor or conduct.

We proposed to include a provision in § 171.200 that addresses the availability and effect of exceptions.

We requested comment on the seven proposed exceptions, including whether they will achieve our stated policy goals.

Comments. We received comments regarding each of the proposed exceptions.

Response. We have responded to the comments regarding each exception in the preamble discussions for each exception. Overall, we have made modifications to the structure and scope of the proposed exceptions.

In this final rule, we have restructured the proposed exceptions (proposed in §§ 171.201–207) and have added another exception for clarity. In addition, we have divided the exceptions into two categories: (1) Exceptions that involve not fulfilling requests to access, exchange, or use EHI, which are finalized in §§ 171.201–205; and (2) exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI, which are finalized in §§ 171.301–303. We also changed the titles of the exceptions to questions for additional clarity. We believe this new structure will help actors better understand our expectations of them and enhance transparency around the exceptions.

We note that we use the term ''fulfill'' throughout the exceptions in the context of an actor ''fulfilling'' a request to access, exchange, or use EHI. This term is intended to reflect not just a response to a request to access, exchange, or use EHI, but also making the EHI available for the requested access, exchange, or use.

We have finalized the seven exceptions with modifications discussed below. Based on requests for comment we included in the Proposed Rule regarding the scope of the EHI definition (84 FR 7513) and the Infeasibility Exception (84 FR 7542 through 7544), we have also established a new exception in § 171.301 (referred to as the Content and Manner Exception) under section 3022(a)(3) of the PHSA as a means to identify reasonable and necessary activities that do not constitute information blocking. We discuss the details of the new Content and Manner Exception in section VIII.D.2.a of this preamble.

We appreciate the FTC's comments on the Proposed Rule and the expertise and informal technical assistance provided by FTC staff for this final rule, which we took into consideration throughout our development of the final rule, including as it relates to the definitions of various terms in the final rule (*e.g.,* the definitions of ''electronic health information'' and ''health information network'' (discussed above)) and the exceptions (*e.g.,* the Infeasibility Exception, Fees Exception, and Licensing Exception; as well as the establishing of the new Content and Manner Exception).

Comments. We did not receive any comments on the provision in § 171.200.

Response. We have finalized § 171.200 as proposed and have included an identical provision in § 171.300 that is applicable to Part C. This addition was necessary based on the new structure of the exceptions discussed above.

1. Exceptions that involve not fulfilling requests to access, exchange, or use EHI

a. Preventing Harm Exception — When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking?

We proposed to establish an exception to the information blocking provision in § 171.201 that would apply to certain practices that are reasonable and necessary to prevent harm to a patient or another person. As discussed in the Proposed Rule's preamble (84 FR 7523 and 7524), this exception is intended to allow for the protection of patients and other particular persons against substantial risks of harm otherwise arising from the access, exchange, or use of EHI in defined circumstances. Strict conditions were proposed to prevent this exception from being misused.

As explained in the Proposed Rule, we use the term ''patient'' to denote the context in which the threat of harm arises (84 FR 7523). That is, this exception has been designed to recognize practices taken for the benefit of recipients of health care — those individuals whose EHI is at issue — and other persons whose information may be recorded in that EHI or who may be at risk of harm because of the access, use, or exchange of the EHI. This use of the term ''patient'' in the Proposed Rule did *not* imply that practices to which the exception is applicable could be implemented only by the licensed health professionals with a clinician-patient relationship to the person whose EHI is affected by the practices.

This exception was proposed to apply to practices when the actor engaging in a practice has a reasonable belief that the practice will directly and substantially reduce a risk of harm to the patient, and/or other particular individuals, that would otherwise arise from the particular access, exchange, or use of EHI affected by the practices. We proposed that actors including but not limited to health care providers would, consistent with conditions of the exception applicable to the circumstances in which the practices are used, be able to engage in practices recognized under this exception without the actor needing to have a clinician-patient relationship with any of the individuals at risk of harm.

Comments. Of more than ninety comment submissions specifically referencing the Preventing Harm Exception, half expressed overarching or general support for the exception. None of the comments specifically referencing this exception expressed opposition to the exception. Some commenters advocated broadening certain aspects of the proposed exception, as discussed in more detail below. Several other commenters expressed support for a relatively narrow exception, and a few of these commenters recommended that once the final rule is effective ONC should engage in monitoring to ensure the exception is not abused in practice. Many commenters requested

clarification on specific points, or expressed concerns or suggested modifications to particular aspects of the exception, as will be discussed in more detail below.

Response. We appreciate the many thoughtful comments on the value of this exception, particular aspects of the proposed exception, and areas where we could streamline how we express the policy so it is easier to understand. Considering all of the comments received, we have decided to finalize the exception largely as proposed, with modifications to better align with HIPAA Rules as discussed below and to make the regulation text more easily understood. These revisions include modification of the title of § 171.201, from ''Exception—Preventing Harm'' (84 FR 7602) to ''Preventing Harm Exception — When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking?'' Throughout this preamble, we use ''Preventing Harm Exception'' as a short title for ease of reference to the exception that has been finalized in § 171.201.

Comments. Several comments suggested broadening the scope of the exception to allow a broader array of actors to decide what might pose a risk of harm to a patient.

Response. The finalized exception is, as we proposed it would be, available to any actor defined in § 171.102, provided that the actor's use of a practice for purposes of harm prevention meets the conditions in § 171.201. Only where practices are applied to a specific patient's EHI and based upon a determination of a risk of harm by a licensed health care professional in the exercise of professional judgment does this exception explicitly require the determination to have been made by a particular subset of actors within the definitions in § 171.102. In order to meet the risk of harm condition based on an individualized determination consistent with § 171.201(c)(1), the licensed health care professional who made the determination must have done so in context of a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination.[137] However, other actors — such as other health care providers treating the same patient, or an HIE/HIN supporting access, exchange, or use of the patient's EHI — could rely on such a determination of a risk of harm. The actor's knowledge of a licensed health care professional's individualized determination (consistent with § 171.201(c)(1)) that access, exchange, or use posed a risk of a harm of a type consistent with § 171.201(d)(1), (2), or (3) (as applicable) could factor into a determination based on facts and circumstances known or reasonably believed by the actor (consistent with the condition finalized § 171.201(f)(2)).

An actor could also implement practices based on knowledge of an individualized determination of risk (§ 171.201(c)(1)) of harm of a type consistent with § 171.201(d)(1), (2), or (3) as applicable and based on an organizational policy (consistent with the condition finalized § 171.201(f)(1)). Thus, the exception is broad enough to cover all actors implementing practices that meet its conditions. We are finalizing this aspect of the exception as proposed, with clarifications to the regulation text to make it easier to understand what the specific conditions of the Preventing Harm Exception are and how they relate to one another.

Comments. A large number of commenters requested additional guidance in this final rule preamble or through other avenues. For example, some commenters requested sub-regulatory guidance and educational resource materials to further illustrate and help actors understand how the Preventing Harm Exception might apply or what it might require without a stakeholder needing to raise particular questions or hypothetical fact patterns.

Response. With the revisions we have made to this exception, we do not believe sub-regulatory guidance is necessary for actors who wish to avail themselves of this exception to understand the Preventing Harm Exception, its conditions, or to conform their practices to the conditions. We have made revisions to the regulation text to provide enhanced clarity, such as separately expressing each of its substantive conditions and incorporating granular alignment to 45 CFR 164.524(a)(3) harm standards. This final rule preamble provides additional information and feedback through discussion of the particular questions and suggestions posed by various commenters and this preamble's statements of finalized policy. We will also provide, in connection to this final rule, educational resources such as infographics, fact sheets, webinars, and other forms of educational materials and outreach. We emphasize, however, that we believe the final rule clearly describes our information blocking policies, and these educational materials are intended only to educate stakeholders on our final policies established in the final rule.

Comments. Several commenters questioned whether ''directly and substantially'' may be a more stringent standard than is necessary for the reduction of risk of harm to a patient or to another person. A number of commenters indicated it could be difficult for actors to know where to draw the line between direct and indirect reductions of risk of harm, given the potential for reasonable minds to disagree on the extent to which a risk arises directly, as opposed to indirectly, from the EHI access, exchange, or use affected by a practice. Several commenters recommended, as an alternative, that the condition be that the actor have a reasonable belief the practice is ''reasonably likely'' to reduce a risk of harm.

Response. After considering comments received, we have finalized in § 171.201(a) that the actor must hold a reasonable belief that the practice ''will substantially reduce'' a risk of harm to a patient or another natural person. In comparison to the regulation text of this exception in the Proposed Rule (84 FR 7602), we have removed ''directly'' from the finalized text of § 171.201(a). We believe omitting ''directly'' from the finalized condition obviates concerns about actors' ability to determine whether the practice directly reduces a risk of harm that could itself arise indirectly. We have retained ''substantially'' in the finalized § 171.201(a) because we believe it is necessary to ensure this exception cannot be misused to justify practices that interfere with access, exchange, or use of EHI to achieve only a trivial or illusory reduction in risk of harm. By extension, we interpret a ''substantial reduction'' as necessarily implying that the risk intended to be reduced was itself substantial and not trivial or illusory.

We note that the harm standard under § 164.524(a)(3) of the HIPAA Rules includes that the access requested be ''reasonably likely'' to cause the type of harm described in the sub-paragraph applicable to a particular denial of access under § 164.524(a)(3). As discussed in context of the finalized type of harm condition (§ 171.201(d)),

[137] For purposes of this exception, we interpret ''clinician-patient relationship'' to include any therapeutic or relationship where the licensed health care professional has or at some point had some clinical responsibility for or to the patient within the professional's scope of practice. Thus, a clinician-patient relationship on which a qualifying individualized determination of risk of harm could be one of substantial duration over time or formed in the course of the first or only occasion on which the clinician furnishes or furnished professional services to the patient in any setting, including but not limited to telehealth.

below, we have aligned the conditions of the Preventing Harm Exception finalized in § 171.201 to use the same harm standards as § 164.524(a)(3) in circumstances where both apply and in circumstances where only § 171.201 applies. In order to maintain alignment and consistency, we clarify that in circumstances where only § 171.201 applies, the risk of harm must also initially be at least ''reasonably likely,'' regardless of whether the risk of harm is consistent with subparagraph (1) or (2) of the type of risk condition finalized in § 171.201(c). To satisfy the reasonable belief condition finalized in § 171.201(a), the actor must reasonably believe their practices (that are likely to, or in fact do, interfere with otherwise permissible access, exchange, or use of EHI) will substantially reduce that likelihood of harm. Actors who are HIPAA covered entities or business associates have extensive experience in complying with § 164.524(a)(3). Therefore, we believe the belief standard finalized in § 171.201(a), combined with reliance on the harm standards used in § 164.524(a)(3), will address commenters' concerns about their ability to understand and apply the reasonable belief and type of harm conditions finalized under § 171.201.

Comments. A number of commenters advocated closer alignment with the HIPAA Privacy Rule. Some commenters expressed concerns about our ability to maintain such alignment without interruption if this rule were to be finalized prior to any applicable potential updates to the HIPAA Privacy Rule pursuant to a proposed rule that HHS had publicly expressed an aim to publish in 2019. Some commenters specifically questioned whether ''life or physical safety'' would remain the standard for the type of harm cognizable under the Privacy Rule for denying an individual's right to access their own information. One commenter stated they had heard the Privacy Rule harm standard might be broadened to recognize additional types of harm, such as emotional or psychological harm, in circumstances where the Privacy Rule would currently recognize only danger to life or physical safety. A number of comments stated that the requirement for the risk to be to life or physical safety for all circumstances where this exception would apply would conflict with current Privacy Rule provisions applicable to individual or proxy access to PHI. A number of commenters recommended we revise the conditions for practices to be recognized under the Preventing Harm Exception so that harm cognizable under the Privacy Rule under particular circumstances would also be cognizable under § 171.201.

Response. We understand commenters' concerns about inconsistency across this exception and the Privacy Rule. In particular, concerns that center on the fact that requiring in § 171.201 that the risk must be to the ''life or physical safety'' of the patient or another person in all circumstances where § 171.201 applies would have set a different harm standard than applies under § 164.524(a)(3) in particular circumstances where both §§ 171.201 and 164.524(a)(3) apply. Specifically, where § 164.524(a)(3)(ii) or (iii) apply, the reviewable grounds for denial of right of access include where a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is likely to cause ''substantial harm.'' In contrast, a uniform application of the ''life or physical safety'' type of harm under § 171.201 would have applied the ''life or physical safety'' type of harm standard to practices that interfere with access, exchange, or use of EHI for purposes of § 171.201 even where § 164.524(a)(3)(ii) or (iii) would also apply and where § 164.524(a)(3)(ii) or (iii) would apply the ''substantial harm'' standard.

In response to comments, we have reviewed the potential for conflict between § 171.201 requiring ''life or physical safety'' as the type of harm in circumstances where § 164.524(a)(3(ii) or (iii) also apply. We have determined that for particular types of circumstances where both §§ 171.201 and 164.524(a)(3) apply, the best approach is to apply under § 171.201 the exact same harm standard that each specific sub-paragraph of § 164.524(a)(3) applies in each of these types of circumstances. We believe that extending the application under § 171.201 of the specific harm standards in § 164.524(a)(3)(i) through (iii) to situations that are similar in significant respects to situations where each of these sub-paragraphs of § 165.524(a)(3) would apply, but where § 164.524(a)(3) does not apply, provides consistency that simplifies compliance for actors subject to both 45 CFR part 171 and 45 CFR part 164. Situations where § 171.201 could apply but where § 164.524(a)(3) would not apply include, but are not limited to, those where the actor's practice is likely to interfere with an individual or their legal representative's access, exchange, or use of the individual's EHI but not to the extent of failing to provide access (as the term is used in context of § 164.524) within the timeframe allowed under § 164.524.

To make the alignment between the Preventing Harm Exception and the Privacy Rule clear, the final regulation text at § 171.201(d) cross-references the specific types of harm that would serve as grounds for denying an individual or their personal representative access to their PHI under the Privacy Rule (§ 164.524(a)(3)) in particular types of circumstances.[138] By cross-referencing to § 164.524(a)(3), we align the regulations to streamline compliance for actors. We also believe this approach will allow that alignment to remain in place if changes were to be made to § 164.524(a)(3) harm standards in the future.[139] In particular types of circumstances where both § 164.524(a)(3) and § 171.201 apply, the subparagraphs of finalized § 171.201(d) (the type of harm condition) cross-reference to the § 164.524(a)(3)(i), (ii), and (iii) harm standard that applies under § 171.201 in each of these types of circumstances. Moreover, where only § 171.201 applies to a practice where the type of risk is consistent with § 171.201(c)(1), the finalized subparagraphs of § 171.201(d) cross-reference and apply the harm standard that § 164.524(a)(3)(i), (ii), or (iii) would apply to denial of the individual's (§ 164.524) right of access to their own PHI, the individual or their representative's access to the PII of another person within that PHI, or the individual's personal representative's access to the individual's PHI.

One example of a particular circumstance in which both § 164.524(a)(3) and § 171.201 would apply is where a health care provider (as defined in § 171.102) that is also a HIPAA covered entity (as defined in § 160.103) denies the patient's personal representative access to the patient's EHI based on a licensed health care professional's determination in the exercise of professional judgment (§ 171.201(c)(1)) that granting that personal representative access to the patient's EHI would pose a risk of substantial harm to the patient.[140] In

[138] Meeting the harm standard is necessary but not alone sufficient for a practice to be recognized as reasonable and necessary under this exception; all other conditions of the exception must also be met.

[139] Alignment between part 171 subpart B and § 164.524(a)(1) and (2) is discussed in Section VIII.D.2. We also acknowledge that it is possible some types of revision to 45 CFR part 164 could necessitate modifications to 45 CFR part 171 in the future.

[140] For purposes of how the § 171.201 requirements and cross-references to § 164.524 operate within this example, it makes no difference whether the health care provider acting on the individualized determination is the licensed health care professional who made the determination

Continued

this circumstance, the finalized § 171.201(d)(1), which cross-references the harm standard applicable under § 165.524(a)(3)(iii), applies. In this example situation, the qualifying determination of risk of harm (§ 171.201(c)(1)) is that *any* access (or exchange, or use) of the EHI by the personal representative is reasonably likely to cause harm consistent with the standard established in § 164.524(a)(3)(iii), and thus the health care professional, or another HIPAA covered entity or business associate with knowledge of the determination, could also deny a request by the representative to access the individual's ePHI under § 164.524(a)(iii).

Under § 164.524(a)(iii), the harm must be a ''substantial harm'' to qualify for the denial of the patient's personal representative's request to access the patient's PHI. Similarly, both § 171.201 and § 164.524(a)(3) apply where an information blocking actor that is also a HIPAA covered entity, acting in reliance on a determination of risk of harm made by a licensed health care professional in the exercise of professional judgment, does not provide the patient or the patient's personal representative any access to information within the patient's EHI that references another person. In this type of circumstance, § 171.201(d)(2) by cross-reference to § 164.524(a)(3)(ii) applies the same ''substantial harm'' standard under § 171.201 that applies to the actor's denying the patient or their representative access to that information under § 164.524(a)(3)(ii).[141]

In § 171.201(d)(1), (2), and (3), as finalized, we also apply the harm standards described in § 164.524(a)(3)(i), (ii), or (iii) to particular types of circumstances where § 164.524 does not apply, but that are similar with respect to whether it is the patient or their representative requesting access, and whether the access requested is to information within the patient's EHI that is another person's identifiable information. For example, § 171.201(d)(3) applies the harm standard described in § 164.524(a)(3)(i) where practices that are likely to interfere with a patient's access, exchange, or use [142] of the patient's own EHI are implemented to substantially reduce a risk of harm arising from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (§ 171.201(c)(2)). Provided its conditions are met in full, the Preventing Harm Exception (§ 171.201) would apply to such practices as delaying access, exchange, or use, for the time necessary to correct the errors that would otherwise pose a risk of harm to the patient (or another person) that would be cognizable under § 164.524(a)(3)(i) if § 164.524(a)(3)(i) applied.[143] Such delays are not explicitly addressed under § 164.524(a)(3), which provides a maximum timeframe for disclosure of PHI to which patients have the right of access, and § 164.524(a)(3) does not expressly contemplate risks of harm arising from data issues as would be consistent with § 171.201(c)(2). By contrast, § 171.201 defines when a practice that is likely to, or does, interfere with the access, exchange, or use of EHI is excepted from the definition of information blocking in § 171.103 that applies to the actor engaged in the practice, and expressly applies where the actor can demonstrate a reasonable belief the practice will substantially reduce a risk of harm arising from data issues consistent with § 171.201(c)(2).

Because risks of harm arising from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (§ 171.201(c)(2)) would apply equally to an individual's or their representative's or their health care provider's access, exchange, or use of the patient's EHI, § 171.201(d)(4) applies the standard in § 164.524(a)(3)(i) to all of these circumstances. Thus, as § 164.524(a)(3)(i) stands at the time of publication of this final rule, the access, exchange, or use of the EHI affected by the practice must be reasonably likely to endanger the life or physical safety of the patient or another person were the practice not implemented. (Please see Table 3 for a crosswalk of the particular types of circumstances addressed by the subparagraphs under § 171.201(d) to the § 164.524 harm standard applicable to each type of circumstance.)

The finalized regulatory text in § 171.201 is revised from the Proposed Rule to reflect this more granular and comprehensive alignment of harm standards across the two regulatory provisions. We believe this alignment achieves the level of granular cross-reference necessary and that is preferable to selecting only one of these standards to apply in all types of circumstances under § 171.201. We further note that the revised regulation text is consistent with our decision to completely align the EHI definition with the definition of ePHI within the designated record set.[144]

Comments. A number of commenters advocated for expanding the definition of harm that is contemplated under this exception to encompass psychological and/or emotional harm in addition to risks to life or physical safety, including but not limited to expanding the concept of individualized determinations of risk of harm by health care professionals. A few commenters specifically advocated recognizing the potential for financial, reputational, or social/cultural harms. A number of other commenters expressed a concern that broadening the exception to address additional types of potential harm could risk its being overused to withhold information from patients where available evidence does not indicate there is a risk. One commenter reported having observed that some clinicians express a belief that mere disclosure of health data directly to patients without the clinician's professional interpretation will routinely cause harm, despite what the commenter described as existing evidence to the contrary.

Response. We believe it would be challenging to define an appropriate and unique standard for purposes of this exception for non-physical harms that all actors defined in § 171.102 could apply consistently and, most importantly, without unduly restricting patients' rights to access their health information. We also recognize, as discussed above, the practical utility of alignment with relevant Privacy Rule provisions. At this time, only danger to the individual's ''life or physical safety'' is recognized as grounds for denial of an individual's right of access under § 164.524(a)(3)(i). However, ''substantial harm'' is the standard applied under the Privacy Rule where the access denied is to information identifying another person (other than a health care provider) or where an individual's personal representative is denied access to the individual's PHI under § 164.524(a)(3)(ii) or (iii). To align with the relevant Privacy Rule provisions, the final regulation text (§ 171.201(d)(1) and

consistent with § 171.201(c)(1), another licensed health care professional, or another type of health care provider (such as a hospital or skilled nursing facility).

[141] Note that the ''individual'' and ''access'' have different meanings under 45 CFR 164.524 from those in 45 CFR part 171. Regarding an individual's right of access under 45 CFR 164.524, the term ''access'' should be understood in that HIPAA Privacy Rule context.

[142] As the terms ''access,'' ''exchange,'' and ''use'' are defined in § 171.102.

[143] Note, again, that ''access'' has a different meaning in subpart E of 45 CFR part 164 than it does in 45 CFR part 171.

[144] See section VIII.C.3 of this preamble and the finalized definition of ''electronic health information'' in § 171.102.

(2)) references the same harm standards as the Privacy Rule uses where § 164.524(a)(3)(ii) or (iii) as well as § 171.201 applies, and in circumstances where § 164.524(a)(3) is not implicated but the actor's practice is both based on an individualized determination of harm (consistent with § 171.201(c)(1)) and likely to interfere with: (§ 171.201(d)(2)) a patient's or their legal representative's access, exchange, or use of information within their EHI that identifies another person (other than a health care provider); or (§ 171.201(d)(1)) the patient's legal representative's access, exchange, or use of the patient's EHI. The finalized § 171.201(d)(3) and (4) also re-use the familiar § 164.524(a)(3)(i) type of harm for the wide variety of circumstances where § 171.201 applies but the type of risk is consistent with § 171.201(c)(2) or the (otherwise legally permissible) access, exchange, or use of EHI with which the practice is likely to interfere is by someone other than the patient or their legal representative. Thus, the finalized § 171.201 does not establish a standard for non-physical harm that would be unique to the Preventing Harm Exception but instead recognizes ''substantial harm'' in circumstances where § 164.524(a)(3)(ii) or (iii) apply, and also applies this familiar type of harm in situations where neither § 164.524(a)(3)(ii) nor (iii) applies but where re-use of this same standard under § 171.201 is consistent with the goal of aligning the types of harm recognized under Preventing Harm Exception with the grounds for denying a right of access request under the Privacy Rule.

Comments. One commenter specifically recommended allowing actors to rely on an individual's own subjective beliefs related to harm.

Response. We interpret this comment as pertaining to the beliefs of the patient whose EHI would be affected by a practice. We appreciate this opportunity to explain that practices implemented to honor and apply the patient's expressed preferences regarding access, exchange, or use of their EHI are addressed by the Privacy Exception finalized in § 171.202.

Comments. A number of commenters requested clarification of how the Preventing Harm Exception and its conditions might operate in situations involving minors where applicable State laws allow non-emancipated minors to independently consent to certain types of health care and provide for keeping records of such care confidential from the minor's parents/guardians. Several of these commenters specifically requested clarification about the operation of this exception where State law provides for minors to be able to consent to some or all types of health care but does not provide for or allow the minors to access their health records information at all, or in specific format(s).

Response. We appreciate commenters' offering us the opportunity to reiterate that where a particular access, exchange, or use of EHI is prohibited by applicable Federal, State, or tribal law, an exception to the definition of information blocking is not needed. Nothing in part 171 calls for access, exchange, use, or other disclosure of EHI that is prohibited by other applicable law. If an actor simply cannot effectively segment EHI they could safely and permissibly share from EHI they are not permitted to share in a given requested format, the actor should refer to the exception for requests that are infeasible (§ 171.204). However, if the EHI they could legally disclose could be shared in a different manner than that initially requested but the different manner would support segmentation, then an actor should provide the EHI they can safely and legally share in the most appropriate manner consistent with the Content and Manner Exception (§ 171.301).

Comments. Several commenters specifically requested clarification as to the information blocking implications where State law and/or the organization's account provisioning process do not provide for minors to obtain the login credentials needed to access their own records through an electronic portal, which will often be the login credentials a patient would use to authorize an app to receive the records through the provider's API.

Response. Where the actor does not have a reasonable belief that a practice interfering with minors' access to their own EHI will substantially reduce a risk of harm cognizable under this exception, the Preventing Harm Exception (§ 171.201) would not apply. This exception would also not apply where any person—whether adult, emancipated minor, or non-emancipated minor—is not able to provide adequate verification of their identity consistent with the actor's health information privacy or security protection policies. Actors should assess practices related to verifying the identity of a patient, or a legal representative of the patient, for consistency with the conditions of the Privacy Exception as finalized in § 171.202 and/or the Security Exception as finalized in § 171.203. Likewise, practices implemented to confirm a representative's legal authority to access or request or authorize access, exchange, or use of a minor's EHI on behalf of the minor, should be analyzed in the context of the Privacy Exception as finalized in § 171.202 and/or the Security Exception as finalized in § 171.203. Where otherwise applicable law prohibits a specific access, exchange, or use of information, an exception to part 171 is not necessary due to the exclusion of ''required by law'' practices from the statutory information blocking definition in section 3022 of the PHSA (as discussed in section VIII.C.1 of this preamble). However, where an actor simply lacks the technical capability to provide access, exchange, or use in a specific requested mechanism, format, or manner, we would encourage the actor to review its practices for consistency with the new Content and Manner Exception finalized in § 171.301 or the Infeasibility Exception finalized in § 171.204.

Comments. Several commenters requested clarification as to whether the Preventing Harm Exception would apply to 42 CFR part 2 data when it is not made available for access, exchange, or use because the patient did not consent to its access, exchange, or use.

Response. We appreciate the opportunity to remedy any confusion that may have been caused by the Proposed Rule's use of an illustrative example (84 FR 7524) within which the requirement to withhold data subject to 42 CFR part 2 regulations rendered a particular access, exchange, or use of only a portion of the patient's EHI legally permissible. In the example, only those portions of the patient's EHI to which 42 CFR part 2 does not apply could be permissibly accessed, exchanged, or used. This example was intended only to illustrate that the mere fact that an actor has knowledge, possession, custody, or control of more EHI than the actor could legally share would not, itself, provide a basis for application of the Preventing Harm Exception to the actor's withholding of any of the EHI that the actor could legally share. When an actor that is subject to 42 CFR part 2 cannot honor a request for access, exchange, or use of data subject to 42 CFR part 2 specifically because the patient has not provided the consent that would be required by 42 CFR part 2 before the actor could disclose that specific data for access, exchange, or use, the Preventing Harm Exception (§ 171.201) would not apply. When an actor has 42 CFR part 2 data for a patient but does not believe it has documented the patient consent that is legally required before the actor can fulfill a request for

access, exchange, or use of that data, the actor should refer instead to the Privacy Exception finalized in § 171.202. If the actor lacks the technical capability to effectively segment data that it can legally share from data that it cannot legally share, the actor should also consider the new Content and Manner Exception finalized in § 171.301 or the Infeasibility Exception finalized in § 171.204.

Comments. Several commenters noted that some State laws prohibit the release of specific information, such as results of particular diagnostic tests, to patients through electronic means (*e.g.,* patient portals or APIs) until particular protocols have been completed. Commenters cited, as an example, State law mandates for initial communication of particular information to the patient by a health professional in real time. The commenters requested clarification of whether or how § 171.201 would apply in those circumstances.

Response. As is the case with 42 CFR part 2 data that the patient has not consented to disclose, the exception finalized in § 171.201 would not apply in these particular types of circumstances. The information blocking definition proposed and finalized in § 171.103 does not include a practice that is likely to, or in fact does, interfere with the access, exchange, or use of EHI when the practice is required by law. If the actor lacks the technical capability to segment data at the level of granularity needed to withhold only those data points, elements, or classes that it is legally prohibited from disclosing in response to a particular request, the actor should consider the Content and Manner Exception finalized in § 171.301 or the Infeasibility Exception finalized in § 171.204.

Comments. Several commenters recommended that we recognize under § 171.201 practices requiring patients to obtain their laboratory results information only through the ordering provider's EHR. Commenters stated that inaccurate display of such results is a safety risk and that other actors such as laboratories and HINs/HIEs may not have the technical capability to display the information accurately in a human-readable interface that would be in full compliance with regulatory requirements otherwise applicable to human-readable displays of laboratory results information.

Response. We agree that display of inaccurate values for laboratory results, or other clinical observations, could represent a safety risk. We do not believe it would be appropriate to broadly limit patients to obtaining their laboratory information only from providers that are (or that employ) professionals whose scope of practice allows them to order the tests. If a laboratory, or a HIN/HIE, has the data in an interoperable format to support its exchange across providers, but does not have the technical capability to appropriately display it for human readability (such as in a patient portal), then the laboratory, or HIN/HIE, should make the data available in the interoperable format to providers or patients who can then view the data using technology the provider or patient has chosen as appropriate to their needs. If any actor receives a request for data access, exchange, or use via a specific mechanism that the actor does not have the technical capability to support, the actor should consider the Content and Manner Exception finalized in § 171.301 or the Infeasibility Exception finalized in § 171.204.

Comments. One commenter suggested recognizing a new exception under the Preventing Harm Exception that would allow a health care provider who is also a research institution to require, as a condition of making EHI available for use in research, that the health care provider be a collaborator in that research. The commenter stated that institutions ensure accuracy in the way data is used and analyzed by requiring they participate in any research involving their patients' information so that they can explain for the research team any anomalies or other characteristics unique to their own institutions' data and collection methods. This commenter stated that disclosing EHI for research purposes when the research being conducted does not involve the health care provider disclosing the EHI could lead to misinterpreted outcomes based on flawed data that could have a negative impact on scientific discovery.

Response. We considered this suggested expansion of the Preventing Harm Exception specifically in the context of the definition of ''electronic health information'' that we proposed, and the more focused definition of ''electronic health information'' that we have finalized.[145] The Preventing Harm Exception is intended to apply to practices an actor reasonably believes will substantially reduce a risk of harm (of a type cognizable under this exception) to particular person(s), such as a patient or a natural person in the patient's life or multiple patients whose EHI was corrupted or mismatched due to a technical failure of an actor's systems. The risk of potential harm described by the comment was specifically of misinterpretations of EHI leading to research findings that negatively impact scientific discovery. This risk is too far removed from a reasonable, and reasonably foreseeable, likelihood of cognizable harm to particular patients or other particular natural persons to fit within the intent of the Preventing Harm Exception finalized in § 171.201. Therefore, we did not modify the exception in response to this comment.

Finalized Belief and Harm Conditions for § 171.201

Having considered comments received on the belief and harm standards, we have finalized the exception at § 171.201 with modification, as discussed in responses to comments. These modifications simplify the belief standard, and more thoroughly and specifically align the harm standard applicable for this exception with either the Privacy Rule harm standard applicable under § 164.524(a)(3)(i) (in most circumstances) or the harm standard in § 164.524(a)(3)(ii) or (iii) (in particular circumstances). The harm standard in § 164.524(a)(3)(ii) or (iii) applies where both §§ 171.201 and 164.524(a)(3)(ii) or (iii) would apply, or in particular circumstances that are sufficiently similar as to be analogous to circumstances where both §§ 171.201 and 164.524(a)(3)(ii) or (iii) would apply.[146] Please reference the finalized § 171.201(a) for the regulatory text of the belief standard. Please reference the finalized §§ 171.201(d)(1)–(3) for regulatory text that establishes the specific § 164.524(a)(3) harm standard that applies in each of the three particular types of circumstances specific to patients and their representatives' access to the patient's EHI, and reference § 171.201(d)(4) for regulatory text establishing the specific § 164.524(a)(3) harm standard applicable in all other types of circumstances where § 171.201 applies.

The circumstances where both §§ 171.201 and 164.524(a)(3) would apply are where the practices do

[145] We note that, although various types of research data and data sets may be or include ''electronic health information'' as defined in § 171.102, not all research data or data sets are or include data meeting this definition.

[146] Please note that the Preventing Harm Exception will not normally apply where a patient or their representative may seek access to EHI that is excluded from the right of access under § 164.524(a)(1) or to which access may be denied on unreviewable grounds under § 164.524(a)(2). In circumstances where § 171.201 conditions are not met but an actor wishes to withhold EHI from an individual's right of access under § 164.524(a)(1) or (2), the actor should refer to the privacy exception (§ 171.202).

interfere with access, exchange, or use by the patient or their legal representative (who is their personal representative for purposes of § 164.524) of some or all of the patient's EHI to the point of denying access (as used in context of § 164.524) on grounds of a risk of harm determined on an individualized basis by a licensed health care professional in the exercise of professional judgment (§ 171.201(c)(1) as finalized). Circumstances where § 164.524(a)(3) is not implicated but that are analogous to circumstances where both §§ 164.524(a)(3) and 171.201 apply are those where the risk of harm is determined on an individualized basis consistent with finalized § 171.201(c)(1) and the practice does not entirely deny but is likely to, or does, interfere with the patient's or their legal representative's access, exchange, or use of the EHI that is otherwise legally permissible. (For example, the practice may result in delaying access, exchange, or use of the EHI but for less time than is permitted for granting of a right of access request under § 164.524.)

In a wide variety of circumstances where § 171.201 will apply, § 164.524 would not apply. Such circumstances include those where the access, exchange, or use of EHI with which the practice is likely to, or does, interfere is not related to right of access under the HIPAA Privacy Rule, such as access, exchange, or use of the patient's EHI by the patient's health care providers. Likewise, § 171.201 will apply but § 164.524(a)(3) will not apply when the risk of harm arises from data issues (§ 171.201(c)(2)) rather than having been determined on an individualized basis by a licensed health care professional (§ 171.201(c)(1)). In these circumstances where § 164.524 would not apply, and that are not analogous to circumstances where § 164.524(a)(3) would apply, § 171.201(d)(4) (type of harm condition) applies the harm standard that would be cognizable under § 164.524(a)(3)(i) so that the actor must reasonably believe the practice will reduce a risk otherwise posed to the life or physical safety of the patient or another natural person.[147] This provides, under § 171.201, consistency across this wide array of circumstances where § 164.524(a)(3) would not be implicated regardless of the extent of interference or length of delay the practice may pose to the access, exchange, or use of the EHI. Because the circumstances to which the finalized § 171.201(d)(4) applies include access, exchange, or use of the patient's EHI by health care providers furnishing services to the patient, we believe it is most appropriate to apply under § 171.201(d)(4) the same standard of harm that would apply to denying a patient access to the patient's EHI. This is consistent with our proposal (84 FR 7602) to require that practices likely to interfere with any access, use, or exchange of EHI would need to reduce a risk to the ''life or physical safety'' of a patient or another person to satisfy the conditions in § 171.201 and be excepted from the definition of information blocking in § 171.103. We have also clarified the regulation text so it is expressly clear on its face that the risk to be reduced must be one that would otherwise arise from the specific access, use, or exchange of EHI affected by the practice.

Under § 164.524(a)(3)(i), a covered entity may deny an individual access to protected health information (PHI) about that individual in a designated record set only if a licensed health care professional in the exercise of professional judgment determines that releasing the information to them would endanger the life or physical safety of the individual or another person. Under § 171.201(d)(3), an actor[148] may implement a practice that is likely to, or does, interfere with the patient's access, exchange, or use of their own EHI when the actor reasonably believes the practice will substantially reduce a risk of harm to life or physical safety of the patient or another person, regardless of whether that risk is determined on an individualized basis (§ 171.201(c)(1)) or arises from data that is known or reasonably suspected to be corrupt due to technical failure, erroneous for another reason, or misidentified or mismatched (§ 171.201(c)(2)).

Under § 164.524(a)(3)(ii) and (iii), the standard of ''substantial harm'' applies where the individual or their representative are denied access to information in the individual's record that identifies another person (other than a health care provider), or an individual's personal representative is denied access to the individual's information. Thus, the type of harm standard applicable under § 171.201 will in most cases require that the actor's practice be based on a reasonable belief that the requested access, exchange, or use with which the practice is likely to or does interfere would otherwise endanger the ''life or physical safety'' of the patient or another person. However, the ''substantial harm'' standard included in § 164.524(a)(3)(ii) and (iii) would apply in specific circumstances as shown in Table 3. As discussed above, we have made this change to the finalized § 171.201 to align the harm standard applied by § 171.201 with the one applied by § 164.524(a)(3) where both would apply, and in analogous circumstances (as described above). As explained above, we revised the harm standard applicable in particular circumstances to avoid setting a higher threshold under § 171.201 for practices likely to interfere with access, exchange, or use[149] of EHI than would be applicable to entirely denying access under § 164.524(a)(ii) or (iii)[150] in the same circumstances. In the finalized § 171.201(d), we have applied the type of harm described in § 164.524(a)(ii) and (iii) to particular circumstances where § 164.524(a)(ii) and (iii) do not apply, but that are analogous to such circumstances, for the reasons stated in responses to comments above.

[147] Please note that although ''individual'' as defined in 45 CFR 169.103 is not limited to natural persons, the belief standard in the finalized § 171.201 is, consistent with the requirement that in most circumstances the risk of harm at issue must be to life or physical safety.

[148] An actor could be any individual or entity meeting the definition of ''health care provider,'' ''health IT developer of certified health IT'' or ''health information network or health information exchange'' in § 171.102, and may or may not also be a HIPAA covered entity or business associate as defined in the HIPAA Rules.

[149] As ''access,'' ''exchange,'' and ''use'' are defined in § 171.102.

[150] Please note that ''access'' has a different meaning under 45 CFR 164.524 than in 45 CFR part 171. Regarding an individual's right of access under 45 CFR 164.524, the term ''access'' should be understood in that HIPAA Privacy Rule context.

TABLE 3—MAPPING OF CIRCUMSTANCES UNDER § 171.201(D) TO APPLICABLE HARM STANDARDS

Requirements under § 171.201(d) type of harm condition	Applicable harm standards [151]
§ 171.201(d)(1)—where the practice interferes with access, exchange, or use of the patient's EHI by their legal representative and the practice is implemented pursuant to an individualized determination of risk of harm made by a licensed health care professional in the exercise of professional judgment (§ 171.201(c)(1)).	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(iii), which is substantial harm to the individual or another person.[152]
§ 171.201(d)(2)—where the practice interferes with the patient's or their legal representative's access to, use or exchange of information that references another natural person and the practice is implemented pursuant to an individualized determination of risk of harm made by a licensed health care professional in the exercise of professional judgment (§ 171.201(c)(1)).	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(ii), which is substantial harm to such other person.
§ 171.201(d)(3)—where the practice interferes with the patient's access, exchange, or use of their own EHI, regardless of whether the risk the practice is implemented to substantially reduce is determined on an individualized basis by a licensed health care professional in the exercise of professional judgment (§ 171.201(c)(1)) or arises from data that is known or reasonably suspected to be corrupt due to technical failure, erroneous for another reason, or misidentified or mismatched (§ 171.201(c)(2)).	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(i), which is a harm to the life or physical safety of the individual or another person.
§ 171.201(d)(4)—where the practice interferes with the patient's legal representative's otherwise legally permissible access, exchange, or use of the patient's EHI and the practice is implemented to reduce a risk arising from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (§ 171.201(c)(2)).	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(i), which is a harm to life or physical safety of the individual or another person.

Types of Risk of Harm to Patients Cognizable Under This Exception

We proposed (84 FR 7524) that to qualify for this exception, an actor's practice must respond to one or more type(s) of risk of harm cognizable under this exception. The three types of risk of harm that we proposed would satisfy the conditions of this exception are:

- Risks arising from corrupt or inaccurate data being recorded or incorporated in a patient's EHI;
- risks arising from misidentification of a patient or patient's EHI; and
- risks identified by a determination made by a licensed health care professional that a specific access or disclosure of EHI is reasonably likely to endanger the life or physical safety of the patient or another person.

We provided additional explanation and discussion of these types of risk of harm in the preamble of the proposed rule (84 FR 7524 and 7425). We also requested comment (84 FR 7525) on:

- Whether these categories of harm capture the full range of safety risks that might arise directly from accessing, exchanging, or using EHI; and
- Whether we should consider other types of patient safety risks related to data quality and integrity concerns or that may have a less proximate connection to EHI but that could provide a reasonable and necessary basis for an actor to restrict or otherwise impede access, exchange, or use of EHI in appropriate circumstances.

We will first discuss those comments that pertain to the cognizable types of risk of harm in general. Comments specific to each of the three types of risk of harm will be discussed separately, in the order they were presented in the Proposed Rule.

Comments. Overall, comments were supportive of the exception recognizing risks of harm arising from corrupt or misidentified information, and individualized determinations of risk of harm made by licensed health care professionals in the exercise of professional judgment. Numerous commenters requested clarification or additional information to help actors more effectively understand and efficiently document their risk determinations in connection to practices for which they would seek to claim that the Preventing Harm Exception applies.

Response. We appreciate the feedback received. In response to comments calling broadly for additional clarification or information, we have provided detailed responses to comments received. Where useful to enrich the discussion, some responses discuss hypothetical example situations that illustrate how a particular aspect of the exception would operate in such a situation.

Comments. Some comments suggested that the determinations and the rationale for individualized determinations by health care professionals in the exercise of professional judgment should be documented in the electronic health record.

Response. We believe documentation in the EHR, such as in appropriate notes field(s), may be a practical, efficient approach to documentation of determinations of risk of harm consistent with § 171.201 for some — perhaps many — licensed health care professionals. Therefore, we confirm that EHRs are considered an appropriate approach or method for the documenting, and for retaining documentation, of determinations of risk consistent with § 171.201(c)(1). We also note that much (perhaps all) of the information about the patient's individual circumstances that factors into the professional's determination of risk will most naturally and most often be documented in the EHR in the ordinary course of furnishing care to the patient. Nothing in § 171.201 would require duplicating information already captured in the EHR in a different form

[151] Note that the ''individual'' and ''access'' have different meanings under 45 CFR 164.524 from those in 45 CFR part 171. Regarding an individual's right of access under 45 CFR 164.524, the term ''access'' should be understood in that HIPAA Privacy Rule context.

[152] Note that grounds for denial of an individual's right of access include that the access is reasonably likely to cause the harm identified in the particular subparagraph under § 164.524(a)(3). For purposes of 45 CFR part 171, we interpret that the stated type of harm must, to the best of the actor's knowledge and belief, be substantial, in absence of particular practice(s), in order for an actor to reasonably believe the practice(s) will substantially reduce that risk. We would interpret a reasonable likelihood of the described harm, as used under § 164.524(a)(3) to be a substantial risk for purposes of § 171.201.

or format specific or unique to § 171.201, whether in the EHR or elsewhere. However, we also believe that there is substantial potential for variability in health care professionals' current methods for documenting risk factors and determinations.

In addition, we do not believe it is necessary to require different or duplicate documentation of information that is already otherwise captured in reliable business records consistent with the HIPAA Privacy Rule and applicable State laws—including, but not limited to, laws protecting patient privacy or mandating provider reporting of particular types of abuse their patients may experience. Therefore, requiring via regulation that all health care professionals document their determination specifically in the EHR in order to satisfy this exception's conditions could impose an unnecessary burden on those who would like to conform their practices to this exception but currently take a different approach to documenting risk factors or to documenting individualized determinations of risk specific to access, exchange, or use of the patient's EHI by the patient or their legal representative(s). Thus, we have not finalized a requirement that licensed health care professionals must document in their EHR or in any other particular system(s) their individualized determinations of risk of harm in order for the determinations of risk to satisfy the risk of harm condition finalized in 171.201(c)(1).

Comments. One commenter noted that minors may not fully understand the implications of downloading and sharing their EHI, which represents a different type of risk than the three discussed in the Proposed Rule. The commenter advocated for health care providers to have discretion to impose restrictions on non-emancipated minors' ability to access their EHI through an API.

Response. We did not modify the Preventing Harm Exception in response to this comment. The Preventing Harm Exception (§ 171.201) is intended to apply to practices an actor reasonably believes will substantially reduce a risk of harm to one or more particular person(s), and in many circumstances (§ 171.201(d)(3) or (4)) a risk of harm to the life or physical safety of particular persons, such as: A patient or person in the patient's life; or multiple patients whose EHI was corrupted or mismatched due to a technical failure of an actor's systems. Where a non-emancipated minor, or other patient, is otherwise legally entitled to access or receive their own health information that does not include identified information about another person, the Preventing Harm Exception will apply only to those practices reasonable and necessary to address risk to the life or physical safety of another person consistent with § 171.201(d)(3) and its specific cross-reference to § 164.524(a)(3)(i). The Privacy Exception (§ 171.202) is intended to recognize reasonable and necessary practices to protect patients' privacy. We also note that we have clarified in this final rule that although practices that purport to educate patients about the privacy and security practices of applications and parties with which a patient chooses to share their EHI would always be subject to review by OIG if there were a claim of information blocking, such practices likely would not be considered to interfere with the access, exchange, and use of EHI if they meet certain criteria (see section VIII.C.6, above).

Risk of Corrupt or Inaccurate Data Being Recorded or Incorporated in a Patient's Electronic Health Record

We proposed (84 FR 7524) that the Preventing Harm Exception could apply to practices that address risks of harm arising from corrupted or inaccurate EHI being recorded or incorporated in a patient's electronic health record. We further proposed that recognized risks from incorrect or inaccurate information would be limited to those arising from known or reasonably suspected corruption and inaccuracies caused by performance and technical issues affecting health IT. We clarified that the Preventing Harm Exception would not extend to purported accuracy issues arising from the incompleteness of a patient's electronic health record generally. We acknowledged that Federal and State laws may require an actor to obtain an individual's written consent before sharing specific health information, such as information subject to 42 CFR part 2. However, we expressly noted in the Proposed Rule that this exception would not apply to an actor's conduct in refusing to provide access, exchange, or use of the remainder of the patient's record on the basis that the information withheld per patient's non-consent would render the remainder of the patient's record incomplete and thus inaccurate. We also noted that known inaccuracies in some data within a record may not be sufficient justification to withhold the entire record so long as the remainder of the patient's EHI could be effectively shared without also presenting the known incorrect or corrupted information as if it were trustworthy.

Comments. Commenters were supportive of the Preventing Harm Exception applying to appropriate practices to address corrupt or incorrect data in EHI and the risks that would otherwise arise from propagation of corrupt or otherwise incorrect EHI within a patient's record.

Response. We appreciate all of the feedback received, including but not limited to confirmation that responding stakeholders are supportive of this exception applying to practices an actor reasonably believes will substantially reduce a risk of harm otherwise arising from access, exchange, or use of corrupt or inaccurate data within a patient's record.

Comments. One commenter, acknowledging that patients' wishes that specific information not be shared should be honored, advocated expanding this exception to cover physicians' declining to disclose any EHI to other physicians where withholding of some information at the patient's request would, in the disclosing physician's view, render the patient's record so distorted as to be misleading.

Response. As we explained in the Proposed Rule, we would not recognize incompleteness of the EHI that an actor can disclose as a source of a risk of harm cognizable under this exception. For instance, patients may make requests that specific information not be accessed, exchanged, or used beyond a specific clinician-patient (or other relevant) relationship because the information is associated with a stigmatized condition, or for personal reasons (such as the patient's subjective perception the information may be embarrassing or otherwise detrimental to them). In the Proposed Rule, we provided an illustrative example of a patient declining consent to share 42 CFR part 2 substance abuse treatment information, and stated we would not consider the remainder of the patient's record inaccurate based on its incompleteness (84 FR 7524). Health care providers receiving any patient's records of prior care presumably have an awareness of the potential that some information may be omitted from the information they receive for a wide variety of reasons that include, but that are not limited to, patients' intentional choices to withhold some information. Therefore, we do not believe it would be appropriate to consider EHI to be corrupt, inaccurate, or otherwise erroneous where it is simply a subset of everything an actor knows about the patient.

We are not persuaded that a patient's withholding consent to share specific

portions of their overall EHI, regardless of the patient's rationale for withholding consent, would render the data set their physician (or other health care provider) could share more dangerous to the patient than sharing none of the patient's EHI with another of the patient's providers. Instead, we remind health care providers that nothing in part 171 overrides Federal, State, or tribal law protections of patients' privacy preferences. Likewise, nothing in part 171 reduces variation in what and how much information patients remember, or are willing, to disclose to their health care providers. Patients remain free to withhold various information from their health care providers, including but not limited to what other providers they may have seen in the past.

Before enactment of the Cures Act, health care providers could not safely assume every patient record they received from any source necessarily included all the information that could or should be known by that source that would be relevant to the patient's health or care by that provider, even where the source can permissibly share everything they do know. Thus, we reiterate that we do not believe it is reasonable or necessary for purposes of preventing harm that a provider withhold the EHI that they could permissibly share in any particular circumstance simply because they happen to have more EHI than they can permissibly share.

However, we also highlight that for purposes of this exception a data export or access mechanism appropriately showing that some data may be unavailable or omitted from the export or presentation is materially different from a data export or presentation that misrepresents the patient's EHI. For example, exports or presentations omitting all medication data and correctly stating ''medication data not available,'' [153] we would not consider corrupt, inaccurate, or otherwise erroneous. By contrast, however, an export or presentation stating ''no current medications,'' or stating ''none'' or ''none known'' in the medication section, when in fact the system producing the export or representation does include current known medications for the patient, represents a type of risk recognized under § 171.201(c)(2).

Under § 171.201(d)(4), as finalized, a practice that is likely to, or that in fact does, interfere with otherwise permissible access, exchange, or use of a patient's EHI by their health care providers must be one the actor implementing the practice reasonably believes will substantially reduce a risk of harm of a type that could serve as grounds for denial of the individual's right of access to their EHI under the 45 CFR 164.524(a)(3)(i). Therefore, in order for a practice likely to interfere with the access, exchange, or use of EHI by one of the patient's health care providers to satisfy the conditions of the Preventing Harm Exception, the actor must hold a reasonable belief that the practice will substantially reduce a risk to the patient's, or another natural person's, life or physical safety that would otherwise arise from the access, exchange, or use of the EHI with which the practice interferes. Erroneous misrepresentations that a patient is not known to be taking any medications, when in fact they are known to be taking one or more medications, is typically a system problem and one that can give rise to risk to the physical safety, or even the life, of any or all patients whose EHI may be affected by the problem.

Comments. One comment submission highlighted a tension between the data-provision preferences of health care providers requesting data and other actors (such as other providers and their health IT developers) from whom data is requested. This commenter indicated providers requesting data, such as long-term/post-acute providers caring for patients after a hospital stay, may currently have to wait days to receive any of the patient's clinical data from the hospital stay because the hospital or its health IT developer refuses to generate and send the C–CDA document until every last data element is finalized. The commenter suggested we clarify whether § 171.201 would apply to such circumstances.

Response. An actor's practice of delaying fulfillment of an otherwise feasible and legally permissible request for exchange, access, or use of EHI that is finalized and available to the actor merely because the actor knows more EHI for that patient will become available at some later date would not satisfy the conditions of § 171.201. As we stated in the Proposed Rule, we do not view mere *incompleteness* of a patient record as rendering the remainder of the patient's record inaccurate (84 FR 7524). We recognize that specific data points may not be appropriate to disclose or exchange until they are finalized. Such data points would include, but are not necessarily limited to: Laboratory results pending confirmation or otherwise not yet considered by the hospital reliable for purposes of clinical decision making; or notes that the clinician has begun to draft but cannot finalize until they receive (confirmed) laboratory or pathology results or other information needed to complete their decision making. We hope it is, and will be increasingly, rare that an actor cannot effectively sequester non-finalized EHI from finalized EHI. However, we cannot rule out the possibility that some actors may face that problem at some point. If an actor cannot effectively sequester non-finalized EHI from a particular access, exchange, or use where inclusion of non-finalized EHI would not be appropriate, the actor should refer to the new Content and Manner Exception (finalized in § 171.301) or the Infeasibility Exception finalized in § 171.204.

Comments. A number of commenters expressed concerns that many actors' health IT systems currently lack the capability to segment data by class and element that would be needed to withhold only those classes or elements that were corrupted or erroneous as described in the Proposed Rule. Commenters requested clarification on whether the § 171.201 Preventing Harm Exception would in these cases apply to the entirety of the patient's EHI, how it would apply, or if another exception would also be needed.

Response. In the circumstances these comments described, the Preventing Harm Exception will apply only to the EHI known or reasonably suspected to be corrupt or erroneous. If an actor lacks the data segmentation capabilities that would be needed to sequester only that data known or reasonably suspected to be corrupt or erroneous from the requested access, exchange, or use, we would encourage the actor to consider meeting the conditions of another exception with respect to the remaining EHI. For example, the Content and Manner Exception (§ 171.301) may allow for the actor to provide the requestor with the EHI not known or reasonably suspected to be corrupt or erroneous, albeit in a different way than was initially requested. Or, if the actor lacks the technical capability to share the EHI that is not known or reasonably suspected to be corrupt or erroneous consistent with the Content and Manner Exception (§ 171.301), then the actor may wish to meet the Infeasibility Exception (§ 171.204). The applicability of the exceptions will depend on the particularized circumstances, including but not limited to the specific request made. We believe the conditions of these exceptions also offer frameworks within which a responding actor and an

[153] Or otherwise indicating, in a manner appropriate to the circumstances, that absence of information in the extract or representation should not be understood as a statement that there is no such data in the source system.

EHI requester may be able to identify a mutually agreeable approach to making trustworthy EHI appropriately available in at least some of the instances where a request cannot be safely fulfilled in exactly the manner of the requester's first preference.

Comments. One comment expressed a concern that some health care providers, particularly those already receiving feedback from payers about their data quality, might believe the Preventing Harm Exception would allow them to withhold patients' access to the patients' own EHI to prevent the patients from seeing data quality issues the provider knows or believes are present in that EHI.

Response. If a provider knows that the data quality issues in their records serve as a source of risk consistent with § 171.201(c)(2), so as to form the basis of a reasonable belief the patient's accessing or using the data would place the patient at risk of harm cognizable under this exception,[154] the exception would apply if all other conditions of the exception were met. However, known corruption or other errors that would place a patient accessing their EHI at risk of harm cognizable under this exception on the basis of accessing—and presumably making health or care decisions based on—that EHI would also raise a substantial concern regarding the safety of that EHI for use by the provider. Thus, we would expect that whenever a given health care provider believes the EHI within their records is safe enough for their own use in the delivery of patient care, the Preventing Harm Exception would not excuse the provider from honoring their patients' requests to access, exchange, or use that EHI simply because the patients might discover error(s) in that EHI. If, to the actor's knowledge or reasonable belief, only some data classes or elements within a patient's EHI are a source of risk consistent with § 171.201(c)(2), the actor should continue to make the remaining data classes and elements available to the patients and other requestors (as appropriate under applicable law). Where the actor lacks the technical ability to appropriately sequester only the corrupt or erroneous data within the EHI they hold for given patient(s), the actor should reference the Content and Manner Exception finalized in § 171.301 or the Infeasibility Exception finalized in 171.204.

Comments. Several commenters requested clarification on whether an actor has a responsibility to assess the data in their possession, custody, or control for risk of harm before making it available for access, exchange, or use.

Response. The conditions finalized in § 171.201 for practices that interfere with the access, exchange, and use of EHI for purposes of preventing harm to be excepted from the definition of information blocking (§ 171.103) do not require that actors generally evaluate data requested for data quality issues or other sources of risk of harm before fulfilling requests for access, exchange, or use of the EHI. At the same time, actors should be aware that where an actor may have an affirmative duty under otherwise applicable law for the quality or accuracy of data, or for assessing other types of risk of harm that could be implicated by an EHI access, exchange, or use request, nothing in § 171.201 should be construed as lessening or otherwise changing that duty. For example, the Preventing Harm Exception does not lessen or otherwise change an actor's existing obligations to ensure patient EHI is created, recorded, and maintained to standards of accuracy and reliability consistent with laws, regulations, and accreditation requirements applicable to the particular actor in any given circumstance.

Comments. Commenters expressed appreciation for the inclusion of this exception so that health care providers will not be forced to share incorrect data. Several of these commenters requested we clarify a provider's responsibility for correcting corrupt or incorrect information once it is discovered.

Response. For health care providers, existing State and Federal laws and regulations address the responsibility to maintain appropriate records of health care furnished and in support of reimbursement sought from various programs and payers. Health care providers that have obtained voluntary accreditations may have made additional commitments related to record-keeping and data quality in context of obtaining and maintaining those accreditations. These existing responsibilities of health care providers are not lessened or otherwise changed by the Preventing Harm Exception. The exception simply provides for exception from the definition of information blocking at § 171.103 of practices interfering with the access, exchange, or use of mismatched, corrupt due to technical failure, or otherwise erroneous EHI in order to substantially reduce a risk of harm. Presuming its conditions are otherwise met, § 171.201 would apply to a variety of practices appropriate to correct mismatched, corrupt due to technical failure, or otherwise erroneous EHI in a manner consistent with otherwise applicable law, regulations, accreditation standards, and payment program standards.

Comments. One comment requested clarity regarding the applicability of this exception to data received from a third party, where the actual accuracy of the data cannot be, or has not been, confirmed by the actor asked to make that data available for access, exchange, or use.

Response. We recognize that in some circumstances the available and feasible mechanisms for EHI access, exchange, or use may not support as much data provenance information as an actor might prefer. In such circumstances, the actor would be free to communicate supplemental information about specific data's provenance to a requestor. However, the conditions of the Preventing Harm Exception would not be met where EHI requested was received from a third party and the actor could not confirm the accuracy of the EHI.

Comments. A comment from the perspective of health IT developers and implementers stated that this exception should allow an actor to err on the side of caution as the actor looks to determine the extent of potential distortions in a record before sharing it. A number of commenters described practices used today by HIEs to assess and resolve data quality issues, including but not limited to taking all of the records from a particular source offline while assessing the extent or cause of issues identified in some record(s) from that source.

Response. The Preventing Harm Exception is intended to apply to a variety of practices reasonable and necessary to protect patients from risk of harm arising from access, exchange, or use of data that is known or reasonably suspected to be corrupt, inaccurate, mismatched, or misidentified. To be covered by the exception, the practice may interfere with the access, exchange, or use of EHI only to the minimum extent necessary to substantially reduce a risk of harm cognizable under the exception, but the exception does not require that every record affected by the practice have first been confirmed to contain corrupt, mismatched, or otherwise dangerously problematic data. In some circumstances, such as a particular data source experiencing a

[154] Note that where the practice interferes with a patient's access to their own EHI, the applicable harm standard is established in § 171.201(d)(3) and is the same one established at § 164.524(a)(3)(i). Currently, that would be harm to life or physical safety.

known or reasonably suspected system or other technical failure producing widespread corruption, mismatching, or other dangerous errors, the minimum reasonable and necessary precautions may make all records from that source unavailable pending resolution of the technical failure and its risk-producing effects. The actor's knowledge or reasonable suspicion could be appropriately derived in various ways. These ways would include, but are not limited to: Detection of specific data quality issues in a sampling of records from the particular source; or receipt of notice from a source that they had experienced technical issues or failures resulting in corruption, mismatching, or other data quality issues giving rise to risks of harm cognizable under this exception.

Comments. A commenter noted that this exception should be applied rarely, and when applied should not be a mechanism to selectively block information from specific actors. However, several other commenters made observations that, in current practice, EHI coming from sources whose data has a pattern of higher-than-normal error rates may be subjected to more extensive review, and potentially delayed in broader availability, compared with EHI from sources whose data error rate is within a more normal range. Comments describing such current practices recommended that this exception should allow for continued application of additional data quality assurance processing to EHI from sources whose data exhibits a history or pattern of more numerous or more risky data quality issues.

Response. If an actor were to engage in practices systematically interfering with access, exchange, or use of EHI from a particular source based on considerations extraneous to the prevalence and risk profile of data quality issues in the EHI, such practices would not meet the conditions to be excepted under § 171.201 from the definition of information blocking finalized in § 171.103. Examples of considerations we would consider to be extraneous in this context notably include, but are not limited to, whether the data source was competitor of the actor and whether the actor may harbor personal animus toward the data source. However, this exception would apply to practices not based in whole or any part on considerations extraneous to the prevalence and risk profile of data quality issues in the EHI, provided each such practice meets all conditions in § 171.201 that are applicable to the circumstances in which it is used.

Comments. Commenters noted that integration of data from various types of sources is challenging because of differences in the data elements that different types of sources can exchange, and because of technical differences in how similar data elements may be structured, defined, or encoded across different types of sources. Commenters also stated that data from new exchange partners may raise questions about potential accuracy issues in interpreting and integrating different types of data as well as integrating similar data from various types of sources. Commenters recommended that § 171.201 recognize that practices may delay integration and availability of EHI in order to address these issues, and also recommended that a time limit be established for completing evaluations of incoming data.

Response. We appreciate commenters' highlighting that the U.S. health care system as a whole includes opportunities for access, exchange, and use of a wider variety of data classes and elements than are currently addressed by standards and implementation specifications adopted in part 170, and more sources than just those actors currently using certified health IT. We are aware that, in a variety of circumstances, safely and appropriately integrating data from a new source may require time to determine and apply appropriate processing approaches to ensure that data are not corrupted in the process of mapping or converting them to the structures and standards used by the recipient. Our finalized exception will apply to appropriately tailored practices for assessing and mitigating risks otherwise posed by integration of data from new sources, that is not standardized, or that is standardized to non-published, proprietary, or obsolete standards. In cases where the original meaning of EHI received cannot be determined in a manner allowing for conversion to the formats and standards used by the recipient's systems, it may sometimes be necessary to decline to integrate such data in the recipient's production systems. However, we believe it would be premature to establish via this rulemaking specific time limits for assessment and processing of EHI received from new exchange partners, in large part due to the considerable variability in systems and circumstances of the actors involved in such exchange relationships. Should the need arise to assess the reasonableness, necessity, and timeliness of an actor's practices applied to data received from new or various types of sources, we would do so in context of the specific circumstances in which particular practices were applied by particular actor(s).

Finalized Policy for Risks of Harm Arising From Corrupt or Inaccurate Data

We have finalized the type of risk condition with modifications to the proposed regulation text. We have reorganized the regulation text, and in the context of that reorganization rephrased the statement of some conditions. We have also, in § 171.201(c)(2) replaced the word ''inaccurate'' (used in proposed § 171.201(a)(2)) with ''erroneous'' to better differentiate between normal shortfalls in the complete accuracy of a record and risk-generating errors in the data. We also combine all data-specific sources of risk of harm in the final § 171.201(c)(2) instead of splitting them across two paragraphs as was the case in § 171.201(a)(1) (''corrupt or inaccurate'' in the Proposed Rule) and § 171.201(a)(2) (''misidentified or mismatched'' in the Proposed Rule). We made this change because misidentified, mismatched, corrupt, and otherwise erroneous data are all sources of risk arising from issues with the data rather than characteristics unique to a patient or their circumstances. Additional conditions must be met for § 171.201 to apply to practices implemented to substantially reduce a risk of harm arising from data issues (consistent with § 171.201(c)(2)), including § 171.201(a), (b), (d)(3) or (4), and (f)(1) or (2). Whether (d)(3) or (d)(4) applies turns on whether the practice is likely to, or does, interfere with a patient's own or other legally permissible access, exchange, or use of the patient's EHI. Whether (f)(1) or (f)(2) applies turns on whether the actor implements the practice consistent with an organizational policy (f)(1) or based on a determination based on the particularized facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use (f)(2).

For purposes of providing additional information and explanation as requested by many commenters, we reiterate that a risk of harm arising from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (§ 171.201(c)(2) as finalized) will not, consistent with discussion and illustrative examples in the preamble to the Proposed Rule (84 FR 7524), satisfy the conditions of the Preventing Harm

Exception if it turns on mere speculation about, or possibilities of, as-yet-undetected inaccuracies or other imperfections in the EHI. An electronic health record, like the paper chart it replaces, is inevitably less than perfectly complete and precisely accurate across 100 percent of the variables potentially relevant to the individual's health. Because the risk that records in general may be imperfect is a risk that we understand as inherent to (and thus ordinarily addressed in the course of) clinical practice, it will not be recognized as justifying practices that implicate the information blocking definition. Thus, the Preventing Harm Exception finalized in § 171.201 does not extend to purported accuracy issues arising from potential, suspected, or known incompleteness of a patient's electronic health record generally, such as the possibility of a patient choosing, or not remembering, to mention some of the medications they regularly take. Similarly, the possibility that any given patient's EHI could at any time contain sporadic, undetected, inaccurate data points as a result of data entry errors—such as an entered weight of 123 instead of the accurate observation of 132—would not be interpreted as satisfying the condition finalized in § 171.201(c)(2).

The Preventing Harm Exception will apply in those instances where specific EHI of one or more patients is affected by a risk consistent with the finalized § 171.201(c)(2). Assuming its other conditions that are applicable to the specific circumstances are met, the Preventing Harm Exception will apply to appropriately tailored practices that affect a particular patient's EHI regardless of the origin or cause of known or reasonably suspected data issues giving rise to risk of harm consistent with § 171.201(c)(2), and to the use of the practices for such time as is reasonable and necessary to amend or correct the patient's EHI. In assessing timeliness and reasonableness of an actor's approach to making such corrections, we would take into consideration the facts and circumstances within which they operate, including but not limited to licensure or certification requirements applicable to the actor's EHI governance. For a health care provider, we anticipate such licensure or certification requirements will typically include clinical records standards set by State licensure laws and additional standards applicable to that provider given their specific circumstances, such as patient records maintenance standards set by issuing bodies of facility/organizational accreditations or professional board certifications the provider may also hold.

Where an actor lacks the technical capability to sequester from otherwise legally permissible access, exchange, or use only that subset of EHI the actor knows or reasonably suspects is affected by data issues giving rise to risk of harm consistent with § 171.201(c)(2), the Preventing Harm Exception will not recognize withholding of the remaining EHI. In such circumstances, an actor should refer to the exceptions for Content and Manner (§ 171.301) and Infeasibility (§ 171.204), as may be applicable, in regard to the EHI that they do not know or reasonably suspect to be affected by data issues giving rise to risk of harm consistent with § 171.201(c)(2).

Risk Arising From Misidentifying a Patient or Mismatching Patients' Electronic Health Information

The Preventing Harm Exception is intended to apply to practices that are designed to promote data quality and integrity and to support health IT applications properly identifying and matching patient records or EHI. As discussed in the preamble to the Proposed Rule (84 FR 7524), accurately identifying patients and correctly attributing their EHI to them is a complex task and involves layers of safeguards. The task requires application of appropriate procedures for verifying a patient's identity and properly registering the patient in health IT systems. Safeguards include such usability and implementation decisions such as ensuring the display of a patient's name and date of birth, and perhaps a recent photograph, on every screen from which clinicians and other caregivers access, enter, and/or modify data in the patient's record. When a clinician, other health IT user, or other actor knows or reasonably suspects that specific EHI is not correctly attributed to one or more particular patient(s), it would be reasonable for them to avoid sharing the EHI that could introduce or propagate errors in patient records and thereby pose risks to the patient(s) affected.[155]

Under the Preventing Harm Exception as proposed, an actor's response to the risk of misidentified patient health information would need to be no broader than necessary to mitigate the risk of harm arising from the potentially misidentified record or misattributed data (84 FR 7524). For example, under the proposed exception, an actor—such as a health IT developer of certified health IT—refusing to provide a batch export on the basis that the exported records *might* contain a misidentified record would not find that practice recognized under this exception. Similarly, a health care provider or other actor that identified that a particular piece of information had been misattributed to a patient would not be excused under § 171.201 from exchanging or providing access to all other EHI about the patient that had not been misattributed. The actor knowing or reasonably suspecting some data had been misidentified or misattributed would also be expected to confirm the extent of such errors and to take appropriate steps to correct their own records, consistent with applicable law, regulations, and accreditation standards applicable to the actor, and best practices or other appropriate industry benchmarks for health records and information management.

Comments. Commenters recommended we consider that actors bear significant responsibility to preserve and promote data quality and integrity, and that actors generally take risk-averse approaches to preventing and to assessing and resolving errors in identifying EHI and matching patient EHI.

Response. We appreciate the opportunity to assure all stakeholders that we are aware that the EHI an actor receives from various sources may feature a variety of characteristics that call for varying degrees of pre-processing to achieve a level of matching accuracy considered by the health care provider community to be sufficient for safe use of the data in patient care. In some circumstances, we understand additional or special processing—including but not necessarily limited to human eyes-on analysis to confirm matches—may be needed before records are deemed to have been accurately matched, and that data requiring human processing may be delayed in integration and availability compared with data that can be satisfactorily matched through an actor's automated means. Section 171.201 will apply to such practices provided all of its conditions are met.

Comments. Commenters recommended the finalized exception recognize as reasonable and necessary to protect patient safety practices such as sequestering from access and exchange all records from a particular source, or

[155] Please note that practices designed and implemented to ensure that persons requesting access to their EHI are who they claim to be and give them access to only that EHI that is theirs would not be cognizable under the Preventing Harm Exception; we have established two other exceptions designed to address practices reasonable and necessary to protect the privacy (*see* § 171.202) and security (*see* § 171.203) of individuals' EHI.

affected by a particular system or technical process, until the scope and cause of patient matching or attribution issues can be identified and appropriately resolved. Commenters stated such practices are commonly used today by HINs/HIEs, and provided illustrative examples of current practice. Comments described as an example current practice of HIEs not making available any record(s) that their monitoring for technical or other issues identifies as an improperly matched patient record—and any other records that may be affected by a similar technical issue—until the record(s) can be corrected to include only accurately matched data.

Response. We do understand that a variety of methods and approaches may currently be needed to assess the scope, identify, and appropriately address the cause of patient matching or attribution errors. Section 171.201 will apply to practices otherwise meeting its conditions that affect more patients' records than those specifically confirmed to include mismatched or misattributed EHI. Where its conditions are otherwise met, the exception will apply to use of practices likely to interfere with access, exchange, or use of EHI that the actor knows includes mismatched or misattributed data or reasonably suspects includes such errors. Reasonable suspicion could be formed on various bases, such as objectively observable patterns of association between detected errors and a particular data source, application, system, or process. However, a practice of delaying the availability of records from any particular data source based on factors extraneous to matching processes and accuracy would not be excepted from the definition of information blocking. Examples of extraneous factors include, but are not limited to, whether the data source was competitor of the actor and whether the actor may harbor personal animus toward the data source.

Comments. One commenter suggested the Preventing Harm Exception allow for providers to refuse to release pediatric data to direct-to-consumer applications unless the provider was satisfied with the applications' ability to properly segment the data where multiple users' records might be stored in the same instance of the application. Specifically, the comment expressed a concern that if applications are not set up to safely handle multiple patients, data from multiple patients could be mixed together in ways that create a potential for serious harm stemming from how those data might then be used or interpreted.

Response. The potential for EHI to be mismatched (or otherwise mishandled) by an application, whether mobile or otherwise, is neither unique to pediatric patients' EHI nor particular to apps that receive the patient's data from a provider's API. A patient whose provider has not yet implemented a standards-based API could use other means to get their EHI into their chosen direct-to-consumer app. Such means could include accessing view, download, and transmit functionality of the provider's certified health IT via the patient portal and transmitting an extract of their data in C–CDA format to the recipient of the patient's (or their legal representative's) choice. An individual or their representative could also exercise the individual's right of access under the HIPAA Privacy Rule to obtain the individual's EHI that is accessible under this right, in another format in which it is readily producible, and then upload it to an app of their choosing. In general, we do not believe it would be appropriate to extend the Preventing Harm Exception to apply to practices whereby actors would limit otherwise legally permissible access, exchange, or use of patient EHI based on concerns that a requestor will not handle patient matching in a manner acceptable to the actor. Therefore, this exception will not apply to actors' refusal to allow access, exchange, or use of EHI on grounds that the actor may not know, or may not be satisfied with, the matching methods to be used by a recipient of the EHI after the EHI has been securely transferred to the recipient. Provided the practices meet its conditions, the Security Exception (§ 171.203) will apply to a variety of practices directly related and tailored to specific security threats to the actor's systems and EHI within those systems that may be posed by particular connections or interfaces with third-party systems or software. We also note that practices that do not inappropriately discourage patients from accessing, exchanging, or using their EHI as they choose, but that are appropriately designed and implemented to help patients make more informed choices about their EHI and apps can be designed and implemented to avoid meeting the definition of information blocking finalized in § 171.103.

Comments. One commenter expressed a concern that this exception could become a pretext for an actor to avoid sharing EHI on basis of the actor not being satisfied with the accuracy achieved by a prospective recipient's patient matching methods. This commenter requested ONC clarify that this exception does not allow for an actor to take a position that it will not share EHI unless the requesting entity demonstrates it will match patients using a method, or to a degree of accuracy, satisfactory to the actor being requested to share the information.

Response. We do not believe it would be appropriate to extend the Preventing Harm Exception to apply to practices whereby actors would limit otherwise legally permissible access, exchange, or use of patient EHI based on concerns that a requestor will not handle patient matching in a manner acceptable to the actor. Various recipients and users of EHI will have different purposes and contexts of data use and thus may appropriately deem differing levels of assurance of match accuracy satisfactory to meet their obligations, for patient safety or otherwise. Therefore, this exception will not apply to actors' refusal to allow access, exchange, or use of EHI on grounds that the actor may not know, or may not be satisfied with, the matching methods to be used by a recipient of the EHI after the EHI has been securely transferred to the recipient.

Comments. Some commenters specifically discussed concerns about potential misuse of this exception on a claim of patient matching concerns, and that this exception could lessen actors' motivations for improving their patient match capabilities. Some commenters suggested specific additional requirements for applicability of this exception to practices implemented to reduce risks of harm arising from mismatch or misidentification of patient EHI, in order to guard against its misuse or potentially incentivizing stagnation in rates of patient matching capabilities advancement. Additional requirements that commenters suggested were:

- That an actor only be able to take advantage of this exception on basis of mismatch if the actor's matching methods met or exceeded a performance threshold;
- that the actor proactively communicates to requestors the actor's minimum matching criteria and other aspects of its matching methods; and
- a requirement for specific features in the actor's systems, such as returning informative error messages regarding match failures.

Response. We are aware there is variation across actors in technical capabilities relevant to patient matching, resources to improve those capabilities, and other operational considerations. We are not aware of clear evidence or broad industry consensus on specific practices or

performance thresholds that should apply to across all EHI use cases and operational contexts. We believe it would be premature to limit the availability of this exception to actors able to implement specific practices or meet particular metrics of patient matching performance specified through this rulemaking. Because this exception is intended to except from the definition of information blocking in § 171.103 practices that are reasonable and necessary to protect patients from risks of cognizable harm attributable to types of risk specifically including risks arising from mismatched EHI, rather than to drive changes in patient matching practices in the industry, such requirements could render this exception unavailable in circumstances where it is intended to apply. Thus, we have determined that it is more appropriate to leave actors engaged in using data the discretion and responsibility for determining what level of certainty in the accuracy of record matching is necessary for their use of the EHI. We appreciate this opportunity to clarify that the Preventing Harm Exception would not excuse actors from making appropriate good faith efforts to match patient records, which we expect will ordinarily include communication and cooperation between data sources and recipients. Moreover, we believe an actor will generally have a natural incentive to communicate proactively, appropriately, and in good faith with those with whom they exchange data, specifically to minimize unnecessary extra processing and follow-up communications on the part of both exchange partners. Therefore, we have not modified the Preventing Harm Exception's conditions in response to these comments.

Comments. One commenter expressed a concern that to ensure they do not release information that has potential errors in patient matching or attribution, they will need to invest in improved patient record matching accuracy, which the commenter indicates would for them include new technical solutions compared with their current practice.

Response. This exception is not intended, and we are not persuaded that as finalized it will function, to impose a new or specific obligation on actors to ensure they do not release information that could contain latent errors. Other commenters did recommend we consider doing so. However, for the reasons stated above in response to those comments, we have not established a pre-requisite that an actor meet a particular threshold of patient-matching performance before this exception will apply to practices otherwise meeting the conditions of § 171.201 applicable in the particular circumstances, including that the actor can demonstrate a reasonable belief the practice(s) will substantially reduce a risk of harm cognizable under § 171.201. We emphasize that we have *not* established a pre-requisite for applicability of § 171.201 that would call upon an actor to use particular methods, or satisfy particular threshold performance rates on any specific metric, for patient identification and matching.

Comments. A few commenters requested clarification as to whether a patient would be liable for accessing another patient's EHI that had been mismatched or misattributed to the patient accessing the information.

Response. This issue is outside the scope of this rulemaking. Those concerned or curious about it should reference Federal,[156] State, or tribal law and regulations—or reliable sources of information about Federal,[157] State, or tribal law and regulations—applicable to any individual's (or entity's) unauthorized access to or use of another's personally identifiable information (PII) in the particular jurisdiction(s) and circumstances of potential concern.

Comments. One commenter suggested creation of a hold-harmless or ''safe harbor'' policy protecting data recipients from liability for actions taken in good faith reliance on information received after applying best-practice matching methods.

Response. The suggestion appears to reference a safe harbor from liability for decisions or other actions taken in reliance on the EHI in question. That is outside the scope of this rule. Actors should implement matching methodologies and practices in full awareness that this final rule will not change their responsibility under other applicable law for maintaining appropriately reliable medical or other business records. This final rule also does not alter clinicians' responsibilities for exercising sound professional judgment in making clinical decisions based on EHI available to them in context of what they know or reasonably believe about the EHI's reliability.

Comments. Commenters requested, in context and reference to the Preventing Harm Exception, guidance regarding what an actor is obligated to do if they receive EHI as a result of provider matching failure. One commenter specifically requested guidance on what sort of good faith efforts to direct the EHI to the correct recipient would be expected of an inadvertent recipient of mis-directed EHI.

Response. A provider or other actor who receives EHI that they have reason to believe may have been directed to them by mistake has no obligation under part 171 to identify the correct recipient or to forward the EHI to the correct recipient. The actor who believes they may have received mis-directed EHI should upon forming such belief follow their established practices for handling of PHI and PII received in known or suspected error. We presume these established practices are consistent with Federal, State, or tribal law applicable to the particular actor in the particular operational circumstances.

Statement of Finalized Policy for Risks Arising From Misidentified or Mismatched EHI

We are finalizing the substance of this part of the exception as proposed, with modifications to how it is expressed in regulation text in comparison with the Proposed Rule. We have reorganized the regulation text in response to comments requesting our regulatory text in general be laid out in a way that is easier to use. For example, we have combined risks arising from misidentified or mismatched EHI with other data-specific sources of risk of harm in the final § 171.201(c)(2), instead of splitting them across two paragraphs as was the case in § 171.201(a)(1) (''corrupt or inaccurate'' in the Proposed Rule) and § 171.201(a)(2) (''misidentified or mismatched'' in the Proposed Rule). We believe this makes the finalized text of § 171.201 easier to use because misidentified, mismatched, corrupt, and otherwise erroneous data are all sources of risk arising from issues with the data rather than characteristics unique to a patient or their circumstances. As was the case in the Proposed Rule, additional conditions must be met for § 171.201 to apply to practices implemented to substantially reduce a risk of harm arising from data issues (consistent with § 171.201(c)(2)). In the structure of the finalized regulation text, these additional conditions are found in § 171.201(a) and (b), and as applicable in the particular circumstances also in (d)(3) or (4), and (f)(1) or (2). Whether (d)(3) or (d)(4) sets out the harm

[156] Potentially applicable Federal law and regulations are not limited to HIPAA and the HIPAA Privacy Rule, but the HIPAA Privacy Rule may be a useful place for those who share interest in the question raised by these comments to begin obtaining additional information.

[157] Authoritative information about the HIPAA Privacy Rule is available in the health information privacy section of the HHS website, starting at *https://www.hhs.gov/hipaa/index.html.*

standard that applies to a practice an actor believes will substantially reduce a risk of harm consistent with § 171.201(c)(2) turns on whether the practice is likely to, or does, interfere with a patient's own or another other legally permissible access, exchange, or use of the patient's EHI. (We note, however, that the harm required to satisfy this condition is the same under (d)(3) and (d)(4), as both cross-reference § 164.524(a)(3)(i).) Whether (f)(1) or (f)(2) applies to a practice an actor believes will substantially reduce a risk of harm consistent with § 171.201(c)(2) turns on whether the actor implements the practice based on an organizational policy (f)(1) or a determination based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use (f)(2).

Determination by a Licensed Health Care Professional That the Disclosure of EHI Is Reasonably Likely To Endanger Life or Physical Safety (§ 171.201(c)(1))

We proposed that this exception would recognize practices interfering with EHI access, exchange, or use in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the access, exchange, or use of the EHI is reasonably likely to endanger the life or physical safety of the patient or another person (84 FR 7524 and 7525). As we explained, the clinician may have in certain cases individualized knowledge stemming from the clinician-patient relationship that, given the particular patient and that patient's circumstances, harm could result if certain EHI were shared or transmitted electronically. We proposed that, consistent with the HIPAA Privacy Rule, a decision not to provide access, exchange, or use of EHI on this basis would be subject to any right that an affected individual is afforded under applicable Federal or State laws to have the determination reviewed and potentially reversed.

Comments. Commenters recommended that actors, such as HINs/HIEs, implementing practices based on a determination by a health care professional, not be required to take steps to review or assess the reasonableness of the health care professional's judgment or determination that a risk of harm exists or that the harm of which a risk was determined to exist met the standard for recognition under this exception.

Response. We did not propose to require that other actors would ordinarily need to evaluate whether they agreed with individualized determinations of risk made by a licensed health care professional in order for the actor's application of practices consistent with that determination to be recognized under this exception. The finalized exception also does not generally require that actors relying on an individualized determination made by a licensed health care professional in the exercise of professional judgment take steps to review or confirm the health care professional's judgment.[158] Actors other than the licensed health care professional who makes the determination—including but not limited to HINs/HIEs or hospitals—could implement practices based on organizational policy (consistent with § 171.201(f)(1) as finalized) to rely on such determinations upon becoming aware of the determination and until such time as they become aware that the determination has been reversed or revised. Such other actors also, either in absence of such policy or in particularized facts or circumstances not fully covered by their existing policy at the time they became aware of a licensed health care professional's individualized determination of risk, could demonstrate for those particularized circumstances the reasonable belief required by § 171.201(a) by referencing the licensed health care professional's determination in making their own determination consistent with § 171.201(f)(2).

Comments. One commenter suggested that this exception should recognize determinations of the existence of a risk of harm made by licensed health care professionals without requiring a clinician-patient relationship.

Response. In order for practices implemented to substantially reduce a type of risk consistent with finalized § 171.201(c)(1) to be excepted under § 171.201 from the definition of information blocking finalized in § 171.103, the individualized determination of risk of harm in the exercise of professional judgment must be made by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination. In the preamble to the Proposed Rule (84 FR 7524) we explained that the clinician may have individualized knowledge stemming from the clinician-patient relationship that, for a particular patient and for that patient's circumstances, harm could result if certain EHI were shared or transmitted electronically. To ensure that both the requirement for a clinician-patient relationship and its specificity to individualized determinations of risk of harm by licensed health care professionals in the exercise of judgment are immediately clear to all actors, we have stated it in the finalized text of § 171.201(c)(1). We are finalizing this as a requirement because a clinician who has never established a clinician-patient relationship to the particular patient would not be expected to have the same individualized knowledge of the individual patient and that patient's circumstances as one who has such a clinician-patient relationship.

In contrast, however, we reiterate that a risk is less individualized when it arises from data issues (consistent with § 171.201(c)(2)) and as a result may be identified by clinicians or by other persons with relevant expertise, including but not limited to biomedical informaticists who are not licensed health care professionals. Nothing in § 171.201 requires the involvement of a licensed health care professional with a clinician-patient relationship to any patient(s) whose data may be affected by the practices in the design of, or decision to implement, practices an actor reasonably believes will substantially reduce a risk arising from data issues consistent with § 171.201(c)(2).

Comments. Several commenters recommended that, in the context of a clinician-patient relationship, the clinician should have broader latitude to consider specifics of a patient's circumstances in determining the existence of a risk of harm or potential harm.

Response. It may be helpful to highlight the significant and broad discretion inherent in the policy as we proposed it. An individualized determination made in the exercise of professional judgment by a licensed health care professional allows for that professional to consider a wide array of individual patient characteristics and circumstances and to apply all of the knowledge and skills within the licensed health care professional's scope of practice. The exception's conditions as proposed would provide licensed health care professionals broad discretion in how or why they form a reasonable belief that a cognizable risk of harm is associated with particular access, exchange, or use of their

[158] To the extent any particular actor may have an obligation under other Federal, state, or tribal law or regulations (as may be applicable in any particularized circumstances) to afford a patient a right of review of the determination—or to facilitate the patient's requesting a review of the determination from another actor—the actor's practices would need to be in compliance with such law or regulations in order for this exception to apply to those practices.

patient's EHI (including by the patient or their legal representative). We have finalized this aspect of the Preventing Harm Exception as proposed, though we have revised how the conditions, and specific requirements within particular conditions, are organized and phrased in regulation text. Nothing in the finalized § 171.201 would limit the types of information on which the licensed health care professional may rely, or the factors they may consider, in exercising their professional judgment to make individualized determinations of risk of harm consistent with § 171.201(c)(1).

Comments. A few commenters advocated for clinician discretion to determine whether a disclosure of health information was in the patient's best interest.

Response. We believe an individual clinician's assessment of the patient's best interest is a less objective standard than one based on the exercise of professional judgment paired with a defined standard of cognizable harm. It would thus render the exception more difficult to administer as well as more susceptible to inappropriate use of the exception. We are finalizing the substance of this condition of the Preventing Harm Exception as proposed: To satisfy the conditions of the Preventing Harm Exception, an individualized determination by a licensed health care professional in the exercise of professional judgment must be that a risk of harm cognizable under this exception is associated with particular access, exchange, or use of the patient's EHI. The harm cognizable under this exception will be one that would be recognized under § 164.524(a)(3)(i) (at this time, danger to the life or physical safety of the patient or another person) where a practice affects a patient's access, exchange, or use of their EHI, per the finalized § 171.201(d)(3). Where § 171.201(d)(1) or § 171.201(d)(2) applies, the harm cognizable under this exception will be one that would be recognized under § 164.524(a)(3)(iii) or § 164.524(a)(3)(ii), respectively. At this time, the harm standard in both § 164.524(a)(3)(iii) and § 164.524(a)(3)(ii) is ''substantial harm.'' For all legally permissible access, exchange, or use of the patient's EHI to which § 171.201(d)(1) through (3) do not apply, the finalized § 171.201(d)(4) applies, by cross-reference, the same § 164.524(a)(3)(i) harm standard of danger to the life or physical safety of the patient or another person that is applicable to practices interfering with the patient's access to their own EHI (that does not include PII of another).

Comments. Several commenters expressed a concern that the exception as proposed might not sufficiently recognize the entire array of circumstances where persons should not be granted access, exchange, or use of EHI. For instance, commenters suggested no access, exchange, or use of a patient's EHI should be available to a person suspected to be abusing, or at risk of beginning to abuse, the patient. Commenters also suggested that the exception should recognize that broader restrictions of EHI access than illustrated by examples in the Proposed Rule would in many cases be indicated by available evidence, widely recognized clinical practice guidelines, or State laws applicable to instances of known or suspected child, intimate partner, elder, or other abuse.

Response. This exception applies to practices the actor reasonably believes will substantially reduce a risk of harm determined on an individualized basis in the exercise of professional judgment by a licensed health care professional with a clinician-patient relationship with the patient whose EHI is affected by the determination (finalized § 171.201(c)(1)). Moreover, and as we noted in the Proposed Rule (84 FR 7524), this exception would apply when an actor implements practices that are likely to interfere with the access, exchange, or use of a patient's EHI pursuant to electing to not treat a person as a personal representative in accordance with 45 CFR 164.502(g)(5). We have finalized the substance of this feature of the exception as proposed, though 45 CFR 164.502(g)(5) is not expressly referenced in the final regulation text.

The listed examples described in the Proposed Rule were intended to be illustrative, not exhaustive. There are many other situations where the Preventing Harm Exception will apply to an actor's practices so long as the conditions of the exception are otherwise met. As another illustrative example, if a determination of risk of harm consistent with § 171.201(c)(1) indicates that a broad withholding of the patient's EHI from a known, suspected, or potential abuser is reasonably likely to substantially reduce a risk of harm to the patient or another person, then the exception will apply to those practices so long as its conditions are met in full. Moreover, provided its conditions are met in full, this exception will also apply to practices that may be likely to, or do, interfere with a legal representative's access, exchange, or use of a patient's EHI to a lesser degree than might an election not to recognize the representative as the patient's personal representative in accordance with § 164.502(g)(5)(i). Because the finalized § 171.201(d)(1) applies when a practice is likely to, or does, interfere with a legal representative's access to the patient's EHI, the harm standard required in such a situation is that stated in § 164.524(a)(3)(iii). Currently, that harm standard is ''substantial harm.''

We also expressly note that, although the ''substantial harm'' standard applied by § 171.201(d)(1) through cross-reference to § 164.524(a)(3)(iii) is not precisely the same as the requirement in § 164.502(g)(5)(i), we will interpret as sufficient for purposes of § 171.201(c)(1) and (d)(1) a licensed health care professional's election not to treat a person as the patient's legal representative in accordance with § 164.502(g)(5)(i). Moreover, having noted above the broad discretion licensed health care professionals have regarding what information to factor into their individualized determinations consistent with § 171.201(c)(1), we highlight that this broad discretion would allow them to consider any knowledge they might have of another licensed health care professional, or other type of covered entity, having elected in accordance with § 164.502(g)(5)(i) not to treat a person as the patient's representative.

Comments. Some comments implied concerns about the potential conflict between the documentation requirements of this exception and those required under other applicable law.

Response. Provided its conditions are met, this exception is applicable in circumstances where a licensed health care professional in the exercise of professional judgment has determined that there is a risk of abuse *beginning,* as well as circumstances in which prior or ongoing abuse is known or suspected. Actors have significant discretion and flexibility in determining how best to document determinations and the bases for their determinations. Where other law or regulations—Federal, State, or tribal—require a specific form, manner, or content of documentation in circumstances that would serve as basis for individualized determinations consistent with the finalized § 171.201(c)(1), we would consider that documentation relevant to assessing the applicability of this exception to those practices. In order to avoid potentially duplicative or other unnecessary burdens on licensed health care professionals or other actors, we have decided not to establish at this time a specific documentation condition and have decided not to establish other

unique documentation requirements for this exception.

Comments. In reference to a specific illustrative example in the Proposed Rule, one commenter indicated that withholding or delaying availability of only specific sensitive data elements may not be sufficient in circumstances such as those described in the Proposed Rule example, and that revoking a suspected abuser's proxy access on the whole may be more clinically appropriate in such circumstances (84 FR 7525).

Response. In response to this comment, we first clarify the intent and function of the example provided in the Proposed Rule. In the example, the licensed health care professional in the exercise of professional judgment had determined that only some information within the record would need to be withheld from the patient's partner's proxy access to her EHI (84 FR 7525). Although not specifically stated in the Proposed Rule, the example presumes a mature technical capability to sequester data from specific user(s) on an itemized basis. The example also presumes that the licensed health care professional, in their exercise of professional judgment, had not formed a reasonable belief that ceasing to recognize the patient's partner as her personal representative, and entirely revoking the partner's proxy access to her EHI, would substantially reduce a risk of harm to the patient. We intended that the example illustrate that where the licensed health care professional determined a risk of harm would arise from making a specific piece of information accessible to the patient's proxy, the minimum interference necessary to substantially reduce that risk of harm would be to withhold that specific piece of information from the patient's partner's proxy access to her EHI.

Comments. A commenter indicated that if a clinician has a suspicion (confirmed or not) that the patient is suffering intimate partner or elder abuse, it is considered clinically important that notes or other data elements indicating the suspicion not be released to the patient in the company of the suspected abuser. The commenter stated that such disclosure could undermine the clinician's ability to help the patient because the patient would likely be forced to switch clinicians. The comment also indicated there may be a risk that an abuser could harm the patient as a result of the disclosure of the clinician's suspicion.

Response. Because information blocking policy is specific to the access, exchange, and use of EHI, we read the commenter's example as suggesting two considerations specific to access, exchange, and use of EHI. First, we believe the comment indicates we should expressly acknowledge that these types of situations are often legally as well as clinically complex. It is not our intent that our policies unnecessarily add to this complexity. It is also not our intent that our policies undermine the ability of a licensed health care professional, or other actor relying on the professional's determination, to take appropriate steps to reduce abuse risks to which the professional's patients would otherwise be exposed. Nothing in § 171.201, or in the information blocking provisions generally, requires an actor to disclose their awareness or suspicion of abuse to the patient's legal representative in order to satisfy the conditions of the Preventing Harm Exception. Second, our understanding of this comment indicates that in some particular individualized circumstances the licensed health care professional may determine in the exercise of professional judgment that to substantially reduce a risk of harm it may be necessary to withhold some portions of a patient's EHI from the patient's own access through an API or patient portal. We can, for example, envision possible circumstances where a licensed health care professional with a clinician-patient relationship to the patient knows or has reason to believe that a person suspected of abusing a patient routinely ''looks over the shoulder'' of the patient while they access their EHI, or uses the patient's own credentials to access the patient's EHI. In such circumstances, this exception would apply to practices interfering with the patient's own access to their EHI to the extent the practices are not inconsistent with the HIPAA Privacy Rule or the conditions in § 171.201.

Comments. Several commenters suggested that the Preventing Harm Exception should recognize more types of abuse, and a broader array of potential types of harm than danger to life or physical safety in the context of interfering with access to a patient's EHI by a legal representative suspected of abusing the patient. One commenter advocated that the Preventing Harm Exception should recognize all types of violence and abuse. The commenter provided citations to professional specialty expert committee opinions in support of their recommendation.

Response. As discussed above in reference to comments that recommended aligning this rule's harm standards more closely to the HIPAA Privacy Rule, we have, by cross-reference in § 171.201(d)(1), finalized as the harm standard applicable to practices interfering with a legal representative's access to a patient's EHI the same harm standard that would apply to denying a personal representative's access to an individual's PHI under § 164.524(a)(3)(iii). As § 164.524(a)(3)(iii) stands at the time this rule is finalized, it references ''substantial harm.'' As discussed above, this exception will also apply to practices likely to interfere with a legal representative's access, exchange, or use that are employed pursuant to an election not to treat that legal representative as a personal representative in accordance with § 164.502(g)(5)(i). For purposes of § 171.201, ''substantial harm'' is interpreted as it is for purposes of § 164.524(a)(3)(iii). Thus, for purposes of not recognizing a personal representative, or otherwise restricting patient EHI access, exchange, or use by a representative known or suspected to be abusing the patient, we believe the harm standard applicable under this exception to practices affecting a legal representative's access, exchange, or use of the patient's EHI is sufficiently broad. We interpret the discretion afforded to a licensed health care professional in making an individualized determination of risk of harm consistent with the finalized § 171.201(c)(1) (type of risk condition) as allowing them to take into consideration clinical practice guidelines and clinical expert groups' studied opinions relevant to abuse-related risks of substantial harm. Only practices based on the potential for harms that would not be recognized as meeting the ''substantial harm'' standard, as it is interpreted by the HHS Office for Civil Rights for purposes of § 164.524(a)(3)(iii), would fail to satisfy the type of harm condition finalized in § 171.201(d)(1). We remind actors that any decision not to provide access, exchange, or use of EHI on the basis of determination of risk of harm consistent with the finalized § 171.201(c)(1) and § 171.201(d)(1), (2), (3), or (4) is subject to rights the individual patient whose EHI is affected may be afforded by applicable regulations or law to have the determination reviewed and potentially reversed. (See the ''patient right to request review of individualized determination of risk of harm'' condition finalized in § 171.201(e), for which we also use ''patient review rights condition'' as a short form of reference for ease of discussion.) Where § 164.524(a)(3) applies in addition to § 171.201, § 164.524(a)(4) specifically

provides for review of determinations made by licensed health care professionals in the exercise of professional judgment. In circumstances where § 171.201 applies but § 164.524 does not, § 171.201(e) requires that an actor's practices be consistent with any rights of review of individualized determinations of risk of harm that the patient may be afforded under applicable Federal, State, or tribal law or regulations. However, for purposes of § 171.201(c)(1) determinations, the type of harm must be consistent with: The harm standard stated in § 164.524(a)(3)(i) (interpreted as it is for purposes of § 164.524(a)(3)(i)) where § 171.201(d)(3) or (4) apply; the harm standard stated in § 164.524(a)(3)(ii) (interpreted as it is for purposes of § 164.524(a)(3)(ii)) where § 171.201(d)(2) applies; or the harm standard stated in § 164.524(a)(3)(iii) (interpreted as it is for purposes of § 164.524(a)(3)(iii)) where § 171.201(d)(1) applies.

Finalized Policy for an Individualized Determination of Risk of Harm by a Licensed Health Care Professional in the Exercise of Professional Judgment

We are finalizing the substance of this aspect of the exception with modifications to the way it is displayed and phrased in the finalized regulation text in comparison to the Proposed Rule. If its other conditions are also met, the finalized Preventing Harm Exception will apply to a practice an actor reasonably believes will substantially reduce a risk of harm consistent with the sub-paragraph of § 171.201(d), as finalized, that applies to the specific access, exchange, or use, where the risk of harm is determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination. In comparison to the proposed text of § 171.201 (84 FR 7602), we have reorganized the regulation text in response to comments requesting our regulatory text, in general, be easier to use for purposes such as understanding how the conditions of the exception relate to one another and how they apply to practices used in particular types of circumstances. We have left the potential sources of risk of harm in a single paragraph (finalized § 171.201(c)), but separated them from the reasonable belief condition paragraph (finalized § 171.201(a)). The sources of risk of harm are also, as discussed above, presented in two sub-paragraphs in the finalized text of § 171.201(c) (type of harm) instead of being split across three sub-paragraphs as they were in the Proposed Rule.

In subparagraph (a)(3) of the proposed text of § 171.201 (84 FR 7602), we expressed the additional condition that practices based on individualized determinations of risk of harm are subject to any rights of review of the determination that the patient may be afforded under applicable law. This patient review rights condition is finalized in § 171.201(e). As finalized, this condition requires that where a risk of harm is determined on an individualized basis (consistent with § 171.201(c)(1) as finalized), the actor must honor any rights the individual patient whose EHI is affected may have under § 164.524(a)(4) or any Federal, State, or tribal law applicable in the circumstances to have the determination reviewed and potentially reversed. We have stated the condition for providing review rights afforded by law in the separate paragraph (e) of § 171.201 instead of including it within subparagraph (c)(1) because in the context of 171.201 the patient review rights condition functions as a condition on how practices based on such belief are implemented more than as a required characteristic of the § 171.201(c)(1) determination itself.

The finalized text of § 171.201(c)(1) also differs from the proposed regulation text specific to individualized determinations of risk in explicitly stating the requirement that the licensed health care professional making the determination must have a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination. For purposes of § 171.201—as we discussed in the Proposed Rule's preamble, and above in this preamble—we believe the broad discretion afforded to licensed health care professionals to make individualized determinations of risks of harm in the exercise of professional judgment is appropriate in the context of the expectation that a licensed health care professional with a clinician-patient relationship to a patient has the opportunity to have knowledge of the patient and their individual circumstances that is not generally available outside the context of a clinician-patient relationship. We believe that explicitly stating in § 171.201(c)(1) the requirement for a clinician-patient relationship accomplishes two purposes: First, it ensures that this is immediately clear on the face of the finalized regulation text that only determinations made by licensed health care professionals who have or have had a clinician-patient relationship with the patient will be considered consistent with § 171.201(c)(1); and, second, it is also clear that the condition for a clinician-patient relationship is specific and limited to determinations of risks of harm on an individualized basis in the exercise of professional judgment by a licensed health care professional (§ 171.201(c)(1) as finalized). Please note that this requirement is specific to the individualized determination of risk of harm, and does not limit application of § 171.201 to practices implemented directly by the licensed health care professional making a determination of risk of harm consistent with § 171.201(c)(1) as finalized. Appropriately tailored practices applied because the actor has a reasonable belief the practice will substantially reduce a risk of harm that was determined on an individualized basis consistent with § 171.201(c)(1) will, if all other applicable conditions of § 171.201 are met, be recognized under this exception whether the practices are undertaken by the licensed health care professional making the determination or by another actor (*e.g.,* another licensed health care professional, a hospital, or a HIN) having custody or control of the patient's EHI and knowledge of the individualized determination of risk of harm associated with particular access(es), exchange(s), or use(s) of that EHI.

As finalized, § 171.201(d) differs from the proposed policy in that it does not uniformly require that the risk determined on an individualized basis be to life or physical safety of the patient or another person in all circumstances. Instead, through specified cross-references to the sub-paragraphs of § 164.524(a)(3), the finalized § 171.201(d) type of harm condition uses the same harm standards for the circumstances where both the Preventing Harm Exception and § 164.524(a)(3) apply. Also through cross-references, the type of harm condition applies the § 164.524(a)(3) harm standards in circumstances similar to those in which § 164.524(a)(3) applies but where only § 171.201 actually applies. The finalized § 171.201(d) does not cross-reference § 164.502(g)(5)(i), but it is constructed so that it does apply to practices interfering with a personal representative or other legal representative's access to a patient's EHI consistent with an actor declining to recognize such a representative on the same bases as a HIPAA covered entity could elect not to recognize a person as an individual's personal representative consistent with § 164.502(g)(5)(i). In order to retain a clear, consistent set of

harm standards throughout the § 171.201 type of harm condition, however, we note that where a HIPAA covered entity elects not to recognize an individual's personal representative consistent with § 164.502(g)(5)(ii), the Preventing Harm Exception would not apply.[159]

Consistent with the HIPAA Privacy Rule, a decision not to provide access, exchange, or use of EHI on the basis finalized in § 171.201(c)(1) is subject to the rights the individual patient whose EHI is affected may be afforded by applicable law to have the determination reviewed and potentially reversed. While any such determination reviews may be pending, application of practices interfering with the patient's access, exchange, or use of their EHI based on an individualized determination by a licensed health care professional (§ 171.201(c)) that are otherwise compliant with the conditions of § 171.201 as a whole will be considered to be covered by the exception.

Upon becoming aware of a reversal of the determination on which the actor's required reasonable belief was based, whether as a result of a review requested by the patient or other processes, the actor's continued application of practices based on the original determination would no longer be consistent with the conditions of § 171.201. Likewise, upon becoming aware of a revision of the determination on which the actor's required reasonable belief was originally based, whether the revision resulted from a review requested by the patient or other processes, practices applied to the patient's EHI after the revision is made will need to comply with the conditions of § 171.201 in light of the revised determination in order for the practice to continue to be covered under § 171.201.

For the specific purposes of § 171.201, the rights to obtain review or reconsideration of a provider's individualized determination of risk of harm reside with the patient whose EHI is affected. The rights in many cases may be exercised on the patient's behalf by the patient's personal or other legal representative. However, it may not be appropriate, or feasible, for the patient's representative to exercise the patient's review rights in circumstances where the individualized determination of risk of harm is or includes a determination that recognizing that same person as the patient's representative, or providing specific information to that same recognized representative, would pose a risk of cognizable harm. In a circumstance where the actor has a reasonable belief that such disclosure could create or increase a risk of harm to the patient, this exception does not require the candid disclosure to a known, suspected, or potential abuser of the rationale for use of particular practices, or even the precise practices, interfering with that representative's access, exchange, or use of EHI. We would, however, generally expect actors to be as candid with the patient *per se* as is clinically appropriate and safely practicable in their individualized circumstances.

Where an actor lacks the technical capability to sequester only that EHI the actor reasonably believes poses a risk of cognizable harm from other data for which the actor does not pose such risk of harm, this lack of segmentation capability would not render § 171.201 applicable to practices likely to, or that do, interfere with access, exchange, or use of the other data. Rather, where such lack of segmentation capabilities renders the actor unable to support an otherwise legally permissible access, exchange, or use of EHI, the actor should reference the Content and Manner Exception (§ 171.301) or the Infeasibility Exception (§ 171.204).

Licensed health care professionals have discretion to determine how to use their EHRs and/or other records kept in their ordinary course of business to capture and preserve documentation of and relevant to their individualized determinations. Information relevant to determinations would include the facts or circumstances that substantially informed each determination, and any other decision-making information that the professional may otherwise have difficulty recalling or reconstructing if later asked to explain how or why they reached their individualized determination in a particular case.

Practices Implemented Based on an Organizational Policy or on Determination Specific to the Facts and Circumstances

To qualify for the Preventing Harm Exception, we proposed that an actor would be required to have, while engaging in the practice(s) for which application of the exception is claimed, a reasonable belief that the practice(s) will ''directly and substantially'' [160] reduce the likelihood of harm to a patient or another person. As discussed in the Proposed Rule and above, the type of risk and the potential harm must also be cognizable under this exception (84 FR 7525 and 7526).

Under § 171.201 as proposed, an actor would be able to demonstrate having satisfied the condition of reasonable belief that a practice will reduce the likelihood of harm (''reasonable belief condition'') through a qualifying organizational policy (proposed § 171.201(b)) and/or a qualifying individualized determination (proposed § 171.201(c)). We discuss below the details of our proposal, respond to comments, and summarize finalized policy specific to each of these approaches to demonstrating the required reasonable belief that a practice will substantially [161] reduce a risk of harm cognizable under this exception.

Practices Implemented Based on an Organizational Policy

In the Proposed Rule (84 FR 7525), we proposed that to qualify for this exception, an actor must have had a reasonable belief that the practice or practices will directly and substantially reduce the likelihood of harm to a patient or another person and that the type of risk must also be cognizable under this exception. We proposed that an actor could meet this condition in two ways: Through a ''qualifying organizational policy'' (§ 171.201(b) as proposed) or through a ''qualifying individualized finding'' (§ 171.201(c) as proposed). We stated in the Proposed Rule that we anticipate that in most instances where § 171.201 would apply, the actor would demonstrate that the practices it engaged in were consistent with an organizational policy that was objectively reasonable and no broader than necessary for the type of patient safety risks at issue. We also noted in the Proposed Rule that within any type of actor defined in § 171.102, organizations may vary significantly in structure, size, and resources. Further, even when an organizational policy exists, it may not anticipate all of the potential risks of harm that could arise in real-world clinical or production

[159] Because § 164.502(g)(5)(ii) currently applies a standard not of harm but of determination by the covered entity that recognizing a person as personal representative is not in the best interest of the individual, we have determined it is more appropriate to address these circumstances in context of the exception for practices promoting privacy of EHI, finalized in § 171.202 and discussed in Section VIII.D.1.b of this final rule preamble.

[160] As, and for the reasons, discussed earlier in this section of this preamble, we have removed ''directly and'' from the belief standard finalized in § 171.201(a).

[161] As, and for the reasons, discussed earlier in this section of this preamble, the belief standard finalized in § 171.201(a) requires the actor believe the practice will ''substantially reduce'' a risk of harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information affected by the practice.

environments of health IT. Thus, we proposed in § 171.201(c) (84 FR 7602) that in lieu of demonstrating that a practice conformed to a policy that met the conditions described in proposed § 171.201(b) and the Proposed Rule preamble at 84 FR 7525, the actor could justify the practice(s) directly by making a finding in each case, based on the particularized facts and circumstances.

We proposed that where the proposed § 171.201(b) (84 FR 7602) would apply, an actor's policy would need to be:

- In writing;
- developed with meaningful input from clinical, technical, and other appropriate staff or others who have expertise or insight relevant to the risk of harm that the policy addresses;
- implemented in a consistent and non-discriminatory manner; and
- no broader than necessary to mitigate the risk of harm.

We stated that the proposed condition would not be met if, for example, a hospital imposed top-down information sharing policies or workflows established by the hospital's EHR developer and approved by hospital administrators without meaningful input from the medical staff, IT department, and front-line clinicians who are in the best position to gauge how effective it will be at mitigating patient safety risks.

Comments. Commenters expressed concern that information blocking policy and its interaction with other applicable laws and regulations, such as the HIPAA Rules, are complex and that there will be costs and other burden associated with understanding how the policies affect an actor's daily operations. Commenters also expressed concern that it would be too burdensome to be required to demonstrate, in any of the ways we proposed, that they have a reasonable belief that practices would reduce a risk of cognizable harm.

Response. We understand that complexity can increase difficulty in understanding and complying with any regulation. We also understand that the interaction between the HIPAA Rules and the information blocking provision is inherently complex. However, without an exception from the information blocking definition for practices appropriately tailored to reduce risks of harm, we believe actors would be subject to the greater burden of needing to craft practices that avoid violating the information blocking provision without also making EHI available for access, exchange, or use in circumstances where that puts patients or other natural persons at risk of harm. This exception's conditions give actors a framework within which they can develop or refine their practices in assurance that practices meeting the conditions in § 171.201 are excepted from the definition of information blocking finalized in § 171.103. At the same time, implementing such an exception without appropriate conditions could have the unintended and undesirable effect of excusing conduct that would more appropriately remain within the definition of information blocking.

Therefore, in § 171.201, we have finalized conditions that strike a practical balance between minimizing burdens on actors and ensuring that the interests of patients in the access, exchange, and use of their EHI are adequately protected. These conditions are, in comparison to the Proposed Rule, more granularly and durably aligned with relevant HIPAA right of access provisions (§ 164.526(a)(3)) and this alignment reduces complexity.

We have revised the way the regulation text is presented and phrased so that it is easier to understand what is required in order for a practice to be excepted from the definition of information blocking under this exception. Moreover, we have avoided specifying particular or unique forms, methods, or content of documentation for purposes of this exception. We believe the flexibility this offers actors to determine the most efficient approach to documenting their practices and determinations relevant to this exception enables them to achieve and document satisfaction of the exception's condition with the lowest practicable burden.

Comments. A number of commenters noted that there will be burden associated with developing or revising organizational policies and training staff so they can use this exception in compliance with its conditions. Several of these commenters suggested we provide additional guidance and informational resources, in this final rule or otherwise, to help actors develop their policies and staff training. Some commenters advocated that we develop templates or models that actors could use to more efficiently develop policies consistent with the conditions for applicability of this exception.

Response. We appreciate the feedback and do recognize that developing or revising internal policies and procedures when compliance requirements change due to changes in law requires some effort. While recognizing the utility of the types of resource materials suggested by commenters, we believe they are best developed and provided outside the rulemaking process. We will continue working to engage with the stakeholder communities to promote understanding and foster compliance with the information blocking provision amongst all actors within the definitions in § 171.102. We also believe that in many cases voluntary groups with relevant expertise, such as professional societies and provider organizations, may be in the best position to develop resources tailored to the particular needs and preferences of specific segments or communities within any given type of actor.

Comments. Some commenters stating that developing new or revised organizational policies and training staff in the policies requires time recommended that we establish a grace period before organizations' policies and actual practices must fully comply with § 171.201 conditions in order to be recognized as reasonable and necessary under § 171.201.

Response. This concern is not unique to § 171.201. Commenters also raised this concern in the context of information blocking in general. As we stated in section VIII.B.3 of this preamble, we thank commenters for their input. Comments related to the overall timing of information blocking enforcement have been shared with OIG. We emphasize that individuals and entities subject to the information blocking provision must comply with the ONC final rule as of the compliance date of the information blocking section of this final rule (45 CFR part 171). We have finalized a compliance date for 45 CFR part 171 as a whole that is six months after the date this final rule is published in the **Federal Register**.

OIG and ONC are coordinating timing of the compliance date of the information blocking section of this final rule (45 CFR part 171) and the start of information blocking enforcement. We are providing the following information on timing for actors. Enforcement of information blocking CMPs in section 3022(b)(2)(A) of the PHSA will not begin until established by future notice and comment rulemaking by OIG. As a result, actors would not be subject to penalties until CMP rules are final. At a minimum, the timeframe for enforcement would not begin sooner than the compliance date of the information blocking section of this final rule (45 CFR part 171) and will depend on when the CMP rules are final. Discretion will be exercised such that conduct that occurs before that time will not be subject to information blocking CMP.

Specific to § 171.201, as discussed above in response to other comments

received specific to the Preventing Harm Exception, we have applied § 164.524(a)(3) harm standards under § 171.201 to circumstances where both sections of 45 CFR would apply, and to circumstances where only § 171.201 applies but that are similar in significant respects to circumstances where § 164.524(a)(3) applies. In substantial part because of this alignment, we do not believe there is a need to delay the applicability of any of the conditions for a practice to be excepted under § 171.201 from the definition of information blocking in § 171.103.

Actors who are also HIPAA covered entities or business associates should already have policies in place consistent with the HIPAA Privacy Rule, including but not limited to § 164.524(a)(3). These actors and their staff members should be well versed in these policies and practices. Where § 164.524(a)(3) would not apply but § 171.201(d)(3) or (4) would apply, we believe using the same, familiar standard for the risk that the actor must believe their practice would reduce as would apply to § 164.524(a)(3)(i) should facilitate efficient updates to organizational policies and streamline any staff training that may be indicated specific to § 171.201. We also note that the finalized Preventing Harm Exception also provides, in § 171.201(f)(2), for coverage of practices implemented in absence of an applicable organizational policy or where existing organizational policy does not address the particular practice in the particularized circumstances. Moreover, although we encourage actors to voluntarily conform their practices to the conditions of an exception suited to the practice and its purpose, an actor's choice to do so simply provides them an enhanced level of assurance that the practices do not meet the definition of information blocking. However, failure to meet an exception does not necessarily mean a practice meets the definition of information blocking. We reiterate, if subject to an investigation by HHS, each practice that implicates the information blocking provision would be analyzed on a case-by-case basis.

Comments. Several commenters indicated that providers' current organizational policies call for practices that delay the release of laboratory results so that the patient's clinician has an opportunity to review the results before potentially needing to respond to patient questions, or has an opportunity to communicate the results to the patient in a way that builds the clinician-patient relationship. Some commenters indicated their standard practice is to automatically time-delay release of results in general, with an automatic release at the end of a time period determined by the organizational policy in place to ensure that patients can consistently access their information within the timeframe targeted by relevant measures under the CMS Promoting Interoperability Programs. Commenters requested we clarify whether such practices would be recognized under § 171.201 or that we recognize such current organizational policies and practices as excepted from the definition of information blocking.

Response. While we recognize the importance of effective clinician-patient relationships and patient communications, we are not persuaded that routinely time-delaying the availability of broad classes of EHI should be recognized as excepted from the information blocking definition under this exception. Consistent with § 171.201(d)(3) as finalized, the harm of which a practice must reduce a risk must, where the practice interferes with the patient's access to their own EHI, be one that could justify denying the patient's right of access to PHI under § 164.524(a)(3). Currently, § 164.524(a)(3)(i) requires that for a covered entity to deny an individual access to their PHI within the designated record set, the disclosure of that PHI must be reasonably likely to endanger the life or physical safety of the patient or another person.[162] No commenter cited evidence that routinely delaying EHI availability to patients in the interest of fostering clinician-patient relationships substantially reduces danger to life or physical safety of patients or other persons that would otherwise routinely arise from patients' choosing to access the information as soon as it is finalized.

Moreover, we are independently aware, and some comment submissions confirmed, that it is not uncommon to automatically release lab and other findings to patients electronically regardless of whether a clinician has seen the information or discussed it with the patient before the patient can choose to access it electronically. We presume these types of automatic releases would not be the case if patients' accessing their information on a timeframe that is more of their own choosing routinely posed a risk to the life or physical safety of these patients or other natural persons. Thus, we believe that where applicable law does not prohibit making particular information available to a patient electronically before it has been conveyed in another way, deference should generally be afforded to patients' right to choose whether to access their data as soon as it is available or wait for the provider to contact them to discuss their results. Only in specific circumstances do we believe delaying patients' access to their health information so that providers retain full control over when and how it is communicated could be both necessary and reasonable for purposes of substantially reducing a risk of harm cognizable under § 171.201(d) (as finalized). Circumstances where § 171.201 would apply to such delay are those where a licensed health care professional has made an individualized determination of risk in the exercise of professional judgment consistent with § 171.201(c)(1), whether the actor implementing the practice is the licensed health care professional acting directly on their own determination or another actor implementing the delay in reliance on that determination. An actor could choose to demonstrate the reasonable belief required by § 171.201(a) through an organizational policy (§ 171.201(f)(1)) with which the practice is consistent, or based on a determination based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use (§ 171.201(f)(2)), to rely on a determination consistent with § 171.201(c)(1).

Comments. Health care professionals commented that clinical experience indicates a systematic and substantial risk that releasing some patient data through a patient portal or API without first communicating the particular results or diagnosis with the patient in a more interactive venue would pose risks of substantial harm to patients. One example commenters specifically cited was genetic testing results indicating a high risk of developing a neurodegenerative disease for which there is no effective treatment or cure. Commenters recommended that we define this exception to allowing delay of the electronic release of such genetic testing results, as a matter of organizational policy, to ensure patients and their families are not exposed to this information without appropriate counseling and context. One comment indicated that delivery by the clinician of the combined results, counseling, and context is clinically appropriate and consistent with the conclusions of relevant research.

[162] Note that for purposes of § 164.524(a)(3)(i), ''individual'' is defined in § 160.103, but for purposes of § 171.201 an actor must reasonably believe a practice will substantially reduce a risk of cognizable harm to patient(s) or other natural person(s).

Response. To satisfy the conditions of § 171.201, and actor would have to demonstrate that they held a reasonable belief that delaying availability of information until the information can be delivered in combination with appropriate counseling and context in an interactive venue will substantially reduce a risk of harm cognizable under this exception. An actor could accomplish such demonstration through showing the practice is consistent with either an organizational policy meeting § 171.201(f)(1) or a determination based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use meeting § 171.201(f)(2). However, for a practice likely to, or that does in fact, interfere with the patient's access to their own EHI (§ 171.201(d)(3)), the actor implementing these practices must demonstrate a reasonable belief that the practice will substantially reduce a risk of harm to the life or physical safety of the patient. The clinician who orders testing of the sort referenced in the comment would, we presume, do so in the context of a clinician-patient relationship. In the context of that relationship, a licensed health care professional should be well positioned to make determinations consistent with § 171.201(c)(1) as to specifically when their patients, or other particular natural persons, would face a risk of harm cognizable under § 171.201(d)(3)—or § 171.201(d)(1) or (2) if or as may be applicable—if the access, exchange, or use of a particular testing result or diagnosis were to be released electronically before it could be explained and contextualized by an appropriately skilled professional, such as a clinician or a health educator, in real time.

Summary of Finalized Policy: Practices Implemented Based on an Organizational Policy

We have finalized that to demonstrate the reasonable belief required by § 171.201(a) based on an organizational policy, the policy must:

(i) Be in writing;

(ii) Be based on relevant clinical, technical, and other appropriate expertise;

(iii) Be implemented in a consistent and non-discriminatory manner;

(iv) Conform each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions of paragraphs (c) through (e) of this section applicable to the practice and its use.

We have modified the regulation text finalized in § 171.201(f)(1) consistent with other revisions to § 171.201. We have redesignated this paragraph from (b) to (f)(1), and redesignated its proposed sub-paragraphs from (1) through (4) to (i) through (iv). We have in comparison to the main paragraph language of the proposed § 171.201(b) modified the phrasing of the finalized paragraph (f) so that § 171.201 as finalized is more immediately clear on its face that what is finalized in § 171.201(f) is a condition for practices to meet the exception, and that paragraph (f) can be satisfied by meeting either subparagraph (1) or (2).

Practices applied based on an organization policy to rely on individualized determinations of risk of harm consistent with § 171.201(c)(1) would be covered under § 171.201 to the extent they otherwise meets its conditions. Neither an organizational policy (§ 171.201(f)(1)), nor a determination based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use ((§ 171.201(f)(2)) would be required to routinely evaluate or otherwise assess the licensed health care professional's exercise of professional judgment in order for practices implemented in reliance on the professional's § 171.201(c)(1) determination to be meet the conditions of § 171.201.

Practices Implemented Based on a Determination Specific to the Facts and Circumstances

As discussed in the Proposed Rule, we recognize that some actors (such as small health care providers and small HINs/HIEs) may not have comprehensive and formal policies governing all aspects of EHI and patient safety. Additionally, even if an organizational policy exists, it may not anticipate all of the potential risks of harm that could arise in real-world clinical or production environments of health IT. In these circumstances, in lieu of demonstrating that a practice conformed to the actor's policies and that the policies met the conditions proposed in § 171.201(b), we proposed that the actor could justify its use of particular practices by making a finding in each case, based on the particularized facts and circumstances, that the practice is necessary and no broader than necessary to mitigate the risk of harm. To do so, we proposed that the actor would need to show that the practices were approved on a case-by-case basis by an individual with direct knowledge of the relevant facts and circumstances and who had relevant clinical, technical, or other appropriate expertise. Such an individual would need to reasonably conclude, based on those particularized facts and circumstances and his/her expertise and best professional judgment, that the practice was necessary, and no broader than necessary, to mitigate the risk of harm to a patient or other persons. We further proposed that a licensed health care professional's independent and individualized judgment about the safety of the actor's patients or other persons would be entitled to substantial deference under this proposed exception. So long as the clinician considered the relevant facts and determined that, under the particular circumstances, the practice was necessary to protect the safety of the clinician's patient or another natural person, we would not second-guess the clinician's professional judgment. To provide further clarity on this point, we provided an illustrative example in the preamble to the proposed rule (see 84 FR 7525).

Comments. Commenters requested that we clarify, provide guidance, or establish specifications for the documentation necessary to substantiate applicability of the Preventing Harm Exception based on qualifying determinations particularized to specific facts and circumstances. Some commenters indicated that such specificity or guidance is needed to avoid imposing on actors such as health care providers and HINs/HIEs excess burden associated with documentation in the absence of such guidance or specification.

Response. We appreciate these commenters highlighting that the potential for uncertainty or confusion about what is minimally necessary to demonstrate satisfaction of a new policy can often lead to capturing and retaining a wide array of information just in case it may be needed or useful later. We have clarified the way in which all of the conditions in § 171.201 are stated and organized within the section. We also note here that an actor does not need to draft for each determination consistent with § 171.201(f)(2) a comprehensive defense of their findings. We believe the finalized statement of the condition, reinforced by this preamble discussion, provides certainty that we do not intend or expect actors to create new records systems or types, or to create or retain duplicate information or documentation across their current medical and other business records. Ultimately, it is the actor's responsibility to demonstrate they met the conditions of an exception.

Summary of Finalized Policy: Practices Implemented Based on a Determination Specific to the Facts and Circumstances

We have finalized the substance of this condition as proposed, with modifications to the regulation text. We have also reorganized § 171.201 so that it is easier to read and understand. We have redesignated this paragraph from (c) to (f), and broken it into subparagraphs. We have in comparison to the main paragraph language of the proposed § 171.201(c) modified the phrasing of the finalized paragraph (f) so that § 171.201 as finalized is more immediately clear on its face that what is finalized in § 171.201(f)(2) is a means to demonstrate a practice implemented in absence of an applicable, or perhaps any, organizational policy nevertheless meets the conditions to be exempted under § 171.201 from the definition of information blocking in § 171.103.

We have separated from both the requirements applicable to individualized determinations of risk (finalized in the type of risk condition in § 171.201(c)(1)) and the requirements applicable to practices implemented based on organizational policy (§ 171.201(f)(1)) or to practices implemented pursuant to a determination based on the facts and circumstances (§ 171.201(f)(2)) the patient review rights condition expressed in subparagraph (a)(3) of the proposed text of § 171.201 (84 FR 7602). We have finalized the patient review rights condition in § 171.201(e) instead of the finalized (f) because it applies equally to practices implemented based on an organizational policy and by practices implemented based on determinations based on facts and circumstances, in parallel to the other conditions for a practice to be excepted under § 171.201 from the definition of information blocking in § 171.103.

In the finalized patient review rights condition (§ 171.201(e)), in comparison with proposed § 171.201(a)(3) (84 FR 7602), we have revised the wording in which we state the condition for honoring any rights that applicable law may afford patients to have these individualized determinations reviewed and potentially reversed. The condition finalized in § 171.201(e) is that where the risk of harm is consistent with paragraph (c)(1) of this section, the actor must implement its practices in a manner consistent with any rights the individual patient whose EHI is affected may have under § 164.524(a)(4) of this title, or any Federal, State, or tribal law, to have the determination reviewed and potentially reversed.

We also revised in finalized § 171.201(e), in comparison with the proposed § 171.201(a)(3), the wording of the condition finalized in § 171.201(e) in comparison to the wording of this condition as proposed in 171.201(a)(3) for two reasons. First, the wording has been revised to fit its placement within the finalized section. Second, the wording has been revised to more clearly and completely state the sources of the review rights that must be afforded, if applicable. We note that such review rights will be afforded by § 164.524(a)(4) in the circumstances where both § 164.524(a)(3) and § 171.201 apply. However, rights that must be honored to meet the conditions of § 171.201 are not limited to those afforded by § 164.24(a)(4) or to circumstances where § 164.524 applies in addition to § 171.201. Rights of review of an individualized determination of risk of harm (§ 171.201(c)(1)) might also be afforded by Federal, State, or tribal law applicable in the particular circumstances.

We do not believe it is necessary to expressly state in the regulation text that we interpret regulations promulgated based on such laws, and that have the force and effect of law on individuals and entities they regulate, to be within the meaning of ''law'' for purposes of § 171.201(e). However, we expressly state this here in order to provide the type of assurance we believe many commenters were seeking when stating in their comment submissions requests or recommendations for additional guidance in the final rule. In order for the practice(s) to satisfy the condition in § 171.201(e), where otherwise applicable law affords a patient right(s) to request review of individualized determinations of risk of harm associated with the patient's access, exchange, or use of their EHI, the actor's practice(s) be implemented in a manner consistent with those rights—regardless of which specific law(s) afford the rights applicable in the particular circumstances.

b. Privacy Exception—When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?

We proposed to establish an exception to the information blocking provision for practices that are reasonable and necessary to protect the privacy of an individual's EHI, provided certain conditions are met (84 FR 7526). The exception and corresponding conditions were set forth in the proposed regulation text in § 171.202. We noted that any interference practice that an actor is engaged in to protect the privacy of an individual's EHI must be consistent with applicable laws and regulations related to health information privacy, including the HIPAA Privacy Rule, the HITECH Act, 42 CFR part 2, and State laws. We emphasized that this exception to the information blocking provision does not alter an actor's obligation to comply with applicable laws (84 FR 7526).

We noted that this exception is necessary to support basic trust and confidence in health IT infrastructure. Without this exception, there would be a significant risk that actors would share EHI in inappropriate circumstances, such as when an individual has taken affirmative steps to request that the EHI not be shared under certain conditions or when an actor has been unable to verify a requester's identity before sharing EHI.

We explained that this proposed exception was structured with discrete ''sub-exceptions.'' An actor's practice must qualify for a sub-exception to be covered by the exception. We noted that the sub-exceptions were, to a large extent, crafted to closely mirror privacy-protective practices that are recognized under State and Federal privacy laws. In this way, the privacy sub-exceptions to the information blocking provision recognize as reasonable and necessary those practices that are engaged in by actors to be consistent with existing laws, provided that certain conditions are met.

We proposed four sub-exceptions that address the following privacy protective practices: (1) Not providing access, exchange, or use of EHI when a State or Federal law requires that a precondition be satisfied before an actor provides access, exchange, or use of EHI, and the precondition is not satisfied (proposed in § 171.202(b)); (2) not providing access, exchange, or use of EHI when the actor is a health IT developer of certified health IT that is not covered by the HIPAA Privacy Rule in respect to a practice (proposed in § 171.202(c)); (3) a covered entity, or a business associate on behalf of a covered entity, denying an individual's request to access to their electronic protected health information (ePHI) in the circumstances provided in 45 CFR 164.524(a)(1)(2) or (3) (proposed in § 171.202(d)); and (4) not providing access, exchange, or use of EHI pursuant to an individual's request, in certain situations (proposed in § 171.202(e)) (84 FR 7526).

We proposed that an actor would need to satisfy at least one sub-exception with respect to a purportedly

privacy-protective practice that interferes with access, exchange, or use of EHI to not be subject to the information blocking provision. Each proposed sub-exception has conditions that must be met in order for an actor's practice to qualify for protection under the sub-exception (84 FR 7526).

Modification

We have changed the title of this exception from ''Exception—Promoting the privacy of electronic health information'' in the Proposed Rule (84 FR 7602) to ''Privacy Exception—When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?'' Throughout this final rule preamble, we use ''Privacy Exception'' as a short form of this title, for ease of reference. As stated in Section VIII.D of this final rule preamble, we have changed the titles of all of the exceptions to questions to improve clarity. We have edited the wording of the introductory text in § 171.202 as finalized, in comparison to that proposed (84 FR 7602) so that it is consistent with the finalized title of § 171.202. We believe these conforming changes in wording of the introductory text also improve clarity in this section.

Specific Terminology Used for the Purposes of This Proposed Exception

We noted that the proposed exception used certain terms that are defined by the HIPAA Rules [163] but that, for purposes of the exception, may have a broader meaning in the context of the information blocking provision and its implementing regulations as set forth in the Proposed Rule. We explained that, in general, the terms ''access,'' ''exchange,'' and ''use'' have the meaning in proposed § 171.102. However, we noted that in some instances we referred to ''use'' in the context of a disclosure or use of ePHI under the HIPAA Privacy Rule, in which case we explicitly stated that the term ''use'' had the meaning defined in 45 CFR 160.103. Similarly, we referred in a few cases to an individual's right of access under 45 CFR 164.524, in which case the term ''access'' should be understood in that HIPAA Privacy Rule context. We emphasized that, for purposes of section 3022 of the PHSA, however, the term ''access'' includes, but is broader than, an individual's access to their PHI as provided for by the HIPAA Privacy Rule (84 FR 7526).

Finally, we noted that the term ''individual'' is defined by the HIPAA Rules at 45 CFR 160.103. Separately, under the information blocking enforcement provision, we noted that the term ''individual'' is used to refer to actors that are health IT developers of certified health IT, HINs, or HIEs (see section 3022(b)(2)(A) of the PHSA). We clarified that for purposes of this exception (and only this exception), we used neither of these definitions. Instead, the term ''individual'' encompassed any or all of the following: (1) An individual defined by 45 CFR 160.103; (2) any other natural person who is the subject of EHI that is being accessed, exchanged or used; (3) a person who legally acts on behalf of a person described in (1) or (2), including as a personal representative, in accordance with 45 CFR 164.502(g); or (4) a person who is a legal representative of and can make health care decisions on behalf of any person described in (1) or (2); or (5) an executor or administrator or other person having authority to act on behalf of the deceased person described in (1) or (2) or the individual's estate under State or other law.

We clarified that (2) varies from (1) because there could be individuals who could be the subject of EHI that is being accessed, exchanged, or used under (2), but who would not be the subject of PHI under (1). For example, an actor which is not a covered entity or business associate as defined under HIPAA such as a health IT developer of certified health IT may access, exchange or use a patient's electronic health information; however this ''health information'' would not meet the definition of PHI, but nonetheless, would be subject to this regulation.

We also clarified that (3) encompasses a person with *legal* authority to act on behalf of the individual, which includes a person who is a personal representative as defined under the HIPAA Privacy Rule. We explained that we included the component of *legal* authority to act in (3) because the HIPAA Privacy Rule gives rights to parents or legal guardians in certain circumstances where they are not the ''personal representative'' for their child(ren). For instance, a non-custodial parent who has requested a minor child's medical records under a court-ordered divorce decree may have legal authority to act on behalf of the child even if he or she is not the child's ''personal representative.'' Further, we noted that in limited circumstances and if permitted under State law, a family member may have *legal* authority to act on behalf of a patient to make health care decisions in emergency situations even if that family member may not be the ''legal representative'' or ''personal representative'' of the patient.

We noted that we adopted this specialized usage to ensure that the Privacy Exception extends protection to information about, and respects the privacy preferences of, *all* individuals, not only those individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates (84 FR 7526 and 7527).

Interaction Between Information Blocking, the Exception for Promoting the Privacy of EHI, and the HIPAA Privacy Rule

We stated in the Proposed Rule that we consulted extensively with the HHS Office for Civil Rights (OCR), which enforces the HIPAA Privacy, Security and Breach Notification Rules, in developing proposals to advance our shared goals of preventing information blocking for nefarious or self-interested purposes while maintaining and upholding existing privacy rights and protections for individuals. We noted that the proposed exception for promoting the privacy of EHI (also referred to as the ''privacy exception'') operates in a manner consistent with the framework of the HIPAA Privacy Rule. We explained that we designed the sub-exceptions to ensure that individual privacy rights are not diminished as a consequence of the information blocking provision, and to ensure that the information blocking provision does not require the use or disclosure of EHI in a way that would not be permitted under the HIPAA Privacy Rule. We emphasized that our intent was that the information blocking provision would not conflict with the HIPAA Privacy Rule. We noted that the sub-exception proposed in § 171.202(d) reflects a policy that an actor's denial of access to an individual consistent with the limited conditions for such denials that are described in the HIPAA Privacy Rule at 45 CFR 164.524(a)(1)(2) and (3), is reasonable under the circumstances (84 FR 7527).

We also noted that the information blocking provision may operate to require that actors provide access, exchange, or use of EHI in situations that the HIPAA Rules would not require access of similar information. This is because the HIPAA Privacy Rule permits, but does not require, covered entities to disclose ePHI in most circumstances. We explained that the information blocking provision, on the other hand, requires that an actor provide access to, exchange, or use of EHI unless they are prohibited from

[163] 45 CFR part 160 and subparts A, C, and E of part 164.

doing so under an existing law or are covered by one of the exceptions. As an illustration, we noted that the HIPAA Privacy Rule permits health care providers to exchange ePHI for treatment purposes but does not require them to do so. Under the information blocking provision, unless an exception to information blocking applies, or the interference is required by law, a primary care provider would be required to exchange ePHI with a specialist who requests it to treat an individual who was a common patient of the provider and the specialist, even if the primary care provider offered patient care services in competition with the specialist's practice, or would usually refer its patients to another specialist due to an existing business relationship (84 FR 7527).

Promoting Patient Privacy Rights

We stated that the information blocking provision would not require that actors provide access, exchange, or use of EHI in a manner that is not permitted under the HIPAA Privacy Rule or other laws. As such, the privacy-protective controls existing under the HIPAA Rules would not be weakened by the information blocking provision. Moreover, we described that we structured the Privacy Exception to ensure that actors can engage in reasonable and necessary practices that advance the privacy interests of individuals (84 FR 7527).

We explained that unless required by law, actors should not be compelled to share EHI against patients' expectations under applicable law or without adequate safeguards out of a concern that restricting the access, exchange, or use of the EHI would constitute information blocking. We acknowledged that this could seriously undermine patients' trust and confidence in the privacy of their EHI and diminish the willingness of patients, providers, and other entities to provide or maintain health information electronically. In addition, we noted that such outcomes would undermine and not advance the goals of the information blocking provision and be inconsistent with the broader policy goal of the Cures Act to facilitate trusted exchange of EHI. We stated that trusted exchange requires not only that EHI be shared in accordance with applicable law, but also that it be shared in a manner that effectuates individuals' expressed privacy preferences. We noted that an individual's expressed privacy preferences will not be controlling in all cases. An actor will not be able to rely on an individual's expressed privacy preference in circumstances where the access, exchange, or use is required by law (84 FR 7527).

For these reasons, we proposed that the sub-exception in § 171.202(e) would generally permit an actor to give effect to individuals' expressed privacy preferences, including their desire not to permit access, exchange, or use of their EHI. At the same time, however, we emphasized that the Privacy Exception must be tailored to ensure that protection of an individual's privacy is not used as a pretext for information blocking. Accordingly, we proposed that this exception would be subject to strict conditions (84 FR 7527).

Privacy Practices Required by Law

We stated in the Proposed Rule that because the information blocking provision excludes from the definition of information blocking practices that are required by law (section 3022(a)(1) of the PHSA), privacy-protective practices that are required by law do not implicate the information blocking provision and do not require coverage from an exception. We noted that practices that are ''required by law'' can be distinguished from other practices that an actor engages in pursuant to a law, but which are not ''required by law.'' Such laws are typically framed in a way that permit an access, exchange or use of health information to be made only if specific preconditions are satisfied but do not expressly require that the actor engage in a practice that interferes with access, exchange, or use of EHI. For example, we noted that the HIPAA Privacy Rule provides that a covered entity *may* use or disclose PHI in certain circumstances where the individual concerned has authorized the disclosure.[164] The effect of this condition is that the covered entity should not use or disclose the PHI in the absence of an individual's authorization. However, we noted that because the condition does not prohibit the actor from exchanging the EHI in all circumstances, the actor would be at risk of engaging in a practice that was information blocking unless an exception applied. For this reason, we included a sub-exception, proposed in § 171.202(b), that provided that an actor will not be engaging in information blocking if a State or Federal law imposes a precondition to the provision of access, exchange, or use, and that precondition has not been satisfied (84 FR 7527 and 7528).

Comments. Commenters recommended that we allow for EHI to be withheld if there are contractual privacy restrictions for the actor that may define conditions or limits on what the actor may do because of those contractual restrictions. In addition, some commenters suggested that contractual restrictions should be treated similarly to State and Federal privacy laws under the Privacy Exception.

Response. Please see section VIII.C.6.a (Prevention, Material Discouragement, and Other Interference) above regarding interference that discusses contracts including business associate agreements where this is discussed in depth.

Definitions in This Exception

As noted above, we stated in the Proposed Rule that we consulted extensively with the HHS Office for Civil Rights (OCR), which enforces the HIPAA Privacy, Security and Breach Notification Rules, in developing proposals to advance our shared goals of preventing information blocking for nefarious or self-interested purposes while maintaining and upholding existing privacy rights and protections for individuals (84 FR 7527).

This Privacy Exception operates in a manner consistent with the framework of the HIPAA Rules. We have finalized the sub-exceptions to ensure that individual privacy rights are not diminished as a consequence of the information blocking provision, and to ensure that the information blocking provision does not require the use or disclosure of EHI in a way that would not be permitted under the HIPAA Privacy Rule. We emphasize that our intent is that the information blocking provision would not conflict with the HIPAA Rules. As such, we added in the definitions section of this exception the term ''HIPAA Privacy Rule'' to mean 45 CFR parts 160 and 164 to improve readability and support the policy goal of alignment with the HIPAA Privacy Rule.

With regards to the definition of ''individual,'' we have finalized this definition as proposed with a minor clarification, and it is not contrary to the HIPAA Rules. We note that the term ''individual'' is defined by the HIPAA Rules at 45 CFR 160.103. Separately, under the information blocking enforcement provision, we noted that the term ''individual'' is used to refer to actors that are health IT developers of certified health IT, HINs, or HIEs (see section 3022(b)(2)(A) of the PHSA). We finalized that for purposes of this exception (and only this exception), we used neither of these definitions. Instead, the term ''individual'' encompassed any or all of the following: (1) An individual defined by 45 CFR

[164] 45 CFR 164.508 (Uses and disclosures for which an authorization is required).

160.103; (2) any other natural person who is the subject of EHI that is being accessed, exchanged or used; (3) a person who legally acts on behalf of a person described in (1) or (2), in making decisions related to health care, as a personal representative, in accordance with 45 CFR 164.502(g); (4) a person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2); or (5) an executor or administrator or other person having authority to act on behalf of a deceased person described in (1) or (2) or the individual's estate under State or other law.

To clarify, we have finalized that § 171.202(a)(2)(iii) encompasses only a person who is a personal representative as defined under the HIPAA Privacy Rule. We distinguish a ''personal representative'' defined under the HIPAA Privacy Rule from all other natural persons who are *legal* representatives and who can make health care decisions on behalf of the individual, and thus those persons are included in § 171.202(a)(2)(iv). We misstated in the Proposed Rule that the HIPAA Privacy Rule gave rights to parents or legal guardians in certain circumstances where they are not the ''personal representatives.'' We clarify in this final rule that, in limited circumstances and if permitted under State law, a family member may be the *legal* representative to act on behalf of a patient to make health care decisions in emergency situations even if that family member may not be the ''personal representative'' of the patient.

Comments. We received no comments opposing this condition of the proposed definition of ''individual'' in the Privacy Exception.

Response. We finalized and clarified that § 171.202(a)(2)(iii) refers to only persons who meet the definition of a personal representative under 45 CFR 164.502(g), and § 171.202(a)(2)(iv) refers to all other persons who are legal representatives of and can make health care decisions on behalf of any person that was proposed in § 171.202(a)(4).

Sub-Exception 1: ''Precondition Not Satisfied''

We stated in the Proposed Rule that State and Federal privacy laws that permit the disclosure of PHI often impose conditions that must be satisfied prior to a disclosure being made. In the final rule we are deleting the word ''privacy'' when it refers to laws in the regulation text in § 171.202(b) in order to alleviate any ambiguity about what is meant as a ''privacy law.''

We proposed to establish a sub-exception to the information blocking provision that recognizes that an actor will not be engaging in information blocking if the actor does not provide access, exchange, or use of EHI because a necessary precondition required by law has not been satisfied. We explained that this exception would apply to all instances where an actor's ability to provide access, exchange, or use is ''controlled'' by a legal obligation required by law that a certain condition (or multiple conditions) must be met before access, exchange, or use of the EHI may be provided. We emphasized that to be covered by this exception, the actor must comply with certain conditions, which are discussed below.

We noted that the nature of the preconditions that an actor must satisfy in order to provide access, exchange, or use of EHI will depend on the laws that regulate the actor. For example, an actor that is regulated by a restrictive State law may need to satisfy more conditions than an actor regulated by a less restrictive State law before providing access, exchange, or use of EHI (84 FR 7527 and 7528).

We requested comments generally on this proposed sub-exception. More specifically, we sought comment on how this proposed sub-exception would be exercised by actors in the context of State laws. We noted our awareness that actors that operate across State lines or in multiple jurisdictions sometimes adopt organization-wide privacy practices that conform with the most restrictive laws regulating their business. We stated that we were considering the inclusion of an accommodation in this sub-exception that would recognize an actor's observance of a legal precondition that the actor is required by law to satisfy in at least one State in which it operates. We noted that, in the event that we did adopt such an accommodation, we would also need to carefully consider how to ensure that before the use of the most stringent restriction is applied in all jurisdictions, the actor has provided all privacy protections afforded by that law across its entire business. This type of approach would ensure that an actor cannot take advantage of a more-restrictive law for the benefit of this exception while not also fulfilling the privacy-protective obligations of the law being relied on. We requested comment on whether there is a need for ONC to adopt such an accommodation for actors operating in multiple states and encouraged commenters to identify any additional conditions that should attach to the provision of such an accommodation. We also requested comment on our proposed approach to addressing variation in State laws throughout this proposed sub-exception (84 FR 7528).

We also recognized that some states have enacted laws that more comprehensively identify the circumstance in which an individual or actor can and cannot provide access, exchange, or use of EHI. We stated that we were considering to what extent health care providers that are not regulated by the HIPAA Privacy Rule, and would rely instead on State laws for this sub-exception, would be able to benefit from this sub-exception when engaging in practices that interfere with access, exchange, or use of EHI for the purpose of promoting patient privacy. We sought comment on any challenges that may be encountered by health care providers that are not regulated as covered entities under the HIPAA Privacy Rule when seeking to take advantage of this proposed sub-exception. We also sought comment on whether there exists a class of health care provider that is not regulated by *any* Federal or State law that prescribes preconditions that must be satisfied in connection with the disclosure of EHI, and whether any such class of health care provider would benefit from a sub-exception similar to that proposed in § 171.202(c) for health IT developers of certified health IT (84 FR 7529).

Comments. Several commenters recommended that actors who operate across multiple states with different preconditions for disclosure under local laws should be able to adopt uniform requirements across their organizations that satisfy the most stringent preconditions of those local laws for purposes of this sub-exception. They stated that this is appropriate because it is often difficult for organizations operating across State lines to develop different workflows for each State. However, other commenters requested that actors should be permitted to select which portions of a State law should be included in procedures implemented across all states rather than being required to provide all privacy protections afforded by that law across its entire business. Other commenters believed that it should be left to the actor's discretion to determine whether it is better to have a uniform approach across all the jurisdictions it operates in or whether a State-by-State approach is more appropriate. They mentioned that such flexibility also would align with the Department's overall goal of reducing administrative burden particularly on providers while ensuring a high degree of privacy protection for patients.

Response. We appreciate the various comments and recognize that it is difficult for organizations operating across State lines to have different workflows for each State while assuring privacy, particularly the individual's right under the HIPAA Rules to obtain their PHI. Additionally, it is important that any uniform policies and procedures must in fact be implemented across an actor's entire organization and not be applied selectively in ways which might be contrary to the information blocking provision.

Balancing these goals, this final rule provides that, except for an individual's access to their EHI as discussed below, actors may meet this sub-exception if they operate across multiple states and elect to adopt and implement uniform policies and procedures required by one State that are more restrictive (*i.e.,* provide greater privacy protections) than would otherwise be required by another specific State or Federal law. To be considered more restrictive in this context, a law might require more or different preconditions to the access, exchange, or use of EHI than Federal law or the law of another State in which the actor operates. Alternatively, an actor could comply with the preconditions of each State in which it operates on a State-by-State basis with respect to the EHI requested. These alternatives provide multi-state actors with significant flexibility without adversely impacting an individual's right to obtain EHI as described below.

An actor that operates in multiple states could either comply with the laws of each State in which it operates or comply with the most restrictive State laws in which it operates and where applicable, comply with Federal law requirements. The actor will need to document either approach in its policies and procedures in which the actor has adopted and implemented in order to meet the conditions of § 171.202(b)(1)(i) because the uniform approach will not be available to actors that operate on a case by case basis without policies and procedures as contemplated by subsection § 171.202(b)(1)(ii). Those actors without uniform policies and procedures will need to comply with each of the applicable State and Federal laws.

As noted above, the uniform policy and procedure approach to individual access requests for EHI must assure alignment with the HIPAA Privacy Rule and individual access implementation specifications to help assure that the broader policy goals for individual access to EHI are met. Specifically, when an actor receives a request by or on behalf of an individual under 45 CFR 164.524 for the individual's EHI, the actor must not impose preconditions in its policies and procedures which would affect the individual's right to access under the HIPAA Rules even when it is operating in multiple states.

We note that an actor may not inappropriately seek to use State or Federal laws as a shield against disclosing EHI. For example, we would expect that actors implement State-mandated preconditions consistently and in a non-discriminatory manner when fulfilling requests to access, exchange, or use EHI. Additionally, we caution actors who repeatedly change their privacy policies depending on the EHI requestor or the request that such actions may be considered intended to materially interfere with, prevent, or discourage the access, exchange, or use of EHI.

We note that we have modified the introductory text in § 171.202(b) for clarity and precision. The final introductory text reads as follows: ''To qualify for the exception on the basis that one or more Federal or State preconditions for providing access, exchange, or use of electronic health information have not been satisfied, the following requirements must be met . . .'' The changes to the final introductory text from the proposed introductory text (see 84 FR 7602) are not substantive and do not change the meaning of the introductory text.

We also note that we have added ''and actions'' in § 171.202(b)(3)—''For purposes of determining whether the actor's privacy policies and procedures *and actions* satisfy the requirements of subsections (b)(1)(i) and (b)(2) above when the actor's operations are subject to multiple laws which have inconsistent preconditions, they shall be deemed to satisfy the requirements of the subsections if the actor has adopted uniform privacy policies and procedures to address the more restrictive preconditions.'' We added this language for accuracy and clarity.

Comments. A commenter requested that we provide clarification on all the Federal and State privacy laws considered when developing the ''applicable State and Federal privacy laws'' threshold condition of this sub-exception. They requested that the final rule make clear that those State privacy laws that are more restrictive than Federal privacy laws (*e.g.,* 42 CFR part 2 and HIPAA) take precedence over the less stringent Federal privacy laws.

Response. As mentioned above, for clarity purposes, we have not included the word ''privacy'' in the final regulation text in § 171.202(b) in order to alleviate any ambiguity regarding what is meant as a ''privacy law.'' The HIPAA Privacy Rule provides a Federal floor of privacy protections for an individual's individually identifiable health information where that information is held by a covered entity or by a business associate of the covered entity. This sub-exception does not alter an actor's ability to comply with applicable Federal or State laws.

To illustrate this sub-exception, we provided the following examples. We note that this list of examples is not exhaustive and that preconditions required by law that control access, exchange, or use of EHI that are not listed below would still qualify under this proposed sub-exception so long as all conditions are met.

- Although the HIPAA Privacy Rule does not have individual ''consent'' requirements for uses and disclosures of PHI for purposes such as treatment, payment, and health care operations, certain Federal and State laws do require that a person provide consent before their EHI can be accessed, exchanged, or used for specific purposes. For example, some State laws require an individual's consent for uses and disclosures of EHI regarding some sensitive health conditions such as HIV/AIDS, mental health, or genetic testing. Additionally, actors that are under ''Part 2 programs,'' which means federally assisted programs (''federally assisted'' as defined in 42 CFR 2.12(b) and ''program'' as defined in 42 CFR 2.11), generally are required to obtain an individual's consent to disclose or re-disclose patient-identifying information related to the individual's substance use disorder, such as treatment for addiction. The sub-exception would operate to clarify an actor's compliance obligations in these situations. In such scenarios, it would not be considered information blocking to refuse to provide access, exchange, or use of EHI if the actor has not received the individual's consent, subject to requirements discussed herein.
- If an actor is required by law to obtain an individual's HIPAA authorization before providing access, exchange, or use of the individual's EHI, then the individual's refusal to provide an authorization would justify the actor's refusal to provide access, exchange, or use of EHI. The actor's refusal would, subject to conditions discussed herein, be protected under this sub-exception.
- The HIPAA Privacy Rule, and many State laws, permit the disclosure of PHI in certain circumstances only once the identity and authority of the person requesting the information has been verified. We acknowledge that it is

reasonable and necessary that actors take appropriate steps, consistent with Federal and State laws, to ensure that EHI is not disclosed to the wrong person or to a person who is not authorized to receive it. Where an actor cannot verify the identity or authority of a person requesting access to EHI, and such verification is required by law before the actor can provide access, exchange, or use of the EHI, the actor's refusal to provide access, exchange, or use of the EHI will, subject to the conditions discussed herein, will not be information blocking.

- Under the HIPAA Privacy Rule, a health care provider may share information with another health care provider for a quality improvement project if it has verified that the requesting entity has a relationship with the person whose information is being requested. Where the actor could not establish if the relationship existed, it would not be information blocking for the actor to refuse to provide access, exchange, or use, subject to the conditions discussed herein.

Comments. We received comments on the Privacy Exception expressing concern about whether a business associate (as defined under the HIPAA Privacy Rule) would be liable for information blocking practices for not providing access, exchange, or use of EHI because doing so would violate its business associate agreement.

Response. Please see section VIII.C.6.a. (Prevention, Material Discouragement and Other Interference) above regarding interference that discusses contracts including business associate agreements where this is discussed in depth.

Sub-Exception 1: ''Precondition Not Satisfied'': Conditions To Be Met To Qualify for This Sub-Exception

We noted that in most circumstances, an actor would be in a position to influence whether a precondition is satisfied. For example, an actor could deprive a person of the opportunity to take some step that is a prerequisite for the exchange of their EHI, could assume the existence of a fact prejudicial to the granting of access without seeking to discover the actual facts, or could make a determination that a precondition was not satisfied without properly considering or seeking all relevant information. As such, we proposed that this exception would be subject to conditions that ensure that the protection of an individual's privacy is not used as a pretext for information blocking (84 FR 7529).

We proposed that an actor can qualify, in part, for this sub-exception by implementing and conforming to organizational policies and procedures that identify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order to satisfy the precondition.

We noted that most actors are covered entities or business associates for the purposes of the HIPAA Privacy Rule, and are already required to have policies, procedures, and training programs in place that address how ePHI (as defined in 45 CFR 160.103) is used and disclosed. As such, we expected that the overwhelming majority of actors will already be in a position to meet this condition or would be able to meet this condition with modest additional effort. However, we acknowledged that some actors may not, for whatever reason, have privacy policies and practices in place, or may have implemented privacy policies and practices that do not sufficiently address the criteria to be used, and steps to be taken, to satisfy a precondition relied on by the actor. As such, we proposed to provide an alternative basis on which to qualify, in part, for this sub-exception. We proposed to permit actors to instead document, on a case-by-case basis, the criteria used by the actor to determine when the precondition will be satisfied, any criteria that were not met, and the reason why the criteria were not met (84 FR 7529).

Separately, we proposed that if the precondition that an actor purportedly needs to satisfy relies on the provision of a consent or authorization from an individual, it is a requirement for the condition(s) of this sub-exception that the actor (i) did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization and (ii) did not improperly encourage or induce the individual to not provide the consent or authorization (84 FR 7529).

Sub-Exception 1: ''Precondition Not Satisfied'': Practice Must Be Implemented in a Consistent and Non-Discriminatory Manner

We proposed that in order for a practice to qualify for this sub-exception, the practice must be implemented in a consistent and non-discriminatory manner (proposed § 171.202(b)(3)(ii)). This condition would provide basic assurance that the purported privacy practice is directly related to a specific privacy risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

We proposed that this condition requires that the actor's privacy-protective practices must be based on objective criteria that apply uniformly for all substantially similar privacy risks. We explained that an actor could not, for example, implement an organizational privacy policy that imposed unreasonably onerous requirements on a certain class of individuals or entities without a legitimate justification for doing so. We explained that this condition provides basic assurance that the purported privacy-protective practice is not being used to interfere with access, exchange, or use of EHI for other purposes to which this proposed exception does not apply (84 FR 7532).

We requested comment on this proposed condition.

Comments. Commenters agreed that having an organizational policy which outlines patient preference categories and restrictions should be created and utilized in a consistent and non-discriminatory manner for all patient requests.

Response. We agree with the commenters, and for clarity, we moved this proposed section to finalize in § 171.202(b)(1), in order to address when an actor has conformed to its organizational policies and procedures and when an actor documents on a case-by-case basis when a precondition has been satisfied. In both cases, the actor's practice must be implemented in a consistent and non-discriminatory manner. We provide the following example to illustrate the requirement that a practice must be implemented in a consistent and non-discriminatory manner.

For example, we noted an actor that offered a patient-facing software application (app) would not be able to benefit from this exception if it refused to exchange EHI with a competitor app because the individual failed to meet onerous authorization requirements that applied only to the exchange of EHI with the competitor app and did not apply to others that presented no greater privacy or security risk.

In context of this condition of the Privacy Exception, and consistent with its interpretation for information blocking exceptions defined in part 171 subpart B in general, ''consistent and non-discriminatory'' should be understood to mean that similarly situated actors whose interactions pose the same level of privacy risk should be treated consistently with one another under the actor's privacy practices. Inconsistent treatment across similarly situated actors whose interactions pose the same level of privacy risk based on

extraneous factors, such as whether they are a competitor of the actor implementing the privacy practices, would not be considered appropriate.

Sub-Exception 1: ''Precondition Not Satisfied'': Practice Must Be Tailored to the Applicable Precondition

We proposed that for actors who seek to qualify for this sub-exception, an actor's privacy-protective practice (proposed (§ 171.202(b)(3)(i)) must be tailored to the specific privacy risks that the practice actually addresses. This condition necessarily presupposes that an actor has carefully evaluated the privacy requirements imposed on the actor, the privacy interests to be managed by the actor, and has developed a considered response that is tailored to protecting and promoting the privacy of EHI. For example, we noted that the HIPAA Privacy Rule at 45 CFR 164.514(h) requires that, in certain circumstances, the disclosure of PHI is only authorized once the identity and authority of the person requesting the information has been verified. The privacy issue to be addressed in this instance is the risk that PHI will be disclosed to the wrong individual or an unauthorized person. We proposed that if an actor chooses not to provide access, exchange, or use of EHI on the basis that the actor's identity verification requirements have not been satisfied, the actor's practice must be tailored to the specific privacy risks at issue. We noted that this would require that the actor ensure that it does not impose identity verification requirements that are unreasonably onerous under the circumstances (84 FR 7531).

For the purposes of this sub-exception, we proposed that engaging in an interference on the basis that a precondition has not been satisfied would be a practice that addresses a privacy risk or interest, and so tailoring that interference to satisfy a precondition could satisfy this requirement if all of the elements are met.

We requested comment on this proposed condition.

Comments. Commenters expressed a belief that a requirement that a ''practice must be tailored to the specific privacy risk or interest being addressed'' could lead to unnecessary complexity, and that such a policy could be overly prescriptive. In addition, commenters expressed that we should provide more use cases to help providers and others better understand how this element of the sub-exception could be met.

Response. We agree. We believe that a precondition should be tailored to the applicable legal requirement and not be tied only to a privacy risk or interest. To require that an actor's practice be tailored to the specific privacy risk or interest without a legally imposed requirement could lead to overly strict as well as an ambiguous requirement. As such, we believe that it is an important policy interest that an actor carefully evaluate the State or Federal law requirements imposed upon an actor, and that the actor develop a response that is tailored to the legal precondition which protect and promote the privacy of EHI. We provide the following use case to provide a greater understanding of how this element of the sub-exception can be met.

- To meet a legal precondition whereby an actor must identify a patient before accessing, exchanging or using EHI, an actor's policy that a driver's license was the only accepted government-issued form of identification (as opposed to other types of legally acceptable forms of identification such as a valid passport) would not be a practice that is tailored to the applicable precondition legal requirement because the provider's preference for one form of government-issued identification over another does not meaningfully address this legal precondition.

We have finalized that to qualify for this sub-exception on the basis that State or Federal law requires one or more preconditions to be met before providing access, exchange, or use of EHI the precondition should be based upon the applicable legal requirements.

Sub-Exception 1: ''Precondition Not Satisfied'': Organizational Policies and Procedures or Case-by-Case Basis

We proposed that if an actor seeks to qualify for this sub-exception, in part, by implementing and conforming to organizational policies and procedures, such policies and procedures must be in writing, and specify the criteria to be used by the actor, and, if applicable, the steps that the actor will take, in order to satisfy the precondition relied on by the actor not to provide access, exchange, or use of EHI. We emphasized that it would not be sufficient for an actor to simply identify the existence of the precondition in their organizational policies and procedures.

We proposed that an actor would only be eligible to benefit from this sub-exception if it has implemented and followed its processes and policies. This would include taking reasonable steps to ensure that its workforce members and agents understand and consistently apply the policies and procedures (84 FR 7529 and 7530).

We requested comment on the proposed condition generally, and specifically, on whether an actor's organizational policies and procedures provide a sufficiently robust and reliable basis for evaluating the bona fides, reasonableness, and necessity of practices engaged in to satisfy preconditions required by State or Federal privacy laws (84 FR 7529 and 7530).

Comments. Some commenters recommended that actors should be able to have written organization-specific policies that may be more restrictive than State or Federal law and that health information networks and exchanges should be given an exemption based on their existing written governance policies. Other commenters recommended adding language indicating that organizational policies must comply with Federal, State, and local laws or that the final rule should specify that organizations should implement policies which conform to the specific State laws in which the information originates.

Response. As noted above, this final rule includes a limited exception that permits an actor that operates in more than one State to adopt uniform policies and procedures based on more restrictive provisions of State and Federal law, subject to certain conditions. ONC reiterates that an actor's organizational policies and procedures should not be used as a pretext for information blocking. For example, information blocking may exist if an actor's policies and procedures impose onerous additional privacy requirements for access, exchange or use of EHI beyond what is required by law, or where an actor repeatedly changes its privacy policies and procedures to circumvent this exception. Further, the actor's policies and procedures must be tailored and must be implemented in a consistent and non-discriminatory manner.

We do not agree that health information exchanges or networks should be given a blanket exemption based on their existing written governance policies because that could lead to a situation involving information blocking if those policies imposed conditions that conflict with the information blocking provision. Secondly, we expect that an actor's organizational policies will conform with applicable laws, including the information blocking provision, so it is not necessary to further require actors to implement policies which conform to the specific laws, including the law of

the State in which the information originated.

Documenting Criteria and Rationale

If an actor's practice does not conform to an actor's organizational policies and procedures as required by § 171.202(b)(1)(i), we proposed that an actor can seek to qualify for this sub-exception, in part, by documenting how it reached its decision that it would not provide access, use, or exchange of EHI on the basis that a precondition had not been satisfied. We proposed that such documentation must be created on a case-by-case basis proposed in § 171.202(b)(1)(ii). We noted that an actor will not satisfy this condition if, for instance, it sought to document a general practice that it had applied to all instances where the precondition had not been satisfied. Rather, we stated that the record created by the actor must address the specific circumstances of the specific practice (or interference) at issue.

We proposed that the record created by the actor must identify the objective criteria used by the actor to determine when the precondition is satisfied. Consistent with the condition to this sub-exception that the practice must be tailored to the privacy interest at issue, those criteria would need to be directly relevant to satisfying the requirement. For example, we explained that if the requirement at issue was the provision of a valid HIPAA authorization, the actor's documented record should reflect, at minimum, that the authorization would need to meet each of the requirements specified for a valid authorization at 45 CFR 164.508(c). The record would then need to document the criteria that had not been met, and the reason why it was not met. We noted that the actor could record that the authorization did not contain the name or other specific identification of the person making the request because the authorization only disclosed the person's first initial rather than a first name, and the actor had records about multiple people with that same initial and last name.

We noted that this condition would provide the transparency necessary to demonstrate whether the actor has satisfied the conditions applicable to this exception. Moreover, we noted that it will help ensure that a decision to not provide access, exchange, or use of EHI is considered and deliberate, and therefore reasonable and necessary (84 FR 7530).

We requested comment on this proposed condition.

Comments. Commenters requested that we should provide specificity on what type of documentation would suffice to demonstrate that an actor met this sub-exception. Commenters were concerned that these were stringent documentation requirements and that provider practices may inadvertently trigger a violation of information blocking. Other commenters suggested that we should remove or consider reducing onerous requirements for documentation for qualifying for the privacy sub-exceptions, and other commenters requested specification on what form the documentation must be and to specify whether existing documentation required by the HIPAA Rules (*e.g.,* patient informed consent and authorization forms, Notice of Privacy Practices, Security Risk Analysis, etc.) would satisfy the documentation requirements under this Privacy Exception.

Response. The documentation requirements are for the actor to comply with applicable State and Federal laws and to assure that after the fact rationalizations are not used to justify practices that have already occurred, consistent with the policy objectives of the information blocking provision.

To finalize the documentation requirements we looked to OIG, which has authority under section 3022(b) of the PHSA to investigate any claim that an actor engaged in information blocking. OIG regulations in other contexts include a writing requirement. For example, OIG has promulgated the ''safe harbors'' provisions at 42 CFR 1001.952, specifying various payment and business practices that would not be subject to sanctions under the Anti-Kickback Statute. Several of these safe harbors include a writing requirement to document in writing an agreement, lease, or other transaction. These documentation requirements do not often get into specific terms or requirements, but rather tend to be more general in nature. However, the documentation requirements do provide indicia of evidence that an entity has met the requirements of the safe harbor provisions.

In addition, we considered the documentation requirements in the HIPAA Rules. The HIPAA Privacy Rule at 45 C.F.R 164.530 (j) requires a covered entity to maintain its policies and procedures in written or electronic form for six years from the date of its creation or the date when it last was in effect, whichever is later. In our review of the OIG and HIPAA regulations, we believe that the documentation requirement for this sub-exception is consistent with the safe harbor and HIPAA Privacy Rule documentation requirements. Further, we do not believe this documentation requirement would be onerous.

Therefore, we have finalized the following requirements for this sub-exception. An actor must document its organizational policies and procedures and specify the criteria used by the actor and as applicable, the steps that the actor will take to satisfy the precondition. Such steps may include providing the actor's workforce members with training on those policies and procedures. Alternatively, we have finalized a requirement an actor must document on a case-by-case basis how it reached its decision that it would not provide access, use, or exchange of EHI on the basis that a precondition had not been satisfied, including the criteria it used to determine when the precondition is satisfied. That is, an actor can provide documentation that identifies the objective criteria that the actor applied in order to determine whether the precondition had been satisfied. Additionally, the actor must provide documentation that the practice is tailored to those criteria that are directly relevant to satisfying the precondition.

Sub-Exception 1: ''Precondition Not Satisfied'': Precondition Relies on a Consent or Authorization

We proposed that if the precondition that an actor purports to rely upon requires the provision of a consent or authorization from an individual, it is a condition of this sub-exception that the actor must have done all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide that consent or authorization. We noted that this requirement will be relevant when, for example, a State privacy law or the HIPAA Privacy Rule requires an individual to provide consent and/or a HIPAA authorization before identifiable information can be accessed, exchanged, or used for specific purposes.

We stated that we were considering addressing this condition in further detail, whether by way of additional guidance or in regulation text. To this end, we requested comments regarding what actions an actor should take, within the actor's control, to provide an individual with a meaningful opportunity to provide a required consent or HIPAA authorization, and whether different expectations should arise in the context of a consent versus a HIPAA authorization. Separately, we proposed that to qualify for this sub-exception, to the extent that the precondition at issue was the provision of a consent or HIPAA authorization by an individual, the actor must not have

improperly encouraged or induced the individual to not provide the consent or HIPAA authorization. We clarified that this does not mean that the actor cannot inform an individual about the advantages and disadvantages of exchanging EHI and any associated risks, so long as the information communicated is accurate and legitimate. However, we noted that an actor would not meet this condition in the event that it misled an individual about the nature of the consent to be provided, dissuaded individuals from providing consent in respect of disclosures to the actor's competitors, or imposed onerous requirements to effectuate consent that were unnecessary and not required by law.

We requested comment on whether the proposed condition requiring the provision of a meaningful opportunity and prohibiting improper encouragement or inducement should apply to preconditions beyond the precondition that an individual provide consent or authorization. We requested comment on whether the conditions specified for this sub-exception, when taken in total, are sufficiently particularized and sufficiently strict to ensure that actors that are in a position to influence whether a precondition is satisfied will not be able to take advantage of this sub-exception and seek protection for practices that do not promote the privacy of EHI. We also requested comment on whether we should adopt a more tailored approach to conditioning the availability of this exception. For example, we noted that we were considering whether different conditions should apply depending on: (i) The nature of the EHI at issue; (ii) the circumstances in which the EHI is being access, exchanged, or used; (iii) the interest being protected by the precondition; or (iv) the nature of the precondition to be satisfied. We encouraged commenters to identify scenarios in which the application of the conditions applicable to this sub-exception, as proposed, give rise to unnecessary burden, or would require activities that do not advance the dual policy interests of preventing information blocking and promoting privacy and security (84 FR 7530 and 7531).

Comments. Some commenters noted that the entire condition was too vague and generally inconsistent with current standard industry relationships and practices. Several commenters suggested that the burden to obtain the consent should be on the organization requesting the data rather than on the organization that holds the data. However, commenters who suggested this often acknowledged that modifying our proposal to fit their suggestion would require an actor to receive assurances that consents are legitimate and in their possession before sharing any data. These commenters often noted that it was not clear how recipients of health care data subject to authorizations and consent would be expected to provide individuals with a meaningful opportunity to consent if they do not have an existing relationship with that individual or means to contact that individual. A few commenters recommended modifying this condition so that an actor that does not have a direct relationship with patients is not required to obtain patient consent or authorization.

Response. We agree with the commenters and have attempted to address concerns about vagueness and consistency with industry practices and relationships. This finalized sub-exception requires the actor to have used reasonable efforts within its control if the actor has already received a form of required consent or authorization that does not meet all applicable requirements. Specifically, the actor must have used reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all applicable requirements or have provided other reasonable assistance with respect to the deficiencies. In effect, this places more of an obligation on the party requesting the EHI and the individual to attempt to satisfy the precondition by providing a consent or authorization. This final rule does not require the actor that receives the request to obtain a patient's consent or authorization to do all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization. Rather, the final rule requires that the actor is obligated to take reasonable steps to provide a sufficient consent or authorization form or other reasonable assistance.

Providing other reasonable assistance does not mean that the actor needs to ''chase'' the individual to obtain a sufficient consent or authorization. Such other reasonable assistance might include notifying the individual of elements that are missing in the consent or authorization initially provided, such as a witness or an expiration date if legally required.

We believe that setting the standard for an actor's actions with respect to an insufficient consent or authorization at reasonable efforts is an appropriate standard to use because it aligns with the case-by-case approach that is captured in the information blocking provision that is the subject of this final rule.

We recognize that actors must accommodate variations in laws across the states in which they operate. As discussed above, this final rule provides flexibility to multi-state providers with respect to how they may structure uniform policies and procedures regarding consents and authorizations provided that they do in fact apply them. We also recognize that some types of actors will not have the necessary legal rights or the technical access to detailed patient information to determine if a consent or authorization is required as a precondition.

We intend that each actor must do what is reasonable and what is within its control. This applies to actors who are providers that have a direct patient relationship and to actors that are supporting a health care provider with respect to an insufficient consent or authorization that must also use reasonable efforts to avoid possible information blocking.

A health information network that receives an insufficient consent or authorization might find that this sub-exception helpful if it does not have lawful access to the individual's information to determine what consent might be required under State or Federal confidentiality laws that apply to information about mental health, substance abuse, HIV status or other highly confidential diseases or conditions. We also note that if a network is not able to review such information under applicable law, providing a corrected consent would not be within its control.

Comments. Many commenters were concerned that our definition of ''meaningful opportunity'' was too broad. These few commenters suggested that, as proposed, our definition of ''meaningful opportunity'' could place a significant burden on providers. Specifically, these commenters suggested that adding a ''meaningful'' opportunity to consent to the patient, with its requisite new forms and procedures, would add new burdens on actors without appearing to solve any existing problems.

One commenter recommended that we modify this requirement to include a reasonable opportunity for the provider to obtain the individual's consent the next time the patient visits the office if the patient is not present in the office to provide consent.

Response. We appreciate the comments that we have received on the meaningful opportunity provision. After considering the comments, we

eliminated the ''meaningful opportunity'' provision in this final rule. However, this sub-exception still requires the actor to use reasonable efforts within its control and to provide reasonable assistance, which might include explaining the required elements of a consent or authorization, or providing a witness if required by law and requested by the patient at an office visit with the actor.

However, the requirement of reasonable efforts is based on an assumption that actors may not use the protection of an individual's privacy as pretext for information blocking. If a requestor provides or obtains some form of patient documented consent or authorization that requires the actor's assistance to satisfy elements that are not required by law and the actor does not provide such assistance, the actor may be engaged in information blocking.

We recognize that meeting certain preconditions may be outside the direct control of the provider. For example, the actor may have a pre-existing consent form from the individual that needs to be modified due to a change in applicable law. The actor may have a very difficult time tracking down a former patient to provide the updated consent form. In most cases, it would be reasonable to mail or email the updated form to the patient's last address on the actor's records or present it to the patient at visit scheduled in the near future. If the patient cancels the visit, it may be reasonable for the actor to wait to obtain the consent until the next time the patient visits the physical location of the actor's office, so long as the actor explains the insufficiency and provides a sufficient consent form at the next visit.

Comments. Commenters have mentioned that a health information network (HIN) does not have operational control over or visibility into the detailed decision-making of an individual's consent or authorization of its participants, and they argue that an actor such as a HIN should not be obligated to review or confirm the individuals' consent or authorization, and that such confirmation is a requirement of the health care provider because health care provider has a direct relationship with the patient.

Response. We believe that actors such as a HIN do have the obligation to comply with the conditions of this sub-exception. We have taken the approach that each actor must use its ''reasonable efforts'' and focus on what reasonable steps they can take to provide their reasonable efforts. We do not, however, believe that actors who have a direct patient relationship would have a higher standard of reasonable efforts than those actors such as HINs which do not have a direct relationship with a patient and are acting on behalf of a health care provider. However, even actors that do not have a direct relationship with an individual, should use their reasonable efforts for the activities under their control as it relates to supporting the providing or obtaining of a consent or authorization.

Comments. Commenters expressed concerns that actors would be required to create new policies beyond HIPAA aimed at offering patients a ''meaningful'' opportunity to consent, and as a result, more challenges than solutions would result from this policy. Commenters noted unnecessary administrative burdens, confusion with HIPAA requirements, and complexity for actors as some of the possible challenges.

Response. As noted above, the ''meaningful opportunity'' requirement was not included in this final rule.

Comments. Many commenters expressed the opinion that actors meeting certain preconditions may be outside the direct control of the actor and recommended that examples should be provided about what actions are sufficient to meet the ''reasonably necessary'' standard. Another commenter argued that the reasonably necessary standard for the meaningful opportunity requirement only stands to further aggravate the burdensome nature of more stringent privacy laws. Other commenters were concerned that the requirement that the actor ''did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization'' was too rigid a requirement and that even if one possible action was not done, the exception would not apply. Other commenters argued that this standard was an extremely onerous requirement and contradicts the stated intent of reducing the overall administrative burden on health care practices.

Response. As noted above, the standard is now based on reasonable efforts within the actor's control, and it applies only after the actor receives a consent or authorization form that does not satisfy all applicable conditions. We believe that this change addresses the comments noted above. We note that we have slightly modified the terminology used in § 171.202(b)(2)(i). We proposed ''a form of consent or authorization'' (84 FR 7602) and have change that language in the final rule to ''a consent or authorization form'' for clarity. This modification does not change the meaning of § 171.202(b)(2)(i).

Comments. A commenter expressed concern to modify this exception to make it clear that a hospital or health system may claim the exception when an entity requesting patient data does not communicate that it has obtained consent.

Response. As noted above, this condition of the sub-exception applies only after an insufficient consent or authorization is received. This condition of the sub-exception in the final rule does not apply when the actor has not received anything regarding the individual's consent or authorization. In such cases, the actor would not be required to communicate to the entity requesting the EHI that the actor has not obtained the individual's consent or authorization in order to meet this sub-exception.

Comments. A commenter argued that actors should provide the individual with a ''reasonably convenient opportunity'' to provide the consent or authorization, rather than requiring ''all things reasonably necessary within its control'' to provide consent or authorization. The commenter noted that where entities make the request on behalf of the individual, the actor making the request should facilitate the gathering of the consent or authorization.

Response. As noted above, both the ''reasonable opportunity'' and the ''all things reasonably necessary'' language are not included in this final rule, but the actor must satisfy the reasonable efforts standard when an insufficient consent or authorization has been received. This might include providing a correct form or reasonable assistance to the individual to solve any consent or authorization documentation problems necessary to address the insufficiency.

Sub-Exception 1: Precondition Not Satisfied: Did Not Improperly Encourage or Induce the Individual To Withhold the Consent or Authorization

We proposed that to qualify for this sub-exception, to the extent that the precondition at issue was the provision of a consent or authorization by an individual, the actor must not have improperly encouraged or induced the individual to not provide the consent or authorization. As proposed, an actor would not meet this condition in the event that it misled an individual about the nature of the consent to be provided, dissuaded individuals from providing consent in respect of disclosures to the actor's competitors, or imposed onerous requirements to effectuate consent that

were unnecessary and not required by law.

We sought comment on whether the proposed condition requiring the provision of prohibiting improper encouragement or inducement should apply to preconditions beyond the precondition that an individual provide consent or authorization. We sought comment on whether the conditions specified for this sub-exception, when taken in total, are sufficiently particularized and sufficiently strict to ensure that actors that are in a position to influence whether a precondition is satisfied will not be able to take advantage of this sub-exception and seek protection for practices that do not promote the privacy of EHI. We also sought comment on whether we should adopt a more tailored approach to conditioning the availability of this sub-exception (84 FR 7531).

Comments. We received no comments opposing this condition applicable to practices that implement the provision of a consent or authorization from an individual to an actor.

Response. Within the sub-exception (§ 171.202(b)) applicable to practices that implement a consent or authorization, we are finalizing in § 171.202(b)(2)(ii) as proposed.

Sub-Exception 2: Sub-Exception: Health IT Developer of Certified Health IT Not Covered by HIPAA

The sub-exception we proposed in § 171.202(b) recognized as reasonable and necessary the activities engaged in by actors consistent with the controls placed on access, exchange, or use of EHI by Federal and State laws. We noted that the sub-exception was limited to actors that are subject to those Federal and State laws; an actor that is not regulated by HIPAA cannot benefit from the exception proposed in § 171.202(b).

We proposed to establish a sub-exception to the information blocking provision that would apply to actors that are health IT developers of certified health IT but not regulated by the HIPAA Privacy Rule in respect to the operation of the actor's health IT product or service (referred to as ''non-covered actors'' for this sub-exception). We noted that we expect that the class of actors to which this proposed sub-exception applies will be very small. We explained that the vast majority of health IT developers of certified health IT operate as business associates to covered entities under HIPAA. As business associates, they are regulated by the HIPAA Privacy Rule, and may be able to benefit from the exception proposed in § 171.202(b) to the extent that the HIPAA Privacy Rule (or applicable State law) imposes preconditions to the provision of access, exchange, or use of EHI. However, we recognized that direct-to-consumer health IT products and services are a growing sector of the health IT market. The privacy practices of consumer-facing health IT products and services are typically regulated by the Federal Trade Commission Act (FTC Act). However, while the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce (15 U.S.C. 45(a)(1)), it does not prescribe specific privacy requirements.[165]

We proposed that where a health IT developer of certified health IT offers a health IT product or service not regulated by the HIPAA Privacy Rule, such product or service is still subject to the information blocking provision. We wanted to ensure that such non-covered actors under the information blocking provisions are able to avail themselves of the Privacy Exception. As such, we proposed that an entity that is not covered by HIPAA will not engage in information blocking if the actor declines to provide access, exchange, or use of EHI where the practice implements a process that is described in the actor's organizational privacy policy and has been disclosed to any individual or entity that uses the actor's health IT. We proposed this sub-exception in § 171.202(c) which sets forth additional detail (84 FR 7532).

In the final rule, we have finalized that when engaging in a practice that promotes the privacy interests of an individual, the non-covered actor must implement the practice according to a process described in the organizational privacy policies, disclosed those organizational privacy policies to the individuals and entities that use the actor's product or service before they agreed to use them, and the non-covered actor's organizational privacy policies must: (1) Comply with applicable State or Federal laws; (2) be tailored to the specific privacy risk or interest being addressed; and (3) be implemented in a consistent and non-discriminatory manner. Public comments on specific conditions are summarized below, in context of each condition proposed. We believe our responses to these comments furnish the clarity non-covered actors need to understand the conditions of the sub-exception finalized in § 171.202(c).

[165] *See* HHS, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA, https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.*

Practice Must Implement Privacy Policy

We proposed that in order to qualify for this sub-exception, the practice engaged in by the non-covered actor—the interference with access, exchange, or use of EHI—must also implement a process described in the actor's organizational privacy policy. This requires that a non-covered actor must have documented in detail in its organizational privacy policy the processes and procedures that the actor will use to determine when the actor will not provide access, exchange, or use of EHI. For example, we explained that a non-covered actor that proposed to require the provision of written consent for the use or disclosure of EHI would need to describe in its organizational privacy policy the processes and procedures to be utilized by the actor to implement that privacy-protective practice so that the practice be considered reasonable and necessary and qualify for this sub-exception. We noted that compliance with this condition ensures that the sub-exception recognizes only legitimate practices that have been tailored to the privacy needs of the individuals that use the non-covered actor's health IT, and does not recognize practices that are a pretext or after-the-fact rationalization for actions that interfere with access, exchange, or use of EHI.

We also proposed that the non-covered actor's practice must implement its documented organizational privacy policy. We noted that practices that diverge from an actor's documented policies, or which are not addressed in an actor's organizational privacy policy, would not qualify for this proposed sub-exception (84 FR 7532).

Policies Must Have Been Disclosed to Users

We proposed that a non-covered actor that seeks to benefit from the sub-exception must also ensure that it has previously disclosed the privacy-protective practice to the individuals and entities that use, or will use, the health IT. These users are affected by the practices engaged in by a non-covered actor but may otherwise have no visibility of the non-covered actor's approach to protecting the privacy of EHI. We noted that we expect that non-covered actors will seek to satisfy this condition by using a privacy notice.[166]

[166] ONC has provided a Model Privacy Notice (MPN) that is a voluntary, openly available resource designed to help developers clearly convey information about their privacy and security policies to their users. The MPN provides a snapshot of a company's existing privacy practices encouraging transparency and helping consumers make informed choices when selecting products.

We emphasized that the disclosure must be meaningful. In assessing whether a non-covered actor's disclosure was meaningful, we explained that regard will be paid to whether the disclosure was in plain language and conspicuous, including whether the disclosure was located in a place, and presented in a manner, that is accessible and obvious to the individuals and entities that use, or will use, the health IT.

We proposed that to qualify for this sub-exception, a non-covered actor would not be required to disclose its organizational privacy policy to its customers or to the public generally. Rather, the non-covered actor need only describe, with sufficient detail and precision to be readily understood by users of the non-covered actor's health IT, the privacy-protective practices that the non-covered actor has adopted and will observe. We explained that this is necessary because a non-covered actor that is not subject to prescribed privacy standards in connection with the provision of health IT will have significant flexibility in the privacy-protective practices that it adopts. If a non-covered actor is not required to inform the individuals and entities that use, or will use, the health IT, about the privacy-protective practices that it will implement in its product, or when providing its service, we noted that there is a risk that the sub-exception will give deference to policies and processes that are post hoc rationalizations used to justify improper practices. We stated that this condition also serves as a check on the nature of the interferences that a non-covered actor writes into its organizational privacy policies; transparency will help to ensure that a non-covered actor takes a balanced approach to protecting privacy interests on one hand, and pursuing business interests that might be inconsistent with the information blocking provision, on the other hand (84 FR 7533).

We proposed that it will be a matter for non-covered actors to determine the most appropriate way to communicate its privacy practices to users. We noted that it would be reasonable that non-covered actors would, at a minimum, post their privacy notices, or otherwise describe their privacy-protective practices, on their websites (84 FR 7533).

The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies. See *https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn.*

Practice Must Be Tailored to Privacy Risk and Implemented in a Non-Discriminatory Manner

Finally, we proposed that in order for a practice to qualify for this sub-exception, an actor's practice must be tailored to the specific privacy risks that the practice actually addresses and must be implemented in a consistent and non-discriminatory manner.

We requested comment on this proposed sub-exception generally. Specifically, we requested comment on whether HIEs or HINs would benefit from a similar sub-exception. We also requested comment on whether the conditions applicable to this sub-exception are sufficient to ensure that non-covered actors cannot take advantage of the exception by engaging in practices that are inconsistent with the promotion of individual privacy. We also requested comment on the level of detail that non-covered actors should be required to use when describing their privacy practices and processes to user of health IT (84 FR 7533).

Comments. Some commenters believed that this sub-exception could be helpful for those developing their own health IT tools, which are outside of the electronic health record.

Response. We agree that this sub-exception would be helpful for those developing their own health IT tools. The sub-exception address those certified Health IT products not covered by HIPAA and would have in place an organizational privacy policy which is tailored to a specific privacy risk or interest.

Comments. Commenters noted that regarding the sub-exception proposed for ''non-covered actors'' that develop patient-facing health IT, they urged the need to balance the conditions of this sub-exception with the requirements placed on actors who institute organizational privacy policies.

Response. We appreciate the comment. In order to meet this sub-exception, the organizational privacy policies of a non-covered actor would need to comply with other applicable State and Federal laws. Further, we have finalized that non-covered actors that seek to benefit from this sub-exception must also ensure that their organizational privacy policies are disclosed to the individuals and entities that use their product or service before the individuals and entities agree to use them. The organizational privacy policies are important for transparency for users of the certified technologies and to demonstrate compliance with applicable State and Federal laws. Non-covered actors have the discretion to determine the most appropriate way to communicate their privacy policies to individuals and users. As stated above and in the Proposed Rule (84 FR 7533), it would be reasonable for non-covered actors to, at a minimum, post their privacy notices, or otherwise describe their privacy-protective practices, on their websites.

Comments. A few commenters stated that it is unclear whether application developers are subject to HIPAA if they are not business associates or covered entities.

Response. We appreciate the feedback. Where application developers are not defined as a covered entity or business associate as defined under 45 CFR 160.103, then the application developer is not covered under the HIPAA Privacy Rule or HIPAA Security Rule.

Comments. Some commenters expressed concern that data will be made available to third-party application suppliers, commercial analytics companies, and/or entities that are not governed by HIPAA and that such availability of data would not serve patients' best interests and could result in potential misuse of patient data.

Response. We appreciate the feedback and agree that an actor who is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule must comply with all applicable State and Federal laws, including the FTC Act. Further, such actors must have an organizational privacy policy that is tailored to the privacy risk or interest being addressed in order to meet this sub-exception. We emphasize that where a health IT developer of certified health IT offers a health IT product or service not regulated by the HIPAA Privacy Rule, such product or service is subject to the information blocking provision. Our goal is to ensure that non-covered actors that engage in reasonable and necessary privacy-protective practices that interfere with the access, exchange, or use of EHI could seek coverage under the sub-exception.

Comments. Some commenters stated that actors that are not covered by HIPAA should make their privacy policies publicly available. Other commenters did not believe that the Proposed Rule fully addressed patient and consumer privacy protections.

Response. We appreciate the comments. We believe that it is important that users know what to expect when electing to use a non-covered actor's product or service.

Sub-Exception 3: Denial of an Individual's Request for Their Electronic Protected Health Information in the Circumstances Provided in 45 CFR 164.524(a)(1) and (2)

We proposed a limited sub-exception to the information blocking provision that would permit a covered entity or business associate to deny an individual's request for access to their PHI in the circumstances provided under 45 CFR 164.524(a)(1) (2) and (3). We noted that this exception would avoid a potential conflict between the HIPAA Privacy Rule and the information blocking provision. Specifically, the HIPAA Privacy Rule contemplates circumstances under which covered entities, and in some instances business associates, may deny an individual access to PHI and distinguishes those grounds for denial which are reviewable from those which are not. We proposed that this exception applies to both the ''unreviewable grounds'' and ''reviewable grounds'' of access. We noted that the ''unreviewable grounds'' for denial for individuals include situations involving: (1) Certain requests that are made by inmates of correctional institutions; (2) information created or obtained during research that includes treatment, if certain conditions are met; (3) denials permitted by the Privacy Act; and (4) information obtained from non-health care providers pursuant to promises of confidentiality. In addition, we noted that two categories of information are expressly excluded from the HIPAA Privacy Rule individual right of access: (1) Psychotherapy notes, which are the notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session and that are maintained separate from the rest of the patient's medical record; and (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[167]

We noted the ''reviewable grounds'' of access as described in § 164.524(a)(3), which provides that a covered entity may deny access provided that the individual is given a right to have such denials reviewed under certain circumstances. We explained that one such circumstance is when a licensed health care professional, in the exercise of professional judgment, determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. In addition, we noted that if access is denied, then the individual has the right to have the denial reviewed by a licensed health professional who is to act as a reviewing official and did not participate in the original decision to deny access (see generally 45 CFR 164.524(a)(3)) (84 FR 7533 and 7534).

As mentioned above with regards to the harm exception (§ 171.201) our purpose is to avoid unnecessary complexity. By including the ''reviewable grounds'' of 45 CFR 164.524(a)(3) in the harm exception at § 171.201, we align these regulations in a way that streamlines compliance for actors subject to the HIPAA Privacy Rule and this regulation. We removed the 45 CFR 164.524(a)(3) reference in the privacy sub-exception in § 171.202(d) and moved it to the harm exception in § 171.201 in order to promote clarity and alignment with the inter-relationship between this final rule and the HIPAA Privacy Rule.

In restricting this privacy sub-exception to only ''unreviewable grounds'' in 45 CFR 164.524(a)(1) and (2), we clarify the regulation text so that it is immediately clear that actors who are covered entities, and in some instances business associates, may deny an individual access to EHI of the individual and such denials would not provide an opportunity for review of the denial under certain circumstances. We clarify in the final rule that if an individual requests EHI under the right of access provision under 45 CFR 164.524(a)(1) from an actor that must comply with 45 CFR 164.524(a)(1), the actor's practice must be consistent with 45 CFR 164.524(a)(2). These ''unreviewable grounds'' are related to specific privacy risks or interests and have been established for important public policy purposes, such as when a health care provider is providing treatment in the course of medical research or when a health care provider is acting under the direction of a correctional institution.

Unlike the ''unreviewable grounds,'' the ''reviewable grounds'' that are finalized § 171.201 are directly related to the likelihood of harm to a patient or another person and requires that actors seeking to avail themselves of this exception must have a reasonable belief that the practice will substantially reduce a risk of harm that would otherwise arise from the specific access, use, or exchange of EHI affected by the practice, and the harm must be one that would be cognizable under 45 CFR 164.524(a)(3) as a basis for denying an individual's right of access to their PHI in analogous circumstances. In other words, the ''reviewable grounds'' of access as described in 45 CFR 164.524(a)(3), provides that a covered entity may deny access provided that the individual is given a right to have such denials reviewed when a licensed health care professional, in the exercise of professional judgment, determines that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. In addition, we noted that if access is denied, then the individual has the right to have the denial reviewed by a licensed health professional who is to act as a reviewing official and did not participate in the original decision to deny access and the risk to be reduced must be one that would otherwise arise from the specific access, use, or exchange of EHI affected by the practice.

We proposed that if an actor who is a covered entity or its business associate denies an individual's request for access to their PHI on the basis of these unreviewable grounds, and provided that the denial of access complies with the requirements of the HIPAA Privacy Rule in each case, then the actor would qualify for this exception and these practices would not constitute information blocking (84 FR 7534).

We requested comment on this proposed sub-exception.

Comments. Commenters were concerned that HINs that are business associates may not be authorized to provide individual access on the behalf of covered entity. Further, commenters sought clarification that this sub-exception would also apply in circumstances where as a business associate, the HIN would deny the individual's request for access because of its obligations as a business associate.

Response. We share this concern. To meet this privacy sub-exception, if an individual requests their ePHI under 45 CFR 164.524(a)(1), the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1) or (2). That is, an actor that is a covered entity may deny an individual's request for access to all or a portion of the PHI and must meet its requirements under the HIPAA Privacy Rule. As we discussed earlier, an individual's right under the HIPAA Privacy Rule to access PHI about themselves includes PHI in a designated record set maintained by a business associate on behalf of a covered entity. However, if the same PHI that is the subject of an access request is maintained in both the designated record set of the covered entity and the designated record set of the business associate, the PHI need only be

[167] See 45 CFR 164.501; 45 CFR 164.524 (a)(1)(i) and (ii).

produced once in response to the request for access.[168]

Comments. Commenters requested clarification that covered entities and business associates could meet this sub-exception when conducting clinical research with a blinded or masked designed. The EHI is typically 'tagged' as part of a blinded or masked research during a research study.

Response. To meet this privacy sub-exception, if an individual requests their ePHI under 45 CFR 164.524(a)(1), the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1) or (2). Under certain limited circumstances under the Privacy Rule, a covered entity may deny an individual's request for access to all or a portion of the PHI requested. In some of these circumstances, an individual does not a right to have the denial reviewed by a licensed health care professional. It is known as ''unreviewable grounds'' for denial.[169] One of the ''unreviewable grounds'' involves individual access to ePHI in a research study. An actor may deny access to an individual provided that the requested PHI is in a designated record set that is part of a research study that includes treatment (*e.g.,* clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual's right of access can be reinstated upon completion of the research study.

Sub-Exception 4: Sub-Exception: Respecting an Individual's Request Not To Share Information

We proposed to establish an exception to the information blocking provision that would, in certain circumstances, permit an actor not to provide access, exchange, or use of EHI if an individual has specifically requested that the actor not do so. This sub-exception was proposed in § 171.202(e). We noted that this sub-exception is necessary to ensure that actors are confident that they can respect individuals' privacy choices without engaging in information blocking, and to promote public confidence in the health IT infrastructure by effectuating patients' preference about how and under what circumstances their EHI will be accessed, exchanged, and used. We recognized in the Proposed Rule that individuals may have concerns about permitting their EHI to be accessed, exchanged, or used electronically under certain circumstances. As a matter of public policy, we explained that these privacy concerns, if expressed by an individual and agreed to by an actor, would be reasonable and necessary, and an actor's conduct in abiding by its agreement would, if all conditions are met, be an exception to the information blocking provision (84 FR 7534).

We proposed that this proposed sub-exception would not apply under circumstances where an actor interferes with a use or disclosure of EHI that is required by law, including when EHI is required by the Secretary to enforce HIPAA under 45 CFR 164.502(a)(2)(ii) and 45 CFR 164.502(a)(4)(i). Stated differently, this sub-exception would not operate to permit an actor to refuse to provide access, exchange, or use of EHI when that access, exchange, or use is required by law. We noted that this sub-exception recognizes and supports the public policy objective of the HIPAA Privacy Rule, which identifies uses and disclosures of EHI for which the public interest in the disclosure of the individual's information outweighs the individual's interests in controlling the information.

We proposed that this sub-exception would permit an actor not to share EHI if the following conditions are met: (1) The individual made the request to the actor not to have their EHI accessed, exchanged, or used; (2) the individual's request was initiated by the individual without any improper encouragement or inducement by the actor; and (3) the actor or its agent documents the request within a reasonable time period.

We described that to qualify for this sub-exception, the request that the individual's EHI not be accessed, exchanged, or used must come from the individual. Moreover, the individual must have made the request independently and without any improper encouragement or inducement by the actor.

We proposed that if an individual submits a request to an actor not to disclose her EHI, and the actor agrees with and documents the request, the request would be valid for purposes of this sub-exception unless and until it is subsequently revoked by the individual. We proposed that once the individual makes the request, she should not, subject to the requirements of applicable Federal or State laws and regulations, have to continually reiterate her privacy preferences, such as having to re-submit a request every year. Likewise, we proposed that once the actor has documented an individual's request, the actor should not have to repeatedly reconfirm and re-document the request. We requested comment, however, regarding whether this approach is too permissive and could result in unintended consequences. We also sought comment on this proposed sub-exception generally, including on effective ways for an individual to revoke their privacy request for purposes of this sub-exception.

We also proposed that in order for a practice to qualify for this sub-exception, an actor's practice must be implemented in a consistent and non-discriminatory manner. This condition would provide basic assurance that the purported privacy practice is directly related to the risk of disclosing EHI contrary to the wishes of an individual, and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply. We noted that this condition requires that the actor's privacy-protective practice must be based on objective criteria that apply uniformly for all substantially similar privacy risks (84 FR 7534 and 7535).

We noted that under the HIPAA Privacy Rule, individuals have the right to request restrictions on how a covered entity will use (as that term is defined in 45 CFR 160.103) and disclose PHI about them for treatment, payment, and health care operations pursuant to 45 CFR 164.522(a)(1). Under 45 CFR 164.522(a), a covered entity is not required to agree to an individual's request for a restriction (other than in the case of a disclosure to a health plan under 45 CFR 164.522(a)(1)(vi)), but is bound by any restrictions to which it agrees (84 FR 7534).

We proposed that if an individual submitted a request to an actor not to disclose her EHI, and the actor agreed with and documents the request, the request would be valid for the purposes of this sub-exception unless and until it was subsequently revoked by the individual. We believed that this approach would minimize compliance burdens for actors while also respecting individuals' requests. We sought comment on this proposed sub-exception generally, including on effective ways for individuals to revoke their privacy request for purposes of this sub-exception (84 FR 7534). In the final rule, we align with the HIPAA Privacy Rule, specifically, 45 CFR 164.522(a)(2) which includes specific requirements with respect to the termination of an individual's restriction. Similar to the HIPAA Privacy Rule, we include § 171.202(e)(4) to address situations where the individual terminates its individual's restriction.

An actor may terminate a restriction with the individual's written or oral agreement. If the individual's agreement

[168] 45 CFR 164.524(c)(1).

[169] 45 CFR 164.524(a)(2).

is obtained orally, the actor must document that agreement. A note in the certified EHR or similar notation is sufficient documentation. If the individual agrees to terminate the restriction, the actor may use and disclose EHI as otherwise permitted under this final rule. An actor may only access, exchange or use EHI after it informs the individual of the termination. The restriction continues to apply to EHI accessed, exchanged or used prior to informing the individual of the termination. That is, any EHI that had been collected before the termination may not be accessed, exchanged or used in a way that is inconsistent with the restriction, but any information that is collected after informing the individual of the termination of the restriction may be used or disclosed as otherwise permitted under the final rule. In § 171.201(e)(4), we clarify that an actor must document a restriction to which it has agreed. We do not require a specific form of documentation; a note in the certified EHR or similar notation is sufficient.

A restriction is only binding on the actor that agreed to the restriction. We encourage actors to inform others of the existence of a restriction when it is appropriate to do so. If a restriction does not permit an actor to disclose EHI to a particular person, the actor must carefully consider whether disclosing the existence of the restriction to that person would also violate the restriction.

We clarified that for the purposes of this proposed sub-exception, the actor may give effect to an individual's request not to have an actor disclose EHI even if State or Federal laws would allow the actor not to follow the individual's request. We explained that this is consistent with our position that, absent improper encouragement or inducement, and subject to appropriate conditions, it should not be considered information blocking to give effect to patients' individual preferences about how their EHI will be shared or how their EHI will not be shared.

We requested comments on this sub-exception generally. Specifically, we sought comment on what would be considered a reasonable time frame for documentation. In addition, we also sought comment on how this sub-exception would affect public health disclosures and health care research, if an actor did not share a patient's EHI due to a privacy preference, including any effects on preventing or controlling diseases, injury, or disability, and the reporting of disease, injury, and vital events such as births or deaths, and the conduct of public health surveillance and health care research (84 FR 7534 and 7535).

Comments. Commenters recommended that we provide guidance regarding what could be considered a ''reasonable time period'' under § 171.202(e)(3) and to provide clarity to health information professionals that will be tasked with documenting the individual's privacy preferences in accordance with this regulation.

Response. In order to align with HIPAA, we looked to the HIPAA Privacy Rule at 45 CFR 164.522 for guidance on this issue. The HIPAA Privacy Rule requires a covered entity to document a restriction of PHI, but gives covered entities the discretion to determine the exact timing of the documentation. The documentation requirement is consistent with the HIPAA Privacy Rule, which is already being observed by covered entities and business associates.

Under the HIPAA Privacy Rule, a covered entity may voluntarily choose, but is not required, to obtain the individual's consent for it to use and disclose information about him or her for treatment, payment, and health care operations.[170] A ''consent'' document is not a valid permission to use or disclose PHI for a purpose that requires an ''authorization'' under the HIPAA Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the HIPAA Privacy Rule for the use or disclosure of PHI.

Similarly, we believe that actors should be given the discretion to document an individual's request and such documentation should be within a reasonable period of time after making such a request. Although we do not require the request form to be dated at the time it is signed, we would recommend that it be dated so that actors and others can document that the request was obtained prior to an actor's agreement for the restriction of the individual's access, exchange or use of EHI. What would be deemed as an unreasonable period of time would be the unreasonable delay in performance and in documentation by the actor as well as whether there were any objective manifestations of expectation expressed between the individual and the actor.

Comments. A commenter recommended that a reasonable time frame should balance and not burden an individual or organization such as reviewing preferences with the individual each year and that the risk/benefit profile in the fast-changing health-IT market may well have changed and that the individual has a right to have those changes disclosed to make an informed decision. Another commenter expressed a belief that not asking the individual to reconfirm their preference is too permissive.

Response. We agree that once the individual makes the request to an actor, she should not, subject to the requirements of applicable Federal or State laws and regulations, have to continually reiterate her privacy preferences, such as having to re-submit a request every year. Likewise, we finalized that once the actor has documented an individual's request within a reasonable period of time, then the actor is not required to repeatedly reconfirm and re-document the request.

Comments. A commenter recommended that the request needs to be in writing, and suggested that we provide guidance regarding how the individual's request could be documented. Another commenter requested that we develop a template consent form whereby patients could indicate if they would like to have their health information disclosed to third parties and to ensure that the content of this form would be absent of any ''improper encouragement or inducement'' and that we should work in consultation with OCR to develop the recommended language for a model consent form.

Response. We agree that an individual's request and an individual's request for revocation should be in writing assuming such a request is not required or prohibited by law. Alternatively, an actor could document a conversation with an individual. Such documentation could be documented in a certified EHR in some manner, and if the individual was provided a specific request form, the form could be included in a certified EHR. We believe that an individual should have sufficient opportunity to consider whether to provide a request and that an actor should minimize the possibility of coercion or undue influence and refrain from any improper encouragement or inducement. Any form provided by the actor should have information provided in plain language that is understandable to the individual.

For example, we noted that it would be improper to discourage individuals from sharing information with unaffiliated providers on the basis of generalized or speculative risks of unauthorized disclosure. On the other hand, we noted that if the actor was aware of a specific privacy or security risk, it would be proper to inform individuals of that risk. Likewise, an

[170] *See* 45 CFR 164.506(b).

actor would be permitted to provide an individual with general information about her privacy rights and options, including for example, the option to not provide consent, provided the information is presented accurately, does not omit important information, and is not presented in a way that is likely to improperly influence the individual's decision about how to exercise their rights.

It is important to note that the sub-exception conditions in the regulation are not intended to preempt any applicable Federal, State, or local laws that may require additional information to be disclosed for an agreement to be legally effective. We will continue to work in consultation with OCR to develop resources as necessary to support actors' compliance with the conditions of this Privacy Exception.

Comments. Commenters requested greater clarity on how this regulation would affect public health disclosures and health care research, if an actor did not share a patient's EHI due to a privacy preference, including any effects on preventing or controlling diseases, injury, or disability, and the reporting of disease, injury, and vital events such as births or deaths, and the conduct of public health surveillance and health care research.

Response. With regard to public health disclosures, to the extent that such disclosures are required by law, the actor would not be in a position to grant the patient's request for restriction. With regard to EHI used for research, the unavailability of the individual's information resulting from a restriction would be consistent with the patient's right to withhold authorization for research uses and disclosures. However, an Institutional Review Board may approve a consent procedure that alters some or all of the elements of informed consent, or waive the requirement to obtain informed consent under HHS regulations at 45 CFR 46.116(c), and to the extent that the researcher has obtained a waiver of informed consent, research could be compromised by the unavailability of certain EHI. One possible way to resolve this issue would be the establishment of a field that actors covered could check in a certified EHR that would indicate that restrictions have been applied to the individual's EHI (without providing detail of the nature of such restriction). In this case, actors could exclude the individual's EHI from research.

Comments. A commenter suggested that EHI should be accessed, exchanged or used despite a patient's privacy agreement with an actor in emergency treatment situations particularly when an individual is unavailable to provide a revocation. The commenter was concerned that if the EHI was not disclosed to health care provider in an emergency, the individual could be subject to imminent harm or death.

Response. In the Proposed Rule (proposed § 171.202(e)), we did not provide how an individual could revoke her privacy agreement with the actor. In response, we included in the final rule in § 171.202(e)(4) to specifically address the termination of an individual's request. In order to address these specific circumstances and align with the HIPAA Privacy Rule, we agree that an individual's restriction may need to be compromised in emergency treatment situations, and we have finalized that an actor may terminate an individual's request for a restriction to not provide access, exchange or use of EHI under limited circumstances.

c. Security Exception—When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information not be considered information blocking?

We proposed in the Proposed Rule (84 FR 7535 through 7538) to establish an exception to the information blocking provision that would permit actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain conditions. We explained that, without this exception, actors may be reluctant to implement security measures or engage in other activities that are reasonable and necessary for safeguarding the confidentiality, integrity, and availability of EHI. This could undermine the ultimate goals of the information blocking provision by discouraging best practice security protocols and diminishing the reliability of the health IT ecosystem.

We noted (84 FR 7535) that robust security protections are critical to promoting patients' and other stakeholders' trust and confidence that EHI will be collected, used, and shared in a manner that protects individuals' privacy and complies with applicable legal requirements. We also noted that public confidence in the security of their EHI has been challenged by the growing incidence of cyber-attacks in the health care sector. More than ever, we explained, health care providers, health IT developers, HIEs and HINs must be vigilant to mitigate security risks and implement appropriate safeguards to secure the EHI they collect, maintain, access, use, and exchange.

We emphasized (84 FR 7535) that, while the importance of security practices cannot be overstated, the proposed exception would not apply to *all* practices that purport to secure EHI. Rather, we stated that the exception would only be available when the actor's security-based practice satisfies the conditions applicable to this exception.[171] We noted that it would not be appropriate to prescribe a ''maximum'' level of security or to dictate a one-size-fits-all approach for all actors as that may not be appropriate in all circumstances and may not accommodate new threats, countermeasures, and best practices in a rapidly changing security landscape. We further noted that we did not intend for the proposed exception to dictate a specific security approach. Moreover, we emphasized that effective security best practices focus on the mitigation and remediation of risks to a reasonable and acceptable level.

With consideration of the above (84 FR 7535), we proposed that actors would be able to satisfy the exception through practices that implement either security policies and practices developed by the actor, or case-by-case determinations made by the actor. We proposed that whether a security-motivated practice meets this exception would be determined on a case-by-case basis using a fact-based analysis of the conditions set forth in the Proposed Rule.

We emphasized (84 FR 7535) that the practices implemented by a single physician office with limited technology resources, for example, will be different to those implemented by a large health system, and that this difference does not affect an actor's ability to qualify for this exception. The fact-based approach that we proposed would allow each actor to implement policies, procedures, and technologies that are appropriate for its particular size, organizational structure, and risks to individuals' EHI. We noted that a fact-based analysis also aligns with the HIPAA Security Rule[172] concerning the security of ePHI. The HIPAA Security Rule requires HIPAA covered entities or business associates to develop security practices and implement administrative, physical, and

[171] In the Proposed Rule (84 FR 7535), we used the phrase ''conditions applicable to this exception'' to mean the conditions (inclusive of requirements within specific conditions) of the exception applicable to a particular practice in a particular circumstance. Where we are not summarizing what we stated in the proposed rule, in this preamble we have generally used plainer-language phrasings, such as ''the conditions of the exception that are applicable to a practice [in the particular circumstances].''

[172] 45 CFR 164.306, 308, 310, and 312.

technical safeguards that take into account: The entity's size, complexity, and capabilities; technical, hardware, and software infrastructure; the costs of security measures; and the likelihood and possible impact of potential risks to ePHI.[173] We noted (84 FR 7535 and 7536), however, that while our proposed approach would be consistent with the regulation of security practices under the HIPAA Security Rule, the fact that a practice complies with the HIPAA Security Rule would not establish that it meets the conditions of the exception to the information blocking provision. We emphasized (84 FR 7536) that the HIPAA Security Rule and the proposed exception have different foci. The HIPAA Security Rule establishes a baseline by requiring certain entities to ensure the confidentiality, integrity, and availability of ePHI by implementing security measures, among other safeguards, that the entities determine are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. In contrast, we explained that the purpose of the exception to the information blocking provision is to provide flexibility for reasonable and necessary security practices without excepting from the definition of information blocking in § 171.103 practices that purport to promote the security of EHI but that are unreasonably broad and onerous on those seeking access to EHI, not applied consistently across or within an organization, or otherwise may unreasonably interfere with access, exchange, or use of EHI.

To qualify for this exception, we proposed that an actor's conduct must satisfy threshold conditions. As discussed in detail in the Proposed Rule (84 FR 7535 through 7538), the particular security-related practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI, implemented consistently and in a non-discriminatory manner, and tailored to identified security risks (84 FR 7535). We also proposed (84 FR 7537) that where an actor has documented security policies that align with applicable consensus-based standards, and where the policies are implemented in a consistent and non-discriminatory manner, a practice's conformity with such policies would provide a degree of assurance that the practice was reasonable and necessary to address specific security risks and thus should not constitute information blocking. We also stated in the Proposed Rule (84 FR 7537) that we recognize that EHI security may present novel and unexpected threats that even a best-practice risk assessment and security policy cannot anticipate. We stated that if a practice that does not implement an organizational security policy is to qualify for this exception; however, it must meet certain conditions. The public comments received, our responses to these comments, and the conditions as finalized in § 171.203 are discussed below in this section of this final rule preamble.

We encouraged comment on these conditions (84 FR 7538), and our overall approach to the proposed exception, including whether our proposal provided adequate flexibility for actors to implement measures that are commensurate to the threats they face, the technology infrastructure they possess, and their overall security profiles and, equally important, whether this exception adequately mitigates the risk that actors will adopt security policies that are unnecessarily restrictive or engage in practices that unreasonably interfere with access, exchange, or use of EHI. Commenters were encouraged to propose additional conditions that may be necessary to ensure that the exception is tailored and does not extend protection to practices that are not reasonable and necessary to promote the security of EHI and that could present information blocking concerns. We also requested comment on whether the use of consensus-based standards and guidance provides an appropriate reference point for the development of security policies.

Finally, we asked commenters to offer an alternative basis for identifying practices that do not offer a security benefit (compared with available alternatives) but that cause an information blocking harm by interfering with access, exchange, or use of EHI (84 FR 7538).

Comments. We received several comments supporting, and did not receive any comments opposed to, the establishment of the Security Exception. We also received no comments offering an alternative basis for identifying practices that do not offer a security benefit (compared with other available alternatives) but that cause an information blocking harm by interfering with access, exchange, or use of EHI to a greater degree than necessary. We received a number of comments requesting additional guidance about how the exception's conditions can be met in practice. Commenters asked questions about, or recommended that we furnish additional guidance on how an actor might determine which a security practices meet the conditions in § 171.203 to qualify for the exception.

Response. We appreciate commenters' feedback. We have finalized the exception in § 171.203, with some modification to the regulation text. We have changed the title of the exception from ''Exception—Promoting the security of electronic health information'' in the Proposed Rule (84 FR 7603) to ''Security Exception—When will a practice likely to interfere with access, exchange, or use of electronic health information in order to protect the security of electronic health information not be considered information blocking?'' Throughout this final rule preamble, we use ''Security Exception'' as a short form of this title, for ease of reference. As stated in Section VIII.D of this final rule preamble, we have changed the titles of all of the exceptions to questions to improve clarity. We have edited the wording of the introductory text of § 171.203 as finalized, in comparison to that proposed (84 FR 7603) so that it is consistent with the finalized title of § 171.203. We believe these conforming changes in wording of the introductory text also improve clarity of expression in this section.

Comments on specific conditions are summarized below, in context of each condition proposed. We believe our responses to these comments furnish the clarity actors need to understand the conditions and of the exception finalized in § 171.203 for practices likely to interfere with access, exchange, or use of EHI in order to protect the security of EHI to be considered excepted from the definition of information blocking in § 171.103.

Condition: The Practice Must Be Directly Related to Safeguarding the Confidentiality, Integrity, and Availability of Electronic Health Information

We proposed that, as a threshold condition, the exception would not apply to practices that are not directly related (84 FR 7536) to safeguarding the security of EHI. We explained that, in assessing the practice, we would consider whether and to what extent the practice directly addressed specific security risks or concerns. We noted that we would also consider whether the practice served any other purposes and, if so, whether those purposes were merely incidental to the overriding security purpose or provided an objectively distinct, non-security-related rationale for engaging in the practice.

We noted (84 FR 7536) that it should not be particularly difficult or onerous for an actor to demonstrate that its

[173] 45 CFR 164.306(b)

practice was directly related to a specific security risk or concern. For example, we explained that the actor may show that the practice was a direct response to a known security incident or threat; or that the practice directly related to the need to verify a person's identity before granting access to EHI; or that the practice was directly related to ensuring the integrity of EHI.

We emphasized (84 FR 7536) that the salient issue under this condition, therefore, would be whether the security practice was actually necessary and directly related to the specific security risk being addressed. To that end, we noted that we would consider the actor's purported basis for adopting the particular security practice, which could be evidenced by the actor's organizational security policy, risk assessments, and other relevant documentation, which most actors are already required to develop pursuant to requirements under the HIPAA Rules. However, we proposed that the documentation of an actor's decision making would not necessarily be dispositive. For example, we noted that if the practice had the practical effect of disadvantaging competitors or steering referrals, this could be evidence that the practice was not directly related and tailored to the specific security risk. We proposed that such an inference would also not be warranted where the actor has not met the other conditions of this exception, as where the actor's policies were not developed or implemented in a reasonable manner; its security policies or practices were not tailored to specific risks; or it applied its security policies or practices in an inconsistent or discriminatory manner.

Comments. We received a number of comments supporting the applicability of this exception to practices directly related to safeguarding the confidentiality, integrity, and availability of EHI and that are consistent with the HIPAA Security Rule. We received no comments recommending that this exception not be applicable to such practices.

Response. We have finalized this condition as proposed. In order to meet this specific condition (finalized in § 171.203(a)), a practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.

Comments. Commenters expressed concerns with what commenters described as the complexity of fact-based analysis and use of terms such as ''directly related.'' Commenters stated that analyzing their policies and practices against such standards could be burdensome, especially in the context of the requirement to meet all conditions at all relevant times.

Response. While fact-based analysis may not be as simple as determining if a particular security practice does or does not conform to a pre-specified approach, we believe that it is the most practical approach given the inherent complexity of the regulatory and threat landscapes relevant to an actor's cybersecurity practices. This landscape complexity contributes substantially to our belief that a one-size-fits-all detailed definition or test for security measures or methods to be deemed ''directly related'' to safeguarding the confidentiality, integrity, and availability of EHI would not be the optimal approach at this time. We have not established a specific, regulatory definition for ''directly related'' as we are using both ''directly'' and ''related'' in their ordinary meanings.[174]

With respect to the condition that a practice meet all conditions in § 171.203 at all relevant times in order to satisfy the exception, we do not believe it would be particularly difficult, in context of a fact-specific analysis, for an actor to demonstrate that its practice was directly related to a specific security risk or concern. For example, the actor may show that the practice was a direct response to a known security incident or threat, or that the practice was directly related to the need to verify a person's identity before granting access to EHI. We also note that, although we encourage actors to voluntarily conform their practices to the conditions of an exception suited to the practice and its purpose, an actor's choice to do so simply provides it an enhanced level of assurance that the practices do not meet the definition of information blocking. Failure to meet an exception does not necessarily mean a practice meets the definition of information blocking. If subject to an investigation by HHS, each practice that implicates the information blocking provision and that does not meet any exception would be analyzed on a case-by-case basis.

The overarching purpose of the Security Exception is to provide flexibility for reasonable and necessary security practices while screening out practices that purport to promote the security of EHI but that otherwise unreasonably and/or unnecessarily interfere with access, exchange, and use of EHI. Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security practices within an organization. The elements of the triad are considered the three most crucial components of information security practices.[175] In assessing whether a practice meets the condition finalized in § 171.203(a), the information that we would expect to consider includes, but is not necessarily limited to, the actor's purported basis for adopting the particular security practice, which could be evidenced by the actor's organizational security policy, risks assessments the actor had performed that informed the actor's security-based practice(s), and other relevant documentation that an actor maintains. We also reiterate our observation that many actors are also HIPAA covered entities or business associates. For that reason, many actors are likely to have, pursuant to their meeting the requirements of the HIPAA Security Rule, documentation relevant to showing their security-based practice(s) satisfy the Security Exception condition that is finalized in § 171.203(a).[176]

Condition: The Practice Must Be Tailored to the Specific Security Risk Being Addressed

To meet the exception, we proposed (84 FR 7536) that an actor's security-related practice must be tailored to specific security risks that the practice actually addressed. We explained that this condition necessarily presupposes that an actor has carefully evaluated the risk posed by the security threat and developed a considered response that is tailored to mitigating the vulnerabilities of the actor's health IT or other related systems.

Comments. Commenters expressed concerns with what commenters described as the complexity of fact-based analysis and use of terms such as ''tailored.'' Commenters stated that analyzing their policies and practices against such standards could be burdensome, especially in context of the requirement to meet all conditions at all relevant times.

Response. While fact-specific analysis may not be as simple as determining if a particular security practice does or does not conform to a pre-specified approach, we believe that it is the most practical approach given the inherent complexity of the regulatory and threat landscapes relevant to an actor's cybersecurity practices. This landscape

[174] Ordinary meanings of the adverb ''directly'' and the adjective ''related'' in American usage can be found in widely published dictionaries, such as *The American Heritage Dictionary of the English Language, Dictionary.com,* or *Merriam-Webster.com.*

[175] *See* NIST Special Publication 800–12, revision 1, An Introduction to Information Security.

[176] 45 CFR 164.316

complexity contributes substantially to our belief that a one-size-fits-all definition or test for security measures or methods to be deemed conformant with the condition finalized in § 171.203(b) would not be the optimal approach at this time. Instead, we have finalized the condition proposed in § 171.201(b) as proposed. We believe requiring that the actor's policies and practices be tailored to the risk being addressed is currently the most appropriate and practical approach. We intend for this exception to be applicable to a wide array of practices that are reasonable and necessary to protect the security of EHI in various actors' specific operational contexts. In assessing whether a practice meets the condition finalized in § 171.203(b), we would consider whether and to what extent the practice directly addresses specific security risks or concerns and whether it was tailored to those risks. We would also consider whether the practice served any other purposes and if so, whether those purposes were merely incidental to an overriding security purpose or provided an objectively distinct, non-security related rationale for engaging in the practice. We also believe the ordinary meaning of ''tailored'' [177] provides sufficient clarity that we expect the practices to be made or adapted to serve the particular purpose or need for which they are deployed. With respect to the requirement that a practice meet all conditions in § 171.203 at all relevant times in order to satisfy the exception, we do not believe it would be particularly difficult, in context of a fact-specific analysis, for an actor to demonstrate that each practice was made or adapted to serve the particular purpose or need for which is was deployed. For example, where a practice meets the condition finalized in § 171.203(a) by being a direct response to a known security incident or threat, it logically follows that the practice should also be made or adapted to the purpose of responding to such incident or threat. In which case, the practice's inherent characteristics would support the actor's ability to show that it meets the condition finalized in § 171.203(b). Similarly, where an identity-proofing practice satisfies the condition finalized in § 171.203(b) by being directly related to the need to verify a person's identity before granting access to EHI, it would be logical to expect the practice would also be tailored to address that need.

Comments. Commenters recommended that actors should be permitted to develop and implement security policies that exceed the minimum requirements of HIPAA with the intent to promote data security or to comply with State law or policies.

Response. If its conditions are otherwise met, this exception would apply to security-based practices that exceed the minimum conditions of the HIPAA Security Rule. As would be the case with a practice implemented to comply with the HIPAA Security Rule requirements, the fact that a practice was implemented to meet another applicable legal mandate would be considered in assessing whether a practice meets this exception. However, a practice that is consistent with a law or regulation setting a minimum requirement for protecting confidentiality, integrity, and availability of EHI might not meet this exception. For example, a practice that is consistent with a minimum legal condition related to the security of EHI might not meet this exception if it is not also tailored to avoid interfering with the access, exchange, or use of EHI to a greater extent than reasonable and necessary to appropriately mitigate the risk it addresses.

We have finalized this condition in § 171.203(b) without modification to the text of this condition as proposed (84 FR 7603).

Condition: The Practice Must Be Implemented in a Consistent and Non-Discriminatory Manner

We proposed (84 FR 7536 and 7537) that in order for a practice to qualify for this exception, the actor's practice must have been implemented in a consistent and non-discriminatory manner. We explained that this condition would provide basic assurance that the purported security practice is directly related to a specific security risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

As an illustration solely of the non-discriminatory manner condition (84 FR 7536 and 7537), we discussed a hypothetical example of a health IT developer of certified health IT that offers apps to its customers via an app marketplace. We stated that if the developer requires that third-party apps sold (or made available) via the developer's app marketplace meet certain security requirements, those security requirements must be imposed in a non-discriminatory manner. We noted that this would mean, for example, that if a developer imposed a requirement that third-party apps include two-factor authentication for patient access, the developer would need to ensure that the same requirement was imposed on, and met by, all other apps, including any apps made available by the developer itself. We also noted that such a developer requirement must also meet the other conditions of the exception (*e.g.,* the condition that the practice be tailored to the specific security risk being addressed).

Comments. We received no comments opposed to the condition that practices must be implemented in a consistent and non-discriminatory manner. We did receive one comment recommending that we recognize under this exception risk-based cybersecurity practices that may result in applying different security requirements to different exchange partners based on risk posed.

Response. We intend this exception, including but not limited to this specific condition, to allow for recognition of risk-based security practices. Assessment of whether practices satisfy the conditions of this exception will be fact-based. We also recognize that objectively reasonable practices applied on the basis of the cybersecurity risks posed by particular system connections or data exchanges may result in practices that are tailored to this risk and thus not necessarily identical across all connections, interchanges, and therefore all individuals or entities with whom an actor engages. In context of this condition of the Security Exception, ''consistent and non-discriminatory'' should be understood to mean that similarly situated actors whose interactions pose the same level of security risk should be treated consistently with one another under the actor's security practices. Inconsistent treatment across similarly situated actors whose interactions pose the same level of security risk based on extraneous factors, such as whether they are a competitor of the actor implementing the security practices, would not be considered appropriate.

We have finalized this condition as proposed. It is codified in § 171.203(c).

Condition Applicable to Practices That Implement an Organizational Security Policy

We discussed in the Proposed Rule (84 FR 7537) that an actor's approach to information security management would reflect the actor's particular size, organizational structure, and risk

[177] *See, e.g.,* sense 1.b. of the entry for the verb ''tailor'' in the Merriam-Webster dictionary: ''to make or adapt to suit a special need or purpose'' (*https://merriam-webster.com/dictionary/tailor*, last accessed Feb. 6, 2020). *See also, e.g.,* sense 3 of the entry for the verb ''tailor'' in The American Heritage Dictionary of the English Language: ''to make, alter, or adapt for a particular end or purpose'' (*https://ahdictionary.com*, last accessed Feb 6, 2020).

posture. Because of this, we emphasized that actors should develop and implement organizational policies that secure EHI. We proposed that, where an actor has documented security policies that align with applicable consensus-based standards, and where the policies are implemented in a consistent and non-discriminatory manner, a practice's conformity with such policies would provide a degree of assurance that the practice was reasonable and necessary to address specific security risks and thus should not constitute information blocking.

We stated (84 FR 7537) that a practice that went beyond an actor's established policies or procedures by imposing security controls that were not documented would not qualify for this exception *under this condition* (although the actor may be able to qualify under the alternative basis for practices that do not implement a security policy). We further stated that such practices would be suspect under the information blocking provision *if* there were indications that the actor's security-related justification was a pretext or after-the-fact rationalization for its conduct or was otherwise unreasonable under the circumstances.

We reiterated (84 FR 7537) that, to the extent that an actor seeks to justify a practice on the basis of its organizational security policies, such policies must be in writing and implemented in a consistent and non-discriminatory manner. We emphasized that what a policy requires will depend on the facts and circumstances. However, we proposed that to support a presumption that a practice conducted pursuant to the actor's security policy was reasonable, the policy would have to meet conditions stated and discussed in Section VIII.D.3 of the Proposed Rule (84 FR 7537). The details within paragraph (d) of § 171.203 were proposed in regulation text (84 FR 7603). The detailed requirements of the condition as proposed in § 171.203(d) were: If the practice implements an organizational security policy the policy must—

- Be in writing;
- Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;
- Align with one or more applicable consensus-based standards or best practice guidance; and
- Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

We discuss each of these requirements (subparagraphs) within the condition applicable to practices that implement an organizational security policy (§ 171.203(d)) in more detail below.

Paragraph (d)(1): Security Policy in Writing

We proposed that the actor's security policy must be in writing (84 FR 7537). This requirement is applicable to practices that implement an organizational security policy and is consistent with the HIPAA Security Rule.[178] The importance of written security policies is also consistent with consensus-based standard and best practice guidance.[179]

Comments. We received no comments opposed to this condition proposed in § 171.203(d).

Response. Within the condition (§ 171.203(d)) applicable to practices that implement an organizational security policy, we have finalized in § 171.203(d)(1) the requirement that the policy must be in writing. We have finalized this condition as proposed.

Paragraph (d)(2): Security Risks Identified and Assessed

We proposed (84 FR 7537) that the actor's security policy must be informed by an assessment of the security risks facing the actor. While we did not propose any requirements as to a risk assessment, we noted that a good risk assessment would use an approach consistent with industry standards,[180] and would incorporate elements such as threat and vulnerability analysis, data collection, assessment of current security measures, likelihood of occurrence, impact, level of risk, and final reporting.[181]

Comments. We received no comments opposed to requiring a linkage between an organization's security policy and a risk assessment. We did receive a couple of comments expressing a concern that not all actors may yet be proficient in identifying and assessing the risks associated with specific health IT functionalities, such as standards-based APIs.

Response. Within the condition (§ 171.203(d)) applicable to practices that implement an organizational security policy, we have finalized § 171.203(d)(2) with a revision to the wording of the regulation text in comparison with that proposed (84 FR 7603). Specifically, we have replaced ''and respond directly to'' that appeared in the regulation text with ''and be directly responsive to'' in the text finalized in § 171.203(d)(2). Thus, the finalized text in § 171.203(d)(2) reads: ''have been prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the actor.''

We made this editorial revision because we believe it makes the resulting regulation text easier to read. Although actors may have obligations under other existing law or regulations, such as the HIPAA Security Rule, to conduct security risk assessments, this condition, which is applicable to security-based practices that implement an organizational security policy, does not establish a set threshold for an actor's proficiency in identifying, assessing, and responding to security risks. If any actor believes it may lack the technical or other expertise necessary to conduct a risk assessment appropriate to its operations and the EHI for which it is responsible, we would encourage that actor to seek additional information, training, or support from an individual or entity with the required expertise. As finalized in § 171.203(d)(2), the requirement that risks have been identified and assessed expressly provides for this to have been done either by the actor or on the actor's behalf. We are sensitive to the possibility that some actors, including but not limited to small clinician practices, may not be in a position to meet the condition finalized in paragraph (d) of § 171.203 immediately or for all of their security-based practices, and we therefore reiterate that we have finalized in § 171.203(e) an alternative condition that an actor may choose to meet in circumstances where it may not be practical for them to meet the condition finalized in § 171.203(d).

We also reiterate that, while we do encourage actors to voluntarily conform their practices to the conditions of an exception suited to the practice and its purpose, an actor's choice to do so simply provides them an enhanced level of assurance that the practices do not meet the definition of information blocking. Failure to meet an exception does not necessarily mean a practice meets the definition of information blocking. If subject to an investigation by HHS, each practice that implicates the information blocking provision and that does not meet any exception would be analyzed on a case-by-case basis.

[178] 45 CFR 164.316

[179] *See* SP 800–53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.

[180] See OCR, Guidance on Risk Analysis, *https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.*

[181] ONC and OCR have jointly launched the HHS HIPAA Security Risk Assessment (SRA) Tool, *https://www.healthit.gov/providers-professionals/security-risk-assessment-tool.*

Paragraph (d)(3): Consensus-Based Standards or Best Practice Guidance

We proposed (84 FR 7537) that the actor's policy must align with one or more applicable consensus-based standards or best practice guidance. We noted that at present, examples of relevant best practices for development of security policies include, but are not limited to: NIST–800–53 Rev. 5; the NIST Cybersecurity Framework; and NIST SP 800–100, SP 800–37 Rev. 2, SP 800–39, as updated and as interpreted through formal guidance. We noted that best practice guidance on security policies is also developed by consensus standards bodies such as ISO, IETF, or IEC. We stated that HIPAA covered entities and business associates may be able to leverage their HIPAA Security Rule compliance activities and can, if they choose, align their security policy with those parts of the NIST Cybersecurity Framework that are referenced in the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework to satisfy this condition. We noted that relevant consensus-based standards and frameworks provide actors of varying sizes and resources with the flexibility needed to apply the right security controls to the right information systems at the right time to adequately address risk.

Comments. One commenter expressed a concern that a small independent clinician practice that conducts a risk analysis consistent with its obligation under the HIPAA Security Rule may lack the technical expertise or other organizational capabilities needed to develop a customized security policy that appropriately applies consensus-based standards to each risk identified. This commenter recommended that we incorporate in § 171.203(d) regulation text a statement that these conditions apply ''subject to the actor's sophistication and technical capabilities.''

Response. We appreciate the point highlighted by the commenter that, even within a given type of actor, specific individuals or organizations may have different operational contexts that include variations in their technical capabilities, expertise, and other resources. We do not, however, believe it is necessary to revise the regulation text as recommended in order to allow for assessment of whether the actor's practices, such as its organizational security policy, were objectively reasonable in the circumstances in which they were implemented.

Comments. A number of commenters requested that this exception allow providers to be proactive when promoting the security of EHI rather than taking a reactive stance. Commenters contended that for novel threats, consensus-based standards and best practice guidance may not exist, making it impossible for an actor to meet the condition that the organizational security policy align with such standards.

Response. With cybersecurity risk continuously evolving and the large number of threat sources active in the modern cybersecurity landscape, we recognize that actors must continuously monitor, assess, and respond to security risks that can themselves represent an impediment to EHI access, exchange, and use. Thus, this exception allows actors flexibility in selecting and tailoring their practices to mitigate specific security risks, provided each such practice otherwise meets the conditions of this exception, notably including that it be directly related and tailored to the specific security risk being addressed and be implemented in a consistent and non-discriminatory manner. We also note that best security practices in security mitigation can take a proactive as well as a reactive approach. A documented policy that provides explicit references to consensus-based standards and best practice guidance (such as the NIST Cybersecurity Framework) offers an objective and robust means by which we can evaluate the reasonableness of a particular security control for the purpose of the exception. We also recognize that, as a practical matter, some actors (such as small health care providers or those with limited resources) may have organizational security policies that are less robust or that otherwise fall short of the minimum conditions proposed. In such circumstances an actor can still benefit from this exception by demonstrating that the practice met the conditions of this exception for circumstances where no formal (organizational) security policy was implemented (see our discussion under ''*conditions applicable to practices that do not implement an organizational security policy*'' header, below within this section of this final rule preamble).

Comments. A commenter noted that it could be a difficult for an actor to meet the standard to that the actor's organizational policy on security must align with one or more consensus-based standards or best practice guidance because there are many emerging security threats that occur that are new and unexpected.

Response. We do not believe that it would be difficult for an actor's organizational policy on security to align with one or more consensus-based standards or best practice guidance documents. An actor's written security policies should be based on consensus-based standards or best practice guidance documents which specifically address security risks and threats. A security policy should be clearly written and observed and refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an actor's information systems and the EHI included in it. We believe a good policy serves as a prominent statement to the outside world about the actor's commitment to security, and that such a policy should be based on objective consensus-based standards and should not be ad hoc or arbitrary.

We do agree that there are emerging and novel security threats that occur, and in those situations which are not specifically addressed by an actor's security policies, we included in the exception as proposed an alternative condition (proposed in § 171.203(e)) to address those situations in which those security risks can be addressed based on particularized facts and circumstances.

Within the condition (§ 171.203(d)) applicable to practices that implement an organizational security policy, the actor's policy must align with one or more applicable consensus-based standards or best practice guidance. The finalized condition is codified in § 171.203(d)(3).

Paragraph (d)(4): Objective Timeframes and Other Parameters

We proposed that the actor's security policy must provide objective timeframes and common terminology used for identifying, responding to, and addressing security incidents. We noted examples of acceptable sources for development of a security response plan include: NIST Incident Response Procedure (*https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final*), US–CERT for interactions with government systems (*https://www.us-cert.gov/government-users/reporting-requirements*), and ISC–CERT for critical infrastructure (*https://ics-cert.us-cert.gov/*) (84 FR 7537).

As a point of clarification, we noted that an actor's compliance with the HIPAA Security Rule (if applicable to the actor) would be relevant to, but not dispositive of, whether the actor's policies and procedures were objectively reasonable for the purpose of the exception. We explained that an actor's documentation of its security policies and procedures for compliance with the HIPAA Security Rule may not offer a sufficient basis to evaluate whether the actor's security practices

unnecessarily interfere with access, exchange, or use of EHI. We further noted that a documented policy that provides explicit references to consensus-based standards and best practice guidance (such as the NIST Cybersecurity Framework) would offer an objective and robust means by which to evaluate the reasonableness of a particular security control for the purpose of the exception (84 FR 7537).

Comments. We received no comments opposing this requirement of the condition applicable to practices that implement an organizational security policy.

Response. Within the condition (§ 171.203(d)) applicable to practices that implement an organizational security policy, we have finalized in § 171.203(d)(4) the condition that the actor's organizational security policy ''provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.'' We have finalized this condition as proposed.

Condition Applicable to Practices That Do Not Implement an Organizational Security Policy

In the Proposed Rule (84 FR 7537), we recognized that, as a practical matter, some actors (such as small health care providers or those with limited resources) may have organizational security policies that are less robust or that otherwise fall short of the minimum conditions proposed. We proposed that in these circumstances an actor could still benefit from the exception by demonstrating that the practice at issue was objectively reasonable under the circumstances, without regard to a formal policy. While we noted in the Proposed Rule (84 FR 7537) that we expect that most security practices engaged in by an actor will implement an organizational policy, we recognized that EHI security may present novel and unexpected threats that even a best-practice risk assessment and security policy cannot anticipate. We noted that if a practice that does not implement an organizational policy is to qualify for this exception, however, it must meet certain conditions. We stated that the actor's practice must, based on the particularized facts and circumstances, be necessary to mitigate the security risk. Importantly, we proposed that the actor would have to demonstrate that it considered reasonable and appropriate alternatives that could have reduced the likelihood of interference with access, exchange, or use of EHI and that there were no reasonable and appropriate alternatives that were less likely to interfere with access, exchange or use of EHI.

We noted (84 FR 7538) that an actor's consideration of reasonable and appropriate alternatives will depend on the urgency and nature of the security threat in question. We further noted that we anticipate that an actor's qualification for the exception would accommodate exigent circumstances. For example, we stated that we would not expect an actor to delay the implementation of a security practice in response to an emergency on the basis that it has not yet been able to initiate a fully realized risk assessment process. However, we also stated that we would expect that in these exigent circumstances, where the actor has implemented a security practice without first considering whether there were reasonable and appropriate alternatives that were less likely to interfere with access, exchange or use of EHI, the actor would expeditiously make any necessary changes to the practice based on the actor's re-consideration of reasonable and appropriate alternatives that are less likely to interfere with access, exchange or use of EHI. We proposed that the exception would apply in these instances so long as an actor takes these steps and complies with all other applicable conditions.

Comments. Commenters stated that the absence of a policy means that one is dealing with an unexpected and evolving situation as best one can (*e.g.,* a sustained and sophisticated attack). Commenters suggested we create a further ''safety valve'' for short-lived actions that are taken in good faith while a situation is being evaluated and understood and that we should recognize the valid need to allow for due diligence as distinct from simply delaying access and such due diligence should not need the Security Exception to avoid implicating or being judged as engaged in information blocking. Commenters stated this is a core need for small medical practices with limited resources.

Response. We anticipate that the exception's conditions as proposed and finalized would accommodate exigent circumstances. For example, we would not expect an actor to delay the implementation of a security measure in response to an emergency such as a cyberattack simply because it has not yet been able to implement a fully realized risk assessment process. We believe the exception as posed does provide a ''safety valve'' for situations where an actor in direct response to exigent circumstances may have implemented in good faith a security practice without first considering whether there were reasonable and appropriate alternatives that were less likely to interfere with access, exchange, or use of EHI, but where the initial-response practice may be in place for only a short while. Presumably, such initial-response practices are in place for only a short time precisely because, upon more fully identifying and assessing current risks in context or as follow-up to the exigent circumstances, the actor will have concluded it carried a greater than necessary burden—including the burden of interference with access, exchange or use of EHI—and consequently modified or replaced its initial-response practice with a less onerous alternative that was reasonable and appropriately tailored to the specific risk addressed.

Comments. A commenter agreed that this exception allows for an actor to maintain flexibility in its approach to address security incidents or threats.

Response. We agree that this exception provides an actor the flexibility to address security incidents or threats based on particularized facts and circumstances which are necessary to mitigate the security risk to EHI, provided that there are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.

We have finalized as proposed, in § 171.203(e), the requirements applicable to practices that meet the threshold conditions established in §§ 171.203(a), (b) and (c) and that do not implement an organizational security policy.

d. Infeasibility Exception—When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?

We proposed in the Proposed Rule in § 171.205 (84 FR 7542 and 7603) to establish an exception to the information blocking provision that would permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, provided certain conditions are met. We proposed that in certain circumstances legitimate practical challenges beyond an actor's control may limit its ability to comply with requests for access, exchange, or use of EHI. In some cases, the actor may not have—and may be unable to obtain—the requisite technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, exchange, or use. In other cases, the actor may be able to comply with the

request, but only by incurring costs or other burdens that are clearly unreasonable under the circumstances (84 FR 7542).

We proposed that the exception would permit an actor to decline a request in certain narrowly-defined circumstances when doing so would be infeasible (or impossible) and when the actor otherwise did all that it reasonably could do under the circumstances to facilitate alternative means of accessing, exchanging, and using the EHI. We proposed a structured, fact-based approach for determining whether a request was ''infeasible'' within the meaning of the exception. We noted that this approach would be limited to a consideration of factors specifically delineated in the exception and that the infeasibility inquiry would focus on the immediate and direct financial and operational challenges of facilitating access, exchange, and use, as distinguished from more remote, indirect, or speculative types of injuries (84 FR 7542).

We encouraged comment on these and other aspects of this proposal (84 FR 7542).

Comments. We received several comments in general support of the proposed exception.

Response. We thank commenters for their support of our proposal. We note that we have changed the title of this exception from ''Exception—Responding to requests that are infeasible'' (84 FR 7603) to ''When will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?'' Throughout this final rule preamble, we use ''Infeasibility Exception'' as a short form of this title, for ease of reference. As stated in Section VIII.D of this final rule preamble, we have changed the titles of all of the exceptions to questions to improve clarity. We have also edited the wording of the introductory text in § 171.204 as finalized, in comparison to that proposed (84 FR 7603 and 7604), so that it is consistent with the finalized title of § 171.204. We believe these conforming changes in wording of the introductory text also improve clarity in this section.

i. Infeasibility of the Request

To qualify for the exception, we proposed that compliance with the request for access, exchange, or use of EHI must be infeasible. We proposed a two-step test that an actor would need to meet in order to demonstrate that a request was infeasible. Under the first step of the infeasibility test, we proposed that the actor would need to show that complying with the particular request in the manner requested would impose a substantial burden on the actor. Second, we proposed that the actor must also demonstrate that requiring it to comply with the request—and thus to assume the substantial burden demonstrated under the first part of the test—would have been plainly unreasonable under the circumstances (84 FR 7542 and 7543). We proposed that whether it would have been plainly unreasonable for the actor to assume the burden of providing access, exchange, or use will be highly dependent on the particular facts and circumstances. We proposed to rely primarily on the following key factors enumerated in proposed § 171.205(a)(1):

- The type of EHI and the purposes for which it may be needed;
- The cost to the actor of complying with the request in the manner requested;
- The financial, technical, and other resources available to the actor;
- Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged;
- Whether the actor maintains ePHI on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains EHI on behalf of the requestor or another person whose access, exchange, or use of EHI will be enabled or facilitated by the actor's compliance with the request;
- Whether the requestor and other relevant persons can reasonably access, exchange, or use the information from other sources or through other means; and
- The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use (84 FR 7543).

We acknowledged in the Proposed Rule that there may be situations when complying with a request for access, exchange, or use of EHI would be considered infeasible because an actor is unable to provide such access, exchange, or use due to unforeseeable or unavoidable circumstances that are outside the actor's control. As examples, we stated that an actor could seek coverage under this exception if it is unable to provide access, exchange, or use of EHI due to a natural disaster (such as a hurricane, tornado or earthquake) or war. We emphasized that, consistent with the requirements for demonstrating that practices meet all the conditions of a proposed exception, the actor would need to produce evidence and ultimately prove that complying with the request for access, exchange, or use of EHI in the manner requested would have imposed a clearly unreasonable burden on the actor under the circumstances (84 FR 7543 and 7544).

We stated that certain circumstances would not constitute a burden to the actor for purposes of this exception and would not be considered in determining whether complying with a request would have been infeasible. We proposed that it would not be considered a burden if providing the requested access, exchange, or use of EHI in the manner requested would have (1) facilitated competition with the actor; or (2) prevented the actor from charging a fee (84 FR 7544).

We requested comment on the proposed approach for determining whether a request is ''infeasible'' within the meaning of the exception. We encouraged comment on, among other issues, whether the factors we specifically delineated properly focus the infeasibility inquiry; whether our approach to weighing these factors is appropriate; and whether there are additional burdens, distinct from the immediate and direct financial and operational challenges, that are similarly concrete and should be considered under the fact-based rubric of the exception (84 FR 7544).

Comments. We received several comments in support of our proposed approach for determining whether a request was ''infeasible.'' We also received several comments that expressed various concerns and suggestions for improvement regarding our proposals. Several commenters expressed concern that the language in the proposed exception, particularly regarding the ''infeasibility'' of a request, was too vague or ambiguous and that the inclusion of undefined terms could create uncertainty for actors regarding whether they meet the conditions under the exception. Commenters noted that such uncertainty could dissuade actors from taking advantage of the exception. Commenters requested additional examples and guidance to clarify the conditions under the exception.

A few commenters questioned whether it would be considered information blocking if they could not segment EHI to respond to a request for a patient's EHI (*e.g.,* when patient consent to share EHI subject to 42 CFR part 2 or a State privacy law has not been provided). These commenters

expressed concern about the ability of their technology to segment a patient's EHI.

Response. We thank commenters for their support of our proposed approach for determining whether a request is ''infeasible,'' as well as the constructive feedback. We agree with commenters that each exception should clearly explain the conduct that would and would not be covered by each exception. We also reiterate that failure to meet the exception does not mean that an actor's practice related to infeasible requests necessarily meets the information blocking definition. However, as we noted in the Proposed Rule, the broad definition of information blocking in the Cures Act means that any practice that is likely to interfere with the access, exchange, or use of EHI implicates the information blocking provision. As a result, practices that do not meet the exception will have to be assessed on a case-by-case basis to determine, for example, the actor's intent and whether the practice rises to the level of an interference.

We have restructured this exception to provide further clarity. Toward that end, we have eliminated the proposed two-step test that an actor would need to meet in order to demonstrate that a request is infeasible (84 FR 7542 and 7543). Instead, we have finalized a revised framework for this exception that provides two new conditions that must be met in order for an actor to be covered by the exception and a revised condition that provides an exception for those actors unable to meet the new Content and Manner Exception. When the practice by an actor meets *one* of the conditions in § 171.204(a) and the actor meets the requirements for responding to requests in § 171.204(b) (which are discussed in more detail below), the actor is not required to fulfill a request for access, exchange, or use of EHI due to the infeasibility of the request.

The first new condition is that the actor cannot fulfill the request for access, exchange, or use of EHI due to events beyond the actor's control, namely a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority (§ 171.204(a)(1)). This is consistent with our statements in the Proposed Rule describing events that an actor could seek coverage for under this exception if it is was unable to provide access, exchange, or use of EHI due to events beyond its control (84 FR 7543). This new condition makes clear that such events are all that are necessary to meet this exception and no consideration of factors must be demonstrated and proven.

The second new condition is that the actor is not required to fulfill a request for access, exchange, or use of EHI if the actor cannot unambiguously segment the requested EHI from other EHI: (1) Because of a patient's preference or because the EHI cannot be made available by law; or (2) because the EHI is withheld in accordance with the Harm Exception in § 171.201 (§ 171.204(a)(2)). For instance, an actor will be covered under this condition if the actor could not fulfill a request to access, exchange, or use EHI because the requested EHI could not be unambiguously segmented from patient records created by federally assisted programs (*i.e.,* Part 2 Programs) for the treatment of substance use disorder (and covered by 42 CFR part 2) or from records that the patient has expressed a preference not to disclose.

The revised condition in § 171.204(a)(3)(i) specifically aligns with our proposal (84 FR 7543) in that an actor would not be required to fulfill a request for access, exchange, or use of EHI if the actor demonstrates, through contemporaneous written record or other documentation, its consideration of the following factors in a consistent and non-discriminatory manner, prior to responding to the request pursuant to paragraph (b) of this section, that led to its determination that complying with the request would be infeasible under the circumstances:

- The type of EHI and the purposes for which it may be needed;
- The cost to the actor of complying with the request in the manner requested;
- The financial and technical resources available to the actor;
- Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and
- Why the actor was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception in § 171.301.

We note that the above provisions align with our proposal in the Proposed Rule that the actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request (84 FR 7544). The difference in the final language is that we have not specified the level of detail required in the written record or other documentation, and have clarified that such a written record or other documentation must be contemporaneous so that an actor cannot use a post hoc rationalization for claiming the request was infeasible under circumstances that were not considered at the time the request was received.

We proposed in the Proposed Rule (84 FR 7544) and have finalized in this final rule in § 171.204(a)(3)(ii) the following factors that may *not* be considered in the determination: (1) Whether the manner requested would have facilitated competition with the actor; and (2) whether the manner requested prevented the actor from charging a fee or resulted in a reduced fee. We note that we have clarified in the final rule that charging ''a'' fee includes a reduced fee as well. Our rationale for carving out these considerations is that the purpose of the Infeasibility Exception is to provide coverage to actors who face *legitimate practical challenges beyond their control* that limit their ability to comply with requests to access, exchange, or use EHI. We do not believe that whether the manner requested would have facilitated competition with the actor or prevented the actor from charging a fee or resulted in a reduced fee qualify as the type of legitimate practical challenges beyond the actor's control that should be covered by the exception. Regarding the consideration of fees, the actor is able to charge fees for costs reasonably incurred, with a reasonable profit margin, for accessing, exchanging, or using EHI under the Fees Exception in § 171.302.

We have finalized in § 171.204(a)(3)(i)(F) the criterion that considers an actor's ability to provide access, exchange, and use of EHI consistent with the Content and Manner Exception in § 171.301 in order to assure alignment of this exception with the Content and Manner Exception. We further discuss the Content and Manner Exception in section VIII.D.2.a of this final rule.

We did not finalize three factors that were proposed in the context of the infeasibility analysis: (1) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the

actor's compliance with the request; (2) whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and (3) the additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use (see the proposed factors at 84 FR 7543). We removed the first factor because it was confusing and was not a strong indicator of whether a request was infeasible. We removed the second and third factors because we proposed them with the intention that they would be indicators of whether the relative burden on the requestor was greater than that on the actor. However, we have shifted away from this relative burden analysis in the final rule. To illustrate, consideration does not have to be given as to whether other means are available for access, exchange, or use of EHI or the cost to the requestor for that alternative means because of the new Content and Manner Exception (§ 171.301) and its relationship to this exception.

Comments. One commenter recommended that claims of infeasibility based on the classification of EHI as proprietary and claims of infeasibility rooted in discriminatory practices should not be included in the exception, as they do not support ONC's policy goals of promoting competition and innovation in health IT and ultimately disadvantage customers and patients.

Response. We agree with the commenter that claiming the *EHI* itself as proprietary is not a justification for claiming this exception. As discussed in more detail in the Fees Exception, we emphasize that almost all of the patient EHI found in the U.S. health care system has been generated and paid for with either public dollars through Federal programs, including Medicare and Medicaid, or directly subsidized through the tax preferences for employer-based insurance.

We explained in the Proposed Rule how use of IP rights for interoperability elements can serve to interfere with access, exchange, and use of EHI. We also explained in the Proposed Rule that the mere fact that EHI is stored in a proprietary format or has been combined with confidential or proprietary information does *not* alter the actor's obligations under the information blocking provision to facilitate access, exchange, and use of the EHI in response to a request (84 FR 7517). We emphasize that actors who control proprietary interoperability elements and demand royalties or license terms from competitors or other persons who are technologically dependent on the use of those interoperability elements would also be subject to the information blocking provision, unless they meet all conditions of the Licensing Exception (§ 171.303).

We note, however, that actors may seek coverage under the Infeasibility Exception (§ 171.204) or Content and Manner Exception (§ 171.301) for certain issues related to IP. For instance, an actor may claim to be unable to fulfill a request to access, exchange, or use EHI because the actor is not the owner of the IP rights and lacks requisite authority to provide the requested access, exchange, or use of EHI. In such a situation, the actor could claim that the request is infeasible under the circumstances (see § 171.204(a)(3)). Under § 171.204(a)(3)(i)(E), one factor that can be considered when determining whether a practice is infeasible under the circumstances is whether the actor owns or has control over a predominant technology, platform, HIE, or HIN through which EHI is accessed or exchanged. The actor could also seek coverage under the Content and Manner Exception. Under § 171.301(b)(2), an actor may provide the EHI requested in an alternative manner if responding to the request in the manner requested would require the actor to license IP. As we have explained throughout this final rule, each information blocking case, and whether the actor's practice would meet all conditions of an exception, will depend on its own unique facts and circumstances. We refer readers to the detailed discussions regarding the Content and Manner Exception (VIII.D.2.a) and Licensing Exception (VIII.D.2.c) in this preamble.

We also agree with the commenter that infeasibility rooted in discriminatory practices should not be a justification for claiming this exception. It was never our intention to allow such conduct to be covered by this exception. In response to this comment, we have clarified the factor in § 171.204(a)(3)(i)(D) to explicitly state that one consideration for determining whether a request is infeasible under the circumstances is whether *the actor's practice is non-discriminatory* and the actor provides the same access, exchange, or use to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship.

Comments. Some commenters expressed concern that this exception does not fully consider potential conflicts between valid contracts, such as business associate agreements (BAAs), and subsequent requests for access, exchange, and use of EHI that are inconsistent with those contracts. Commenters urged ONC to specify whether an actor can refuse a request to access, exchange, or use EHI as being infeasible due to such contractual restrictions and obligations.

Response. We appreciate these comments. We reiterate, as we explained in the Proposed Rule, that one means by which actors restrict access, exchange, or use of EHI is through formal restrictions, such as contract or license terms, EHI sharing policies, organizational policies or procedures, or other instruments or documents that set forth requirements related to EHI or health IT (84 FR 7518). We emphasize that such restrictions are one of the forms of information blocking the Cures Act and our final rule seek to address. We refer readers to the discussion of ''Practices that May Implicate the Information Blocking Provision'' in section VIII.C.6 of this final rule for a more detailed discussion of when contracts and agreements will be considered an ''interference'' with access, exchange, or use of EHI.

Comments. A few commenters encouraged ONC to add a provision to the exception that would enable entities who have joined Trusted Exchange Framework and Common Agreement (TEFCA) to claim the Infeasibility Exception if a requestor or third party refused to join the TEFCA and instead demanded a one-off interface.

Response. We appreciate these comments, but have decided not to adopt this suggested addition at this time. The TEFCA is still new, the Common Agreement is not yet finalized, and it would be premature to establish special treatment for entities that join the TEFCA. We may reconsider this suggestion at a later date. We note that this does not necessarily mean that actors in these situations will not be covered by the exception, as they could still show that a request for a one-off interface is infeasible under the circumstances (see § 171.204(a)(3)). However, not joining TEFCA is not de facto proof of infeasibility. We note that in addition to seeking coverage for infeasibility under the circumstances, the actor could also seek coverage from: (1) The Content and Manner Exception if the actor could not fulfill request to access, exchange, or use EHI in the manner requested (via a one-off interface), but could fulfill the request through an acceptable alternative manner (see § 171.301(b)); or (2) the Fees Exception or Licensing Exception if the actor chooses to provide the one-off interface as requested, but charges

fees/royalties related to developing or licensing the one-off interface, which could include fees or royalties that result in a reasonable profit margin (see § 171.302 and 303).

ii. Responding to Requests—Timely and Written Responses

We proposed, in addition to demonstrating that a particular request was infeasible, that an actor would have to show that it satisfied additional conditions. Specifically, we proposed that to qualify for the exception, the actor must have timely responded to all requests relating to access, exchange, and use of EHI. Further, we proposed that for any request that the actor claims was infeasible, the actor must have provided the requestor with a detailed written explanation of the reasons why the actor could not accommodate the request. We proposed that the actor's failure to meet any of these conditions would disqualify the actor from the exception and could also be evidence that the actor knew that it was engaging in practices that contravened the information blocking provision (84 FR 7544).

We proposed that the duty to timely respond and provide reasonable cooperation would necessarily be assessed from the standpoint of what is objectively reasonable for an individual or entity in the actor's position. We emphasized that we will look at the specific facts and circumstances of each case to determine whether the practice is objectively reasonable (84 FR 7544).

We encouraged comment on these conditions and related considerations. Specifically, we requested comment regarding potential obstacles to satisfying these conditions and improvements we could make to the proposed process (84 FR 7544).

Comments. Many commenters, primarily provider organizations, expressed concern that the proposed response requirements could create burden on providers, hospitals, and clinical data registries. Commenters explained that each time a requester makes a request that an actor deems infeasible, the actor would be required to timely respond and provide a detailed written explanation of its reasons for denial. A commenter also recommended that, in the event a request is infeasible and a written explanation is necessary, that such explanation need not contain detailed technical information.

Response. We appreciate these comments and have revised the response condition in this exception to address commenters' concerns and establish a set timeframe for responding to requests (§ 171.204(b)). We removed the use of the term ''timely'' and restructured the provision to more clearly explain ONC's expectations for responding to requests. Under the response condition, if an actor does not fulfill a request for access, exchange, or use of EHI for any of the reasons in § 171.204(a), the actor must, within ten business days of receipt of the request, provide to the requestor in writing the reason why meeting the request was infeasible. Our decision to finalize a 10-business day response timeframe was informed by our knowledge of the industry, stakeholder commenters, and a desire to create consistent timeframes across exceptions, such as alignment with the 10-business day response timeframe in the Licensing Exception (see § 171.303(a)(1)).

In instances when an actor is unable to respond within 10 business days, the actor may be unable to avail themselves of the requirements of the exception. As part of an information blocking investigation, ONC and OIG may consider documentation or other writings maintained by the actor around the time of the request that provide evidence of the actor's intent. Additional documentation would not permit the actor to avail themselves of this exception, but ONC or OIG could examine the actor's intent using this documentation when assessing the information blocking claim.

We have decided not to specify the level of detail or specific type of information (such as technical information) that must be contained in a written response. We believe it would be imprudent to create such boundaries for the written response given that the facts and circumstances will vary significantly from case to case. Instead, the finalized provision allows actors to determine what content is necessary to include in the written response in order to explain the reason the request is infeasible. We note that we have revised the requirement for the written response from the Proposed Rule. In the Proposed Rule an actor was required to provide a ''detailed written explanation of the reasons why the actor cannot accommodate the request'' (84 FR 7544) whereas we have finalized the requirement that the actor must provide ''in writing the reason(s) why the request is infeasible'' (§ 171.204(b)). We believe this revised requirement will alleviate burden on actors by providing them discretion to decide the appropriate level of detail to include in their written responses. It also places a greater emphasis on establishing that the request was infeasible to meet.

Reasonable Alternative

We proposed that, if the actor could not meet the request for EHI, the actor must work with the requesting party in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI, as applicable (84 FR 7544).

Comments. Commenters, primarily provider organizations, were supportive of the proposed requirement to provide a reasonable alternative. We also received a range of comments related to improving ONC's proposals regarding the provision of a reasonable alternative, including comments requesting more examples and guidance as to what would be considered a ''reasonable alternative.'' Another commenter requested that ONC provide greater deference to the actor to determine the appropriate format/functionality for sharing the requested EHI when a comparable functionality, distinct from the format/functionality requested, is made available and enables access, exchange, or use of EHI on equivalent terms. One commenter requested ONC place guardrails around requests for information sharing, such that if an actor is able to share data in an industry-accepted format, the requesting organization cannot make an information blocking claim if that format does not meet their preferred, specific data transmission standard.

A few commenters requested that ONC remove the requirement that an actor both ''identify'' and ''provide'' a reasonable alternative means of accessing EHI, and instead require only that an actor ''identify'' a reasonable alternative. One commenter requested that ONC clarify that the proposed requirement to identify a reasonable alternative means of accessing, exchanging, or using EHI is only necessary where any such alternative exists. The commenter noted that there could be instances in which no reasonable alternative exists, and the request is in effect impossible to comply with. One commenter requested that ONC clarify that, regarding the provision of a reasonable alternative, an actor must only work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI as applicable. One commenter expressed concern that this exception could be used to send patients to other sources to get their health information because that approach would be less burdensome than providing the information to the patient directly. The commenter recommended that ONC

preclude the use of this exception for patient access requests.

Some provider, hospital, and clinical data registry commenters expressed concern regarding the potential burden on the actor related to identifying and providing a reasonable alternative means of accessing, exchanging or using the EHI. Other commenters, primarily health IT developers, expressed concern regarding the potential impact and burden on health IT developers, HINs, and HIEs of complying with a request to access, exchange, or use EHI, especially when the request requires custom development. Commenters explained that if a system, even a large system, were required to comply with many custom forms of integration, collectively they would cause a significant burden to both business and budget. Some commenters also noted that the proposed exception seems imbalanced, favoring the requester of the EHI over the actor providing the EHI.

Response. We appreciate the support for our proposal, as well as the array of constructive comments. We first note that, in many instances, the exceptions, including the finalized third condition of this exception (§ 171.204(a)(3)), favor the request for EHI because the overall information blocking paradigm is to eliminate interference with access, exchange, and use of EHI. We have removed the ''reasonable alternative'' requirement from this exception and instead have finalized the new Content and Manner Exception in § 171.301 that establishes the content (*i.e.,* the EHI) required in the response and the manner in which the actor may respond to the request for access, exchange, or use of EHI. This new exception improves on the ''reasonable alternative'' requirement in the Proposed Rule by clarifying actors' obligations for providing access, exchange, or use of EHI in all situations and creating actionable technical procedures.

We believe the Content and Manner Exception in § 171.301 is responsive to the above comments, will reduce burden on actors, and is principled and tailored in a manner that will promote basic fairness and encourage parties to work cooperatively to implement efficient solutions to interoperability challenges. We refer readers to the Content and Manner Exception and the discussion of such exception in this preamble in sections VIII.C and VIII.D.2.a. With regard to the comment suggesting that no reasonable alternative may exist, we believe that the new exception will address this concern. However, if the actor still could not meet the new exception, the actor could avail itself of the third condition in this exception and demonstrate that the request was infeasible under the circumstances.

e. Health IT Performance Exception—When will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information not be considered information blocking?

We proposed to establish an exception to the information blocking provision for certain practices that are reasonable and necessary to maintain and improve the overall performance of health IT, provided certain conditions are met (84 FR 7550). We stated in the Proposed Rule that this exception would apply to the unavailability of health IT occasioned by both planned and unplanned maintenance and improvement. We noted that planned maintenance or improvements are often carried out at regular intervals and address routine repairs, updates, or new releases while unplanned maintenance or improvements typically respond to urgent or time-sensitive issues. We proposed to codify the exception's regulation text in § 171.207 (84 FR 7605).

To ensure that the actor's practice of making health IT, and in turn EHI, unavailable for the purpose of carrying out maintenance or improvements is reasonable and necessary, we proposed conditions that would need to be satisfied at all relevant times a practice to be recognized as excepted from the definition of information blocking under this proposed exception.

Comments. We received numerous comments supporting the establishment of this exception. We did not receive comments opposing the establishment of this exception. Many of the comments received requested clarification or recommended revisions to specific points within the proposed exception. The comments requesting clarification or making recommendations are summarized below.

Response. We appreciate the feedback. We have established the proposed exception with modifications from the regulation text proposed in the Proposed Rule. We have retitled the exception from ''Exception—Maintaining and improving health IT performance'' (proposed § 171.207, at 84 FR 7605) to ''Health IT Performance Exception—When will a practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information not be considered information blocking?'' (§ 171.205 as finalized). For ease of reference and discussion, we use ''Health IT Performance Exception'' as a short title for the finalized exception throughout this preamble. Unless we are directly quoting the Proposed Rule or accurate re-statement of Proposed Rule content requires otherwise, we use ''Health IT Performance Exception'' in this section of this preamble when discussing this exception as proposed as well as the finalized exception. As stated in section VIII.D of this preamble (under the heading ''modifications''), we changed the titles of all of the information blocking exceptions to questions for additional clarity. We revised the wording of the finalized § 171.205 introductory text in comparison with that proposed in § 171.207 so that it is consistent with the finalized title of the exception (and § 171.205). Consistent with the restructuring of part 171 that is also described in section VIII.D of this preamble (under the heading ''modifications''), this exception has been redesignated from § 171.207 in the Proposed Rule (84 FR 7605) to § 171.205 as finalized. Commenters' requests for clarification and suggested revisions on specific points are discussed below. Other revisions we have made to the regulation text finalized in § 171.205 in comparison to that proposed in § 171.207 are also discussed below.

Unavailability of Health IT Must Be for No Longer Than Necessary To Achieve the Maintenance or Improvements for Which the Health IT Was Made Unavailable

We proposed that any unavailability of health IT must be for a period of time no longer than necessary to achieve the maintenance or improvement purpose for which the health IT is made unavailable or its performance degraded (84 FR 7550 and 7551). We provided as an illustrative example that a health IT developer of certified health IT that has the right under its contract with a large health system to take its system offline for four hours each month to conduct routine maintenance would not qualify for this exception if an information blocking claim was made about a period of unavailability during which no maintenance was performed.

Comments. We received comments from a variety of stakeholders on the proposed requirement that any unavailability of health IT would need to be for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable. Some commenters agreed that temporary unavailability of health IT ''for a period

of time no longer than necessary'' created an appropriate standard for both planned and unplanned downtimes. Other commenters indicated they did not support this standard, stating concerns that the requirement that the health IT be made unavailable ''for a period of time no longer than necessary'' would be too difficult to assess without more specific criteria such as defined time periods. Some commenters suggested we modify our language to allow for greater flexibility in maintenance downtime situations.

Response. We have finalized within the condition for maintenance and improvements to health IT in § 171.205(a)(1) the requirement proposed in § 171.201(a)(1), with modifications to the regulation text that are described below (immediately preceding the preamble discussion of the next subparagraph of § 171.205(a)). When an actor choosing to conform its practice to the health IT performance exception implements a practice that makes health IT under that actor's control temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the actor's practice must be (§ 171.205(a)(1)) implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded. We believe that establishing specific timeframes applicable to various maintenance and improvement purposes would be impractical at this time due to the wide variety of system architectures and operational contexts in which health IT to which part 171 is applicable is currently, or may in the future be, deployed. We have finalized the ''no longer than necessary'' requirement of this condition, which we believe provides substantial flexibility to consider the particular circumstances of each case, and a variety of factors including but not limited to the service level agreements in place for the specific health IT at issue, the type of maintenance or improvements, the technical resources available to the actor, or best practices or other industry benchmarks relevant to the particular maintenance or improvements.

Comments. Noting our use of the phrase ''as soon as possible'' in the Proposed Rule's preamble discussion of this condition (84 FR 7551), specifically in an example where an actor takes health IT offline in response to a software failure, some commenters requested we clarify how we interpret that phrase. A commenter described practices such as procedures that phased restoration of full functionality across a complex system, to manage system loads or confirm the original failure is fully resolved, and asked if we would interpret this exception's proposed conditions as excluding such procedures. Some comments from members of the developer community suggested that we modify our proposed language from ''for a period of time no longer than necessary'' to ''a reasonable period of time.''

Response. The ''no longer than necessary'' standard provides actors substantial flexibility to address the particular circumstances of each case, allowing for consideration of a variety of factors including but not limited to the service level agreements in place for the specific health IT at issue, the type of maintenance or improvements, the technical resources available to the actor, or best practices or other industry benchmarks relevant to the particular maintenance or improvements. In response to comments requesting we clarify how we interpret ''as soon as possible'' and how it would apply to specific types of practices, we first ask readers to note that in this final rule preamble for the Health IT Performance Exception we use the phrase ''as soon as possible'' *only* in summarizing and responding to these comments. We see how this phrase could be read as implying that we might uniformly expect restarts in a shorter time or more abrupt manner than might be consistent with best practices for ensuring the affected component(s) or production environment are restored to stable, reliable operating status. We do not, however, interpret the finalized condition as uniformly mandating immediate full restarts of any or every system. In determining whether an actor's practice made health IT under its control unavailable, or degraded the health IT's performance, for longer than was necessary in the particular circumstances, we would consider a variety of factors such as (but not limited to) the service level agreements in place for the specific health IT at issue, the type of maintenance or improvements, the technical resources available to the actor, or best practices or other industry benchmarks relevant to the particular maintenance or improvements.

Comments. Several commenters recommended that this exception apply to downtime necessary for testing whether a maintenance or improvement activity, such as deploying a new or updated application into a particular production environment for the first time, will operate in that environment as it is intended to operate or without adversely affecting other functions of the system.

Response. We interpret ''minimum time necessary'' to complete a maintenance or improvement purpose, objective, or activity to include reasonable and necessary practices, such as confirmatory testing and phased restart protocols, to ensure that a newly deployed or newly updated application functions in a particular production environment as it is intended to perform and does not adversely affect system stability or the performance of critical functions or components of that system. In determining whether an actor's practice affected health IT's availability or performance for longer than was necessary in the particular circumstances, we reiterate that we would consider a variety of factors such as (but not limited to) the service level agreements in place for the specific health IT at issue, the type of maintenance or improvements, the technical resources available to the actor, or best practices or other industry benchmarks relevant to the particular maintenance or improvements.

Comments. Some commenters recommended that we recognize there may be circumstances where an instance of downtime may exceed service level agreements but still be no longer than necessary to address the issue. These commenters suggested such violations of service level agreements and other provisions of contracts between the parties should remain to be resolved through contractual mechanisms and not automatically considered information blocking on basis of exceeding the terms of the agreements. One commenter suggested actors who make their health IT temporarily unavailable under this exception be held to industry standards for necessary timeframes to complete any maintenance or improvements.

Response. For purposes of determining whether a period of health IT unavailability or performance degradation is (or was) no longer than necessary to accomplish its purpose, we note that service level agreements and industry practices would be relevant information to be considered but not necessarily dispositive. For example, a period of health IT unavailability or performance degradation could be within the parameters of applicable service level agreements but still be longer than necessary to accomplish the maintenance or improvement purpose for the health IT was made unavailable or its performance degraded. For a contrasting example, a period of health IT unavailability or performance

degradation could be outside the parameters of applicable service level agreements—a contractual matter for the parties to resolve through other appropriate channels—without being ''longer than necessary'' in the totality of applicable circumstances and, therefore, without necessarily constituting information blocking as defined in § 171.103.

Comments. Several commenters requested we clarify whether this exception would apply to practices that degrade some aspects of a health IT system's performance, without making it entirely unavailable, for purposes of conducting maintenance and improvement of the health IT system or some of its components.

Response. We appreciate the feedback. We agree that there may be circumstances where the minimum disruption of an overall health IT system's availability needed to accomplish particular maintenance or improvement purposes may be less than total. We do not intend that this exception would apply only to complete unavailability of health IT. We intend the exception to apply to reasonable and necessary practices that disrupt EHI access, exchange, or use not only for the shortest time but also to the least extent practicable to accomplish their specific maintenance or improvement purposes under the particular circumstances. Accordingly, we have modified the language of § 171.205(a)(1) as finalized to expressly include temporary performance degradation as well as temporary unavailability of health IT affected by maintenance and improvement practices.

Discussion of Finalized Text of § 171.205(a)(1)

The regulation text finalized in § 171.205(a)(1) has been modified in comparison to the regulation text proposed in § 171.207(a)(1) in several ways. The finalized regulation text expressly includes ''or the health IT's performance degraded,'' for the reasons stated in response to comments (above). In the text of this provision, finalized at § 171.205(a)(1), we have also replaced the verb ''to achieve'' with the verb ''to complete.'' Reflecting on the comments received, we have reviewed the dictionary definition of ''achieve'' and now believe that our use of ''achieve'' in the regulation text proposed in in § 171.207(a)(1) may have contributed to commenters' concerns about whether we would interpret time for confirmatory testing of system performance or phased restart protocols as falling within the ''minimum time necessary'' for any particular maintenance or upgrade.

We believe ''complete'' less ambiguously expresses our intent that this requirement of this condition encompasses the minimum time necessary, in the totality of the particular circumstances, to fully complete the maintenance or improvement activity, including any confirmatory testing or other protocols necessary to ensure an orderly and reliable restoration of normal operating status. We have also revised the wording of § 171.205(a) as finalized so that it is consistent with the title and introductory text of § 171.205 as finalized.[182] We made modifications to the titles and introductory text of all of the finalized exceptions for reasons described in section VIII.D of this preamble (under the heading ''modifications''). As finalized, § 171.205(a)(1) requires, in order to meet the condition in § 171.205(a), that when an actor implements a practice that makes health IT under that actor's control temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the actor's practice must be implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded.

Unavailability of Health IT for Maintenance or Improvements Must Be Implemented in a Consistent and Non-Discriminatory Manner

We proposed (in proposed § 171.207(a)(2)) that any unavailability of health IT occasioned by the conduct of maintenance or improvements must be implemented in a consistent and non-discriminatory manner (84 FR 7551). We explained that this condition provides a basic assurance that when health IT is made unavailable for the purpose of performing maintenance or improvements the unavailability is not abused by the actor that controls the health IT. However, we indicated that this condition would not require that actors conduct all planned maintenance or improvements simultaneously, or require that every health IT contract provide the same promises in regard to planned maintenance or improvements. We further noted that a recipient of health IT could agree to a longer window for unavailability in exchange for a reduced fee for system maintenance, which would not contravene this condition of this exception.

Comments. Several commenters expressed support for requiring practices be implemented in a non-discriminatory manner to meet the conditions of the Health IT Performance Exception. One commenter supported the requirement but stated that they believed practices applied selectively against an actor or third-party application inappropriately accessing interoperability resources should be exempt from this condition.

Response. We appreciate the opportunity to clarify two points. First, we want to reiterate that there is an important distinction between conduct of individuals or entities (or the behavior of applications) that poses a security risk and conduct or behavior that may merely adversely affect performance of a health IT system or its core functions. If an actor or an application is making or attempting unauthorized access to systems or to EHI, the actor with control of the system subject to that security risk should take prompt action to address that risk. As stated in the finalized § 171.205(d), the Health IT Performance Exception expressly does *not* apply to security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the conditions of § 171.205, but must comply with all applicable conditions of § 171.203 at all relevant times if they wish to seek the added assurance of conforming their practices to an exception to the information blocking provision. Second, we recognize there are circumstances where an application's behavior does not pose a security risk but does adversely impact the performance of a health IT system's overall or core functions performance. We decline to modify § 171.205(a)(2) in the manner the commenter recommended in order to address adverse impacts on health IT performance. Instead, in response to this and other comments, we have finalized in § 171.205(b) an alternative condition that expressly provides for the finalized Health IT Performance Exception to apply to practices implemented to mitigate a third-party application's negative impact on an actor's health IT's performance.

[182] As noted above in this section of this preamble, titles of all the finalized exceptions have been revised to be more clear and easy to understand.

Unavailability of Health IT for Maintenance or Improvements Must Be Agreed

In order to benefit from this exception, we proposed that the unavailability of health IT due to maintenance or improvements initiated by a health IT developer of certified health IT, HIE, or HIN, must be agreed to by the individual or entity to whom the health IT is supplied (84 FR 7551). We noted that the availability of health IT is typically addressed in a written contract or other written agreements, that puts the recipient of the health IT on notice about the level of EHI and health IT unavailability that can be expected for users of the health IT. By such agreements, the recipient of the health IT willfully agrees to that level of planned and unplanned unavailability (typically referred to in health IT contracts as ''downtime''). We proposed that in circumstances where health IT needs to be taken offline for maintenance or improvements on an urgent basis and in a way that is not expressly permitted under a health IT contract an actor could satisfy the proposed condition so long as the maintenance or improvements are agreed to by the recipient of the health IT. We proposed that this could be achieved by way of an oral agreement such as reached between the parties by telephone, but we noted that because an actor must demonstrate that it satisfies the conditions of this exception, it would be best practice for an actor to ensure the agreement was in writing or, at minimum, contemporaneously documented.

We proposed that this condition would *only* apply when the unavailability of health IT is caused by a health IT developer of certified health IT, HIE, or HIN because it is the supplier of the health IT and thus controls if and when health IT is intentionally taken offline for maintenance or improvements. We proposed that this condition would not apply when health IT is made unavailable for maintenance or improvements at the initiative of a recipient (or customer) of health IT, noting that when it is a customer of health IT who initiates unavailability, the unavailability would not need to be the subject of an agreement with the supplier of that health IT, nor anyone else, in order for the customer of health IT to benefit from this exception.

Comments. Several commenters from the provider community recommended advance notice of downtime. Several commenters from the provider community suggested that planned downtimes should be documented, scheduled, and executed within a predefined window of time. One commenter recommended that actors create a public website that displays planned and unplanned system downtime and allow other actors to subscribe to notifications of these downtimes. One commenter suggested we explicitly prohibit an entity from regularly scheduling extensive time periods where query and response services are unavailable. Another commenter suggested we make allowances within the conditions of this exception for an actor who may fall slightly out of compliance with terms agreed to regarding downtime in a service level agreement if the impact is *de minimis* and the actor was acting in good faith. One commenter contended that the information blocking provisions should not regulate the level of service provided by health IT developers to their customers. We also received several comments from members of the HIE and HIN community that recommended against any requirement to include specific details such as dates and times for maintenance because such a requirement could result in HIEs and HINs having to undertake the process of amending thousands of legal agreements.

Response. We do not believe it is necessary to dictate the availability or health IT or other contractually defined details of the business relationship between parties for the purposes of this exception. Parties to a health IT contract can determine and communicate their respective service level needs and capabilities or commitments in legally enforceable contracts. Contractual provisions can establish specific details of service levels, planned downtime, unplanned downtime, and communications regarding planned and unplanned downtime, that are practical and appropriate to the context of a particular contract. In the event parties do not honor such contract provisions, remedies are available to the parties outside and independent of part 171. We also agree with commenters' observations that any specific requirements, such as those recommended by some other commenters, could require amending contracts in ways that could create significant burden and costs for actors. Thus, we did not modify this exception in response to commenters' recommendations that we require service level or other contractual agreements between parties conform to specific prescribed timeframes, scheduling (including specifically or query and response services), notice, and scope of planned downtimes expectations in order for maintenance and improvement health IT downtimes to meet the information blocking exception for maintenance and improvement. Similarly, we have not modified the exception in response to recommendations from some commenters that we require display of planned and unplanned downtime on publicly available websites. We are not persuaded such measures would generally render benefits commensurate with the time and effort that would be needed for actors to implement and maintain them.

Comments. Two commenters disagreed with our proposed requirement that temporary unavailability initiated by a health IT developer of certified health IT, HIE, or HIN must be agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT. Both commenters recommended removing the ''agreed upon with user'' provision we proposed and recommended that ONC eliminate the requirement for prior agreement of planned downtime in order to meet the conditions of this exception. These commenters suggested that we instead allow for unilateral notice to organizations at least 10 days prior to scheduled maintenance.

Response. We continue to believe that unplanned downtime must be done with the agreement of the individual or entity to which the health IT is supplied. This condition protects health care providers and other uses or health IT under the specific circumstance of health IT being made temporarily unavailable due to unplanned maintenance or improvements. It also reduces the potential for downtime purportedly for purposes of health IT maintenance or improvement to be a pretext for information blocking and thus makes it less likely that this exception will be abused. However, the conditions of this exception finalized in § 171.205 can be met by unplanned downtime in the absence of contemporaneous agreement so long as it is consistent with an existing service level agreement. We also note that specific agreement by all users to temporary unavailability is not required in all instances of unplanned downtime not already covered by an existing service level or other contractual agreement, such as downtime resulting from events beyond the actor's control that prevent it from meeting the requirement, and practices that are consistent with the conditions of the Preventing Harm Exception (§ 171.201),

Security Exception (§ 171.203), or Infeasibility Exception (§ 171.204).

Comments. Several commenters from the developer community expressed appreciation for the opportunity to comment on throttling, arguing that it is a reasonable approach to maintain access to functionality. Many of these commenters stated that, when applied with the agreement of health IT users, strategies such as throttling or metering certain health IT functions should not be considered information blocking. One commenter suggested that throttling should not be considered information blocking if the health IT developer or health care provider is forced to throttle access so as not to negatively impact hospital operations. The commenter recommended that when requests for EHI from third-party applications created an unreasonable and significant burden on health IT and the installed infrastructure, the two contracting parties could mutually agree that the third-party application was poorly designed and could be throttled or even denied access. Another commenter suggested that the practice of throttling should only occur if that portion of the health IT affected by an application is impacting highly critical functions such as inpatient or emergency department care delivery and documentation. The commenter stated that it was important to distinguish between the practice of throttling generally and the practice of throttling as a response to impact on critical functions because the practice of throttling generally could be applied too broadly.

Response. We appreciate commenters' input. We recognize that in some circumstances it may be appropriate for actors to take action (*e.g.,* deny access, throttle, or meter) to limit the negative impact on the performance of health IT that may result from the technical design, features, or behavior of a third-party application. This would include, but not be limited to, third-party applications that a patient might choose to use to access their EHI. The regulation text finalized in § 171.205 has been expanded, in comparison to the text proposed in § 171.207 (84 FR 7605), to include paragraph (b), which we have titled ''assured level of performance.'' As finalized, § 171.205(b) establishes a condition expressly applicable to actions taken against a third-party application that is negatively impacting the health IT's performance. The specific requirements for action against a third-party application to meet the condition finalized in § 171.205(b) and thus be excepted from the definition of information blocking parallel the requirements finalized in § 171.205(a), the condition applicable to practices that make health IT temporarily unavailable, or its performance degraded, for purposes of maintenance and improvement.

To meet the Health IT Performance Exception under the assured level of performance condition, an action against a third-party application (§ 171.205(b)) must be: (1) For a period of time no longer than necessary to resolve any negative impacts; (2) implemented in a consistent and non-discriminatory manner; and (3) consistent with existing service level agreements, where applicable. For example, if the service level agreement stated how and to what extent negative impacts should be addressed (*e.g.,* over-capacity), then it is expected that such provisions of an existing service level agreement would be followed unless they violated one of the other requirements of the (§ 171.205(b)) assured level of performance condition (*e.g.,* resulted in discriminatory application or lasted longer than necessary to resolve the negative impacts). We believe this approach will help to address situations where actions such as throttling become necessary to protect the overall performance of health IT.

Interaction With the Preventing Harm and Security Exceptions

We proposed that when health IT is made unavailable for maintenance or improvements aimed at preventing harm to a patient or other person, or securing EHI, an actor must comply with the conditions specified in the proposed Harm Exception or proposed Security Exception, respectively, in order for these particular practices to be excepted from the definition of information blocking in § 171.103.

Comments. We received a few comments that expressed concern that our maintenance exception, as proposed, did not address unplanned downtime without notice in the instance of a potential threat to security of EHI.

Response. Unplanned downtime or other practices reasonable and necessary in response to exigent threats to EHI security should be implemented consistent with the conditions for the Security Exception as finalized in § 171.203. We expressly stated in the proposed regulation text at § 171.207(c), and have finalized in § 171.205(d), that if the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to EHI, the actor does not need to satisfy the conditions of the Health IT Performance Exception, but must comply with all conditions of § 171.203 at all relevant times for such practices to be excepted from the definition of information blocking in § 171.103. We believe this paragraph of the finalized Health IT Maintenance Exception's regulation text (finalized in § 171.205(d)) provides ample clarity that this exception is not intended to apply to unplanned downtime implemented specifically in response to emergent security threats. We have finalized this approach to the relationship between the Health IT Performance Exception and Security Exception as proposed, because we continue to believe it ensures that the Health IT Performance Exception cannot be used to avoid compliance with conditions applicable under the Security Exception when the practice leading to unplanned downtime is implemented specifically in response to a risk to security of EHI.

Comments. We received several comments from stakeholders in the developer community that it would be impossible for certified health IT developers, HIEs, or HINs to meet the conditions of this exception as proposed in the event of downtime as a result of something like a natural disaster because those parties would be unable to secure agreement from entities and individuals prior to uncontrollable downtime.

Response. The Infeasibility Exception finalized in § 171.204 has been revised, in comparison to the proposed regulation text in the Proposed Rule, to expressly address uncontrollable events. In cases of natural or human-made disaster, public health emergency, public safety, incident war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority, an actor can avail itself of the Infeasibility Exception. We determined these situations should be addressed in the Infeasibility Exception rather than the Health IT Performance Exception in part because the breadth of circumstances where access, exchange, or use of EHI may be interfered with due to these uncontrollable events is more consistent with the intent and function of the Infeasibility Exception. Thus, we have not modified the Health IT Maintenance Exception (§ 171.205) to address uncontrollable events of the type expressly addressed by the finalized Infeasibility Exception (§ 171.204).

We have finalized the substance of the relationship between the Health IT Maintenance Exception and the Preventing Harm and Security Exceptions as proposed. We have also

finalized as proposed the provisions of the Health IT Maintenance Exception specific to ''*practices that prevent harm*'' and ''*security-related practices,*'' but have redesignated them within the structure of the Health IT Maintenance Exception as finalized in § 171.205 in comparison to the structure proposed at § 171.207 (84 FR 7605). Specifically, the ''*practices that prevent harm*'' provision is finalized in paragraph (c) of the finalized Health IT Maintenance Exception in § 171.205 instead of paragraph (b) as was the case in the Proposed Rule (84 FR 7605). Likewise, the ''*security-related practices*'' provision is finalized in paragraph (d) of the finalized Health IT Maintenance Exception in § 171.205 instead of paragraph (c) as was the case in the Proposed Rule (84 FR 7605). Both of these provisions were moved down to accommodate the addition of the ''*assured level of performance*'' condition as paragraph (b) of § 171.205 as finalized.

The paragraph of the Health IT Maintenance Exception finalized in § 171.205(c), specific to ''*practices that prevent harm,*'' continues to provide that if the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all conditions of § 171.201 at all relevant times to qualify for an exception. Likewise, the paragraph of the Health IT Maintenance Exception finalized in § 171.205(d), specific to ''*security-related practices,*'' continues to provide that if the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all conditions of § 171.203 at all relevant times to qualify for an exception.

Request for Comment

We requested comments on the exception in general, and on whether the proposed conditions would impose appropriate limitations on actor-initiated health IT maintenance or improvement activities that lead to temporary unavailability of EHI.

Comments. We did not receive comments generally opposed to the establishment of this exception. One commenter recommended that if a patient is affected by a practice that could be recognized under this exception, such as unavailability of health IT for an app registration, the patient should be provided an opportunity to access the EHI through another means, such as the patient portal.

Response. The Health IT Performance Exception is applicable to a variety of specific practices making health IT unavailable. It does not recognize only downtime or performance degradation of an actor's entire health IT system. An actor who takes down one means of EHI access to conduct health IT maintenance or improvement could provide alternative access to EHI, in circumstances where this may be practical, and remain in compliance with the requirements for their practices to be excepted under § 171.205 from the definition of information blocking in § 171.103. However, we stress that an actor conducting maintenance or improvement of health IT in the actor's control is not *required* to provide an alternative electronic health information access mechanism during the downtime in order for the Health IT Performance Exception to apply to the actor's maintenance or improvement practices. We are aware that actors' operational contexts and existing health IT capabilities vary substantially throughout the health IT ecosystem. In a variety of circumstances where downtime or performance degradation may be reasonable and necessary to maintain or improve health IT performance, an actor may not have the capability needed to meet a requirement that EHI must always be immediately available in response to every patient request. For example, in some circumstances it may be impossible to achieve a particular maintenance or improvement purpose within a specific system without temporarily rendering all EHI in the system unavailable to all functions, services, and other components of the system (such as APIs and portals) through which EHI is ordinarily accessed, exchanged, or used.

2. Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

a. Content and Manner Exception—When will an actor's practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information not be considered information blocking?

In this final rule, we have established a new exception in § 171.301 (referred to as the Content and Manner Exception) under section 3022(a)(3) of the PHSA as a means to identify reasonable and necessary activities that do not constitute information blocking. Although we did not propose this exception in the Proposed Rule, it is related to our proposals and requests for comment in the Proposed Rule regarding the proposed EHI definition (84 FR 7513) and the proposed requirement to identify and provide a reasonable alternative means for accessing, exchanging, or using EHI as part of the proposed Infeasibility Exception (84 FR 7544). We discuss below the connection between these proposals and requests for comment in the Proposed Rule and the conditions in the Content and Manner Exception.

We note that a failure to meet the Content and Manner Exception does not mean that an actor's practice meets the information blocking definition. However, as we noted in the Proposed Rule, the broad definition of information blocking in the Cures Act means that any practice that is likely to interfere with the access, exchange, or use of EHI implicates the information blocking provision (see 84 FR 7515). As a result, practices that do not meet the Content and Manner Exception will have to be assessed on a case-by-case basis to determine, for example, the actor's intent and whether the practice rises to the level of an interference. We discuss the comments received regarding the proposals related to the EHI definition (84 FR 7513) and the requirement to identify and provide a reasonable alternative means for accessing, exchanging, or using EHI under the Infeasibility Exception (84 FR 7544) below.

Comments. As discussed in more detail section VIII.C.3, we received many comments expressing concerns regarding the breadth of the proposed EHI definition and requesting flexibility in the implementation of the information blocking provision. Many commenters stated that it would be difficult for actors to provide the full scope of EHI as it was proposed to be defined, particularly as soon as the final rule was published. Some commenters opined that we were trying to do too much too fast. Commenters requested that we provide flexibility for actors to adjust to the scope of the EHI definition, as well as the exceptions. Commenters asserted that such an approach would permit them to adapt their processes, technologies, and systems to enable the access, exchange, and use of EHI as required by the Cures Act and this final rule. Some commenters suggested that EHI under the information blocking provision should be limited to ePHI as defined in 45 CFR 160.103, while others requested that ONC consider constraining the EHI covered by the information blocking provision to only the data included in the USCDI.

We also received a range of comments requesting clarification and concerning improvements to our proposal in the Infeasibility Exception that, for any request that the actor claims is infeasible, the actor must work with the requesting party in a timely manner to identify and provide a *reasonable alternative means* of accessing, exchanging, or using the EHI, as applicable (proposed in § 171.205(d), 84 FR 7604). Commenters, primarily provider organizations, were supportive of the proposed condition. Some commenters requested clarification and additional examples about what manner of response would constitute a ''reasonable alternative'' and when it would be acceptable to enable requestors to access, exchange, or use EHI in an alternative manner. One commenter requested that ONC place guardrails around requests for information sharing, such that if an actor is able to share data in an industry-accepted format, the requesting organization cannot make an information blocking claim if that format does not meet the organization's preferred, specific data transmission standard. One commenter requested that ONC clarify that the proposed requirement to identify a reasonable alternative means of accessing, exchanging, or using EHI is only necessary where any such alternative exists. The commenter noted that there could be instances in which no reasonable alternative exists, and the request is in effect impossible to comply with.

A few commenters requested that ONC remove the requirement that an actor both ''identify'' and ''provide'' a reasonable alternative means of accessing EHI, and instead require only that an actor ''identify'' a reasonable alternative. One commenter expressed concern that this exception could be used to send patients to other sources to get their health information because that approach would be less burdensome than providing the information to the patient in the manner requested. The commenter recommended that ONC preclude the use of this exception for patient access requests.

Some provider, hospital, and clinical data registry commenters expressed concern regarding the potential burden on the actor related to identifying and providing a reasonable alternative means of accessing, exchanging or using the EHI. Other commenters, primarily health IT developers, expressed concern regarding the potential impact and burden on health IT developers, HINs, and HIEs of complying with a request to access, exchange, or use EHI, especially when the request requires custom development. Some commenters also noted that the proposed exception seems imbalanced, favoring the requester of the EHI over the actor providing the EHI.

Response. The Content and Manner Exception in § 171.301 addresses the two groups of comments noted above: (1) Comments expressing concerns regarding the breadth of the proposed EHI definition (proposed in § 171.102, 84 FR 7601) and requesting flexibility in the implementation of the information blocking provision; and (2) comments requesting clarification concerning and improvement to our proposal in the Infeasibility Exception regarding the provision of a reasonable alternative (proposed in § 171.205(d), 84 FR 7604). In response to these comments, we have removed the reasonable alternative provision from the Infeasibility Exception and we have finalized the Content and Manner Exception in § 171.301 which describes the content (*i.e.,* the EHI) required to be provided in an actor's response to a request to access, exchange, or use EHI and the manner in which an actor must fulfill the request in order to satisfy the exception. We believe this new exception will address the broad range of comments we received about the content of an actor's response to and manner for fulfilling a request to access, exchange, or use EHI, and will provide the clarity and transparency sought by commenters. We also believe, as discussed in more detail below, that this new exception provides market participants the ability to reach and maintain market negotiated terms for the access, exchange, and use of EHI.

Content

The first condition of this exception (''content condition'') in § 171.301(a) establishes the content an actor must provide in response to a request to access, exchange, or use EHI in order to meet this exception. As discussed in section VIII.C.3 of this preamble, we have focused the scope of the EHI definition in this final rule to ePHI as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, with limited exception. We also address commenter concerns regarding the scope of the EHI definition and the pace at which we are implementing the information blocking provision through the Content and Manner Exception. Specifically, section 171.301(a)(1) states that for up to May 2, 2022, an actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard adopted in § 170.213. Section 171.301(a)(2) states that on and after May 2, 2022, an actor must respond to a request to access, exchange, or use EHI with EHI as defined in § 171.102.

We explained in section VIII.C of this final rule that we have finalized a new paragraph in the information blocking definition in § 171.103 that aligns with the content condition described above. That new paragraph, which is finalized in § 171.103(b), states that, until May 2, 2022, EHI for purposes of part 171 is limited to the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213. We have included a detailed discussion in section VIII.C of our rationale for including the content condition in the Content and Manner Exception and for including paragraph (b) in § 171.103. That discussion includes an explanation of how those provisions address the commenters' concerns detailed above. We refer readers to the discussion in section VIII.C.

Manner

The second condition of this exception (''manner condition'') in § 171.301(b) establishes the manner in which an actor must fulfill a request to access, exchange, or use EHI in order to meet this exception. This condition is similar to our proposal in the Infeasibility Exception in the Proposed Rule that, for any request the actor claims is infeasible, the actor must have worked with the requesting party in a timely manner to identify and provide a *reasonable alternative* means of accessing, exchanging, or using the EHI, as applicable (see proposed § 171.205(d), 84 FR 7604). We explained in the Proposed Rule that this proposed condition would minimize the risk that the Infeasibility Exception could protect improper refusals to enable access, exchange or use of EHI, including discriminatory blanket refusals as well as other practices, such as improper delays for access or exchange that would present information blocking concerns (84 FR 7544).

After review of comments, further consideration of proposed conditions, and taking into account the revised structure of the exceptions, we determined that the concept of providing a ''reasonable alternative'' fits better in the Content and Manner Exception than in the Infeasibility Exception. As such, we removed the ''reasonable alternative'' requirement from the Infeasibility Exception and incorporated the general concept into

the Content and Manner Exception. We believe this approach improves on the ''reasonable alternative'' requirement in the Proposed Rule by clarifying actors' obligations for providing access, exchange, or use of EHI in all situations; creating actionable technical procedures; and aligning the requirement for providing an alternative with the Fees and Licensing Exceptions.

Under § 171.301(b)(1), an actor must fulfill a request described in the content condition (paragraph (a) of the exception) in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request (§ 171.301(b)(1)(i)). If an actor fulfills a request described in the content condition in any manner requested: (1) Any fees charged by the actor in relation to its response are not required to satisfy the Fees Exception in § 171.302; and (2) any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the Licensing Exception in § 171.303 (§ 171.301(b)(1)(ii)).

Section 171.301(b)(2) provides requirements for fulfilling a request to access, exchange, or use EHI in an alternative manner than the manner requested. If an actor does not fulfill a request described in the content condition of this exception in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner in order to satisfy the exception. Section 171.301(b)(2)(i) states that the actor must fulfill the request without unnecessary delay in the following order of priority, starting with the first paragraph and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph. That order of priority is as follows: (1) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor (§ 171.301(b)(2)(i)(A)); (2) using content and transport standards specified by the requestor and published by the Federal Government or a standards developing organization accredited by the American National Standards Institute (ANSI) [183] (§ 171.301(b)(2)(i)(B)); and (3) using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor (§ 171.301(b)(2)(i)(C)). Section 171.301(b)(2)(ii) requires that any fees charged by the actor in relation to fulfilling the request must satisfy the Fees Exception in § 171.302. Similarly, § 171.301(b)(2)(iii) requires that any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the Licensing Exception in § 171.303.

We chose this approach because we believe actors should, first and foremost, attempt to fulfill requests to access, exchange, or use EHI in the manner requested. This principle is central to our information blocking policies (*e.g.,* it was part of the proposed Infeasibility Exception) and will help ensure that EHI is made available where and when it is needed. Our approach acknowledges, however, that there may be instances when an actor should not be required to respond in the manner requested.

First, if an actor is *technically unable* to fulfill a request to access, exchange, or use EHI in the manner requested, the actor is allowed to fulfill the request in an alternative manner (§ 171.301(b)(1)(i)). We emphasize that we use ''technically unable'' in this context to mean that actors *cannot* fulfill a request to access, exchange, or use EHI due to technical limitation. For example, if an individual requested their EHI via an API and the actor could not fulfill the request via the API, but the individual then requested the EHI be provided via email and the actor was technically able to do so, we expect that the actor would fulfill the request in that ''manner requested.'' This standard sets a very high bar, and would not be met if the actor is technically able to fulfill the request, but chooses not to fulfill the request in the manner requested due to cost, burden, or similar justifications. If, for instance, under the alternative manner, fulfilling the request would prove costly for the actor, the actor would be able to charge a fee that results in a reasonable profit margin under the Fees Exception in § 171.302 or license any requisite interoperability elements and make reasonable royalties under the Licensing Exception in § 171.303. If the burden on the actor for fulfilling the request is so significant that the actor chooses not to fulfill the request at all, the actor could seek coverage under the Infeasibility Exception in § 171.204. We believe this framework for utilizing this exception, which works in harmony with the Infeasibility Exception (§ 171.204), Fees Exception (§ 171.302), and Licensing Exception (§ 171.303), is principled and tailored in a manner that will promote basic fairness and encourage parties to work cooperatively to implement efficient solutions to interoperability challenges.

Second, we establish that an actor is not required to fulfill a request to access, exchange, or use EHI in the manner requested if the actor cannot reach agreeable terms with the requestor to fulfill the request (§ 171.301(b)(1)(i)). We also establish that if an actor fulfills a request to access, exchange, or use EHI in *any manner requested,* the fees or licenses associated with fulfilling such requests will *not* be limited by the conditions in the Fees Exception or Licensing Exception. These provisions will allow actors to first attempt to negotiate agreements in any manner requested with whatever terms the actor chooses and at the ''market'' rate—which supports innovation and competition. We then allow flexibility for actors to still satisfy the exception by fulfilling the request in an alternative manner if the actor cannot reach agreeable terms with the requestor to fulfill the request. For instance, under the exception, actors who cannot reach agreeable terms with the requestor to fulfill the request are *not* required to license their IP to proprietary technology in order to satisfy the exception.

In contrast, § 171.301(b)(2)(ii) and (iii) require that any fees charged or licenses granted by the actor in relation to fulfilling a request to access, exchange, or use EHI in an *alternative* manner *must* satisfy the Fees Exception in § 171.302 and the Licensing Exception in § 171.303. We recognize that it is possible that responding in an alternative manner may require licensing of interoperability elements. However, we do not believe that, in most cases, licensing certified technology (§ 171.301(b)(2)(i)(A)) or standards-based technology (§ 171.301(b)(2)(i)(B)) would involve the type of licensing of proprietary interoperability elements that concerned the majority of commenters because the standards in § 171.301(b)(2)(i)(a) and (B) are ''open'' standards. Therefore, it is our understanding that a health IT developer of certified health IT would not normally be required to license its IP in order to meet the requirements for fulfilling a request to access, exchange, or use EHI in those alternative manners. On the other hand, the technology/software that the developer uses to fulfill a request in any manner requested *could* constitute the developer's IP, depending on the request. We emphasize that this exception does *not* require developers to open-source their technology/software.

For instance, if a health IT developer of certified health IT enables access to

[183] *See https://www.ansi.org/.*

EHI using HL7 (which is an ANSI-accredited standards developing organization) FHIR Release 2 (R2) Standard, that means the developer will provide EHI in the format specified in FHIR R2. In this example, the actual software code that is used by the developer to convert the EHI from the developer's proprietary format to FHIR R2 is the developer's IP and is not required to be provided to the requestor. We also note that our experience and knowledge of the health IT landscape indicate that the market is increasingly moving toward open standards, and we believe this movement will further decrease the need to license IP in the future. We believe this framework and approach are supportive of innovation and address commenter concerns regarding their ability to protect their IP.

We included in § 171.301(b)(2)(i) that an actor must fulfill the request *without unnecessary delay* in order to make clear that actors seeking coverage under this exception by responding in an alternative manner will be held to same unnecessary delay or ''timeliness'' considerations as all actors are in determining whether there is an interference under the information blocking provision. The fact that an actor responds in an alternative manner does *not* entitle that actor to any additional time to respond to a request to access, exchange, or use of EHI that the actor would not be afforded if responding in any manner requested. As such, any unnecessary delays related to responding in an alternative manner could disqualify an actor from meeting the alternative manner condition in the same way that an unnecessary delay in responding to a request to access, exchange, or use EHI in any manner requested could constitute an interference. We refer readers to the discussion of ''Limiting or Restricting the Interoperability of Health IT'' in section VIII.C.6.c.ii.

Under § 171.301(b)(2)(i)(A), if an actor does not fulfill a request described in the content condition of this exception in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner. Specifically, the actor must attempt to fulfill the request using technology certified to standards adopted in part 170 specified by the requestor. This manner of response is given precedence because it advances a certified, standards-based approach that supports the Promoting Interoperability Programs (previously Medicare and Medicaid EHR Incentive Programs) administered by the Centers for Medicare & Medicaid Services (CMS), other Federal and State programs that use certified health IT, and other Federal Departments (Department of Defense and Veterans Affairs). In addition, the certification criteria under the ONC Health IT Certification Program (the Program) include robust oversight, including technical and interoperability requirements, ONC-Authorized Certification Body (ONC–ACB) in-the-field surveillance expectations, and cost transparency and other disclosure requirements. To illustrate how this would work, if the requestor only requests the EHI using the C–CDA 2.1 content standard, then the actor would not have to also use the Direct transport standard to provide the EHI. However, if the requestor requests the EHI through the use of both standards, then the actor would be expected to respond in such a manner if the actor has certified health IT that supports both standards.

If the actor is technically unable to respond using technology certified to standards adopted in part 170 specified by the requestor, then the actor may respond using content and transport standards specified by the requestor and published by the Federal Government or a standards developing organization accredited by the ANSI (§ 171.301(b)(2)(i)(B)). We chose to specify that standards published by a standards developing organization accredited by ANSI would qualify for this manner of response because ANSI oversees the development of voluntary consensus standards in the United States and it accredits standards that are developed by representatives of other standards organizations. ANSI accreditation signifies that the procedures used by standards developing organizations meet the institute's requirements for openness, balance, consensus, and due process. Voluntary consensus standards developed by an ANSI-accredited standards developing organization carry a high degree of acceptance both in United States and internationally. ANSI has broad membership across government agencies, industry, academia, and international bodies and is the official United States representative to the International Organization of Standards (ISO). This manner of response also advances interoperability through standards-based exchange, even if the standard is not certified under the Program.

As noted above, the ''manner'' of response specific in § 171.301(b)(2)(i)(B) includes two distinct components: (1) Content standard; and (2) transport standard. The content standard deals with whether the information is in an appropriate format and is universally understood. This standard includes the structure (*i.e.,* syntax) and terminology (*i.e.,* semantics) of the EHI. Examples of content standards include: US Fast Healthcare Interoperability Resources (FHIR) Core IG; Consolidated Clinical Document Architecture (C–CDA 2.1); HL7 V2.5.1; HL7 v2.7 (which is a standard that is not part of certification from an ANSI-accredited standards developing organization); and Argonaut Data Query Implementation Guide. The transport standard is the method to connect two or more parties without a focus on the data that is transported from one party to another. Put another way, the transport standard is the method by which information moves from one point to another. Examples of transport standards include: *Direct Project Standard,* ONC Applicability Statement for Secure Health Transport, Version 1.0 (incorporated by reference in § 170.299) (§ 170.202(a)); and Simple Object Access Protocol (SOAP) based exchange specifications such as ''Nationwide Health Information Network Messaging Platform Specification.'' [184] Under the manner condition, an actor could proceed to the next consecutive ''manner'' under § 171.301(b)(2)(i) if the actor was technically unable to respond with *either* the content standard or the transport standard requested.

Last, if an actor is technically unable to fulfill a request for access, exchange, or use of EHI using a content and transport standard specified by the requestor and published by the Federal Government or a standards developing organization accredited by ANSI, *only then* can the actor respond using an alternative machine-readable format, including the means to interpret the EHI, agreed to by the actor and requestor (§ 171.301(b)(2)(i)(C)). This option to respond using an agreed upon alternative machine-readable format is a flexible option for actors who cannot meet the ''manner'' requirements in § 171.301(b)(2)(i)(A) and (B), but still want to be responsive to the requestor and seek coverage under this exception. Examples of alternative machine readable formats include CSV, public domain standards, public advisory

[184] *See* ONC, Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap, FINAL Version 1.0, *https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf*; ONC, 2015 Interoperability Standards Advisory, *https://www.healthit.gov/isa/sites/default/files/2015interoperabilitystandardsadvisory01232015final_for_public_comment.pdf.*

standards, and other community efforts used to represent the data.

We emphasize two key components of § 171.301(b)(2)(i)(C). First, the alternative machine-readable format must include the means to interpret the EHI. The goal with this requirement is to ensure that, if an actor fulfills a request for access, exchange, or use of EHI using an alternative machine-readable format, the EHI provided through that format will be usable by the requestor. As an example, the format used for the EHI Export functionality (§ 170.315(b)(10)) discussed earlier in this final rule could be used to fulfill such a request. Second, the alternative machine-readable format must be agreed upon with the requestor. This condition ensures that, even if the actor is technically unable to meet the requirements in § 171.301(b)(2)(i)(A) and (B), the actor is still providing the requestor the opportunity to access, exchange, or use the EHI in a manner that is amenable to the requestor.

b. Fees Exception—When will an actor's practice of charging fees for accessing, exchanging, or using electronic health information not be considered information blocking?

We proposed in the Proposed Rule to establish an exception at § 171.204 (84 FR 7589) to the information blocking provision that would permit the recovery of certain costs reasonably incurred for the access, exchange, or use of EHI. We interpreted the definition of information blocking to include *any* fee that is likely to interfere with the access, exchange, or use of EHI. We noted that this interpretation may be broader than necessary to address genuine information blocking concerns and could have unintended consequences on innovation and competition. Specifically, unless we establish an exception, actors may be unable to recover costs that they reasonably incur to develop technologies and provide services that enhance interoperability. This could undermine the ultimate goals of the information blocking provision by diminishing incentives to invest in, develop, and disseminate interoperable technologies and services that enable more robust access, exchange, and use of EHI. Therefore, we proposed to establish an exception that would permit the recovery of certain costs that we believe are unlikely to present information blocking concerns and would generally promote innovation, competition, and consumer welfare, provided certain conditions are met. We emphasized that actors can make a reasonable profit under this exception, provided that all applicable conditions are met (84 FR 7538 through 7541).

We proposed that the exception would be subject to strict conditions to prevent its potential abuse. Specifically, we explained our concern that a broad or insufficiently tailored exception for the recovery of costs could protect rent-seeking, opportunistic fees, and exclusionary practices that interfere with the access, exchange, and use of EHI. We explained that these practices fall within the definition of information blocking and reflect some of the most serious concerns that motivated its enactment (see 84 FR 7538 and section VIII.B of this preamble). For example, in the Information Blocking Congressional Report,[185] we cited evidence of wide variation in fees charged for health IT products and services. While we cautioned that the issue of fees is nuanced, and that variations in fees could be attributable in part to different technology architectures, service models, capabilities, service levels, and other factors, we concluded that these factors alone could not adequately explain all of the variation in prices that we had observed. Based on these and other indications, we concluded that some actors were engaging in opportunistic pricing practices or, in some cases, charging prices designed to deter connectivity or exchange with competing technologies or services. In the time since we published the Information Blocking Congressional Report, these practices have persisted and, in certain respects, become more pronounced. In a national survey of HIE executives published in 2017, 47 percent of respondents reported that EHR developers ''often/routinely'' charge high fees for exchange that are unrelated to cost, and another 40 percent reported that they ''sometimes'' do.[186] Meanwhile, we have continued to receive credible evidence of rent-seeking and other opportunistic behaviors, such as fees for data export and data portability that are not plausibly related to any time, materials, or other costs that a developer would reasonably incur to provide these services. And, while some practices described in the Information Blocking Congressional Report have become less prevalent (such as the charging of per-transaction fees), other practices have emerged that are equally concerning (84 FR 7538).

As just one illustration, some EHR developers have begun conditioning access or use of customer EHI on revenue-sharing or royalty agreements that bear no plausible relation to the costs incurred by the EHR developer to grant access to the EHI. We have also heard of discriminatory pricing policies that have the obvious purpose and effect of excluding competitors from the use of interoperability elements. Many of the industry stakeholders who shared their perspectives with us in listening sessions prior to the Proposed Rule, including several health IT developers of certified health IT, condemned these practices and urged us to swiftly address them (84 FR 7538).

In light of these concerns, we proposed that this exception would apply only to the recovery of certain costs and only when the actor's methods for recovering such costs comply with certain conditions at all relevant times. In general, these conditions would require that the costs the actor recovered were reasonably incurred, did not reflect costs that are speculative or subjective, were appropriately allocated, and based on objective and verifiable criteria. Further, the exception would not apply to certain fees, such as those based on the profit or revenue associated with the use of EHI (either being earned by the actor, or that could be realized by another individual or entity) that exceed the actor's reasonable costs for providing access, exchange, or use of the EHI (84 FR 7539 through 7541).

Finally, the exception would provide additional conditions applicable to fees charged in connection with: (1) The certified APIs described in § 170.404 (84 FR 7594); and (2) the EHI export criterion proposed in § 170.315(b)(10) (84 FR 7590) to support single patient EHI export and to support the export of all EHI when a health care provider chooses to migrate information to another health IT system. We emphasized that access to EHI that is provisioned by supplying some form of physical media, such as paper copies (where the EHI is printed out), or where EHI is copied onto a CD or flash-drive, would not be a practice that implicated the information blocking provision provided that the fee(s) charged for that access complied with the HIPAA Privacy Rule (45 CFR 164.524(c)(4)) (84 FR 7539).

Clarification

We clarify that the Fees Exception we have finalized in this rule in no way supports or encourages the *sale of EHI.*

[185] ONC, Information Blocking Congressional Report (April 2015), *https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.*

[186] Julia Adler-Milstein and Eric Pfeifer, *Information Blocking: Is It Occurring And What Policy Strategies Can Address It?,* 95 Milbank Quarterly 117, 124–25 (Mar. 2017), *available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full.*

We emphasize that this exception permits the recovery of certain costs reasonably incurred for the *access, exchange, or use* of EHI. We note that many individuals and entities who are considered ''actors'' under the information blocking provision are also subject to the HIPAA Privacy Rule and therefore prohibited from selling PHI unless certain conditions are met, and in particular, receiving remuneration for a disclosure of PHI in accordance with 45 CFR 164.502(a)(5)(ii). This exception to the information blocking definition in no way affects existing HIPAA Privacy Rule compliance responsibilities of entities subject to the HIPAA Rules.

Comments. We received many comments in general support of the proposed exception. Commenters appreciated ONC's goal of addressing rent-seeking, opportunistic fees, and exclusionary practices that interfere with the access, exchange, and use of EHI. Some commenters suggested that ONC should take additional steps and measures to ensure that the requirements under this exception are clear. A couple of commenters recommended that fees and costs of information exchange should be made publicly available. Another commenter suggested that ONC develop a process for actors to routinely report their use of this exception, including specific timeframes for actors to submit information to ONC and for ONC to determine whether the exception can be applied under specific circumstances.

Response. We thank commenters for their support of and feedback on this exception. We appreciate the suggestions for improved transparency under this exception. We believe actors should have discretion to decide if they would like to enhance transparency by making fees and costs of information exchange publicly available. We believe that choosing not to disclose fees, on its own, would not likely implicate the information blocking provision. Further, while we wholeheartedly support the goal of enhanced transparency and commend commenters' desire to enhance transparency in the final rule, we believe their suggestions could create additional burden for actors and such burden could outweigh the benefits of the measures they suggest. We will continue to consider steps to further promote transparency regarding our information blocking policies in future rulemakings.

We appreciate the comment that we should develop a process for letting actors know whether this exception could be applied under certain circumstances. We may consider developing materials in the future regarding the application of the exceptions should the need arise. However, we believe the final rule clearly describes the conditions actors must meet in order to be covered by each exception, and informational materials are not necessary at this time.

Requirement That Costs Be Reasonably Incurred

In the Proposed Rule, we stated that, regardless of the type of cost at issue, a basic condition of the proposed exception was that any costs the actor seeks to recover must have been reasonably incurred to provide the relevant interoperability elements for the access, exchange, or use of EHI. Whether a cost was reasonably incurred will ultimately depend on the particular facts and circumstances. We requested comment on considerations that may be relevant to assessing the reasonableness of costs incurred for purposes of this exception (84 FR 7539).

Comments. Several commenters requested additional clarity in the final rule regarding various terms and concepts in the proposed exception. Commenters noted that many terms and concepts regarding the reasonableness of fees, and which fees would or would not be considered ''reasonably incurred'' under the exception, were ambiguous and overly broad. Some commenters were concerned that such ambiguity and vagueness could undercut ONC's overall intent to prevent rent-seeking and opportunistic fees and could create a loophole that would enable actors to use the exception to continue to charge unreasonably high fees. Some commenters requested additional examples of ''costs reasonably incurred'' under the exception. One commenter asked that ONC outline different cost categories (such as development costs, deployment costs, usage costs) and indicate which of those costs would or would not fall under the exception. A couple of commenters requested that ONC explicitly state that fees the actor pays to a developer for ''Release of Information'' (ROI) services and technology would be considered ''costs reasonably incurred.''

Response. We appreciate these comments. Actors may choose to satisfy the conditions of this exception to be certain that the fees they charge for the access, exchange, or use of EHI do not implicate the information blocking provision. We reiterate that failure to meet the exception does not mean that an actor's practice related to charging fees meets the information blocking definition. However, as we explained in the Proposed Rule, we interpret the broad definition of information blocking in section 3022(a) of the PHSA to encompass *any* fee that is likely to interfere with the access, exchange, or use of EHI (84 FR 7521). Fees that do not meet this exception may implicate the information blocking provision and will have to be assessed on a case-by-case basis to determine, for example, the actor's intent and whether the practice rises to the level of an interference. Consistent with the conditions of this exception, an actor seeking the significant protection afforded by this exception will have to assess the fees they charge in light of the costs incurred.

We emphasize that our intention with this exception is not to set any particular fees related to products or services for accessing, exchanging, or using EHI, but rather to allow the market to define the appropriate price for such products or services so long as certain methods are followed and certain criteria are met. We believe this approach is appropriate for this exception in light of the considerable diversity in the types of costs actors might incur and the range of factors that could bear on the reasonableness of those costs. For example, the costs of developing software may vary with the purposes it is intended to serve, the settings in which it will be deployed, the types and scope of capabilities included, and the extent to which these development efforts build on existing development efforts and know-how. Additionally, the costs of providing services, including the implementation of technology in production environments, may vary based on the technology design or architecture, individual customer needs, local implementation conditions, and other factors. An analysis of the approach for recovering costs will also account for different distribution and service models under which the costs are calculated. For these reasons, we have decided not to specify cost categories, such as development costs, deployment costs, usage costs, or ROI services and technology costs. However, we note that if an actor meets all necessary conditions of the finalized exception, the actor *could* recover such categories of cost under the exception.

We have taken a few distinct steps to clarify this exception and address the overall concern from commenters regarding the clarity of this exception. First, we have restructured the exception for clarity. We have changed the title of the exception from ''Exception—Recovering costs reasonably incurred'' to ''When will an actor's practice of charging fees for

accessing, exchanging, or using electronic health information not be considered information blocking?'' Throughout this final rule preamble, we use ''Fees Exception'' as a short form of this title, for ease of reference. As stated in Section VIII.D of this final rule preamble, we have changed the titles of all of the exceptions to questions to improve clarity. We have also edited the wording of the introductory text in § 171.302, in comparison to that proposed (84 FR 7603), so that it is consistent with the finalized title in § 171.302. We believe these conforming changes in wording of the introductory text also improve clarity in this section.

We have also divided the exception into three conditions in § 171.302—(a) Basis for fees condition; (b) Excluded fees condition; and (c) Compliance with the Conditions of Certification condition. We explain upfront in the introductory sentence of the exception that, pursuant to these conditions, an actor may charge fees, including fees that result in a reasonable profit margin, for the access, exchange, or use of EHI without implicating the information blocking provision. We believe this framework provides actors with a clear roadmap for voluntarily satisfying the conditions of the exception. We discuss the substantive changes we have made to these provisions in the discussion of each condition later in this section of the preamble.

We also note that we have further clarified the fees allowed under this exception by focusing the scope of the EHI definition (discussed in section VIII.C.3 of this preamble) and adding paragraph (b) to the information blocking definition in § 171.103 (discussed in section VIII.C of this preamble). By changing the definition of EHI to electronic protected health information (ePHI) as defined in 45 CFR 160.103 included in a designated record set as defined in 45 CFR 164.501, we have focused the scope of information covered by the information blocking provision. In addition, under the finalized information blocking definition, for up to 18 months after the six-month delayed compliance date of the information blocking section of this final rule (part 171) (a total of 24 months after the publication date of this final rule), EHI for purposes of the information blocking definition is limited to the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213 (see (§ 171.103(b)).

Basis for Fees Condition

To qualify for this exception, we proposed that the method by which the actor seeks to recover its costs must meet certain conditions. We proposed that this would require that the actor base its recovery of costs on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. We proposed that any differences in prices or price terms would have to be based on actual differences in the costs that the actor incurred or other reasonable and non-discriminatory criteria. We further proposed to require that the method by which the actor recovers its costs must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged (84 FR 7539).

We also proposed that the costs must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported. A reasonable allocation of costs would require that the actor allocate its costs in accordance with criteria that are reasonable and between only those customers that either cause the costs to be incurred or benefit from the associated supply or support of the technology (84 FR 7539).

We proposed that the exception would not apply if the method by which the actor recovers its costs is based, in any part, on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor. The use of such criteria would be suspect because it suggests the fee the actor is charging is not based on its reasonable costs to provide the services and may have the purpose or effect of excluding or creating impediments for competitors, business rivals, or other persons engaged in developing or enabling the use of interoperable technologies and services (84 FR 7539).

Last, we stated that the method by which the actor recovers its costs must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of EHI, including the secondary use of such information, that *exceeds* the actor's reasonable costs for the access, exchange, or use of EHI (84 FR 7539).

We requested comment on the proposed conditions and other issues we should consider in assessing whether the methodology by which an actor distributes costs and charges fees should be considered reasonable and necessary for purposes of the exception. In particular, we noted that we were considering whether to introduce specific factors and methods for assessing when profit will be reasonable. We requested comment on whether the pro-competitive or efficiency-adding aspect of an actor's approach to providing access, exchange, or use of EHI should be taken into account when assessing the reasonableness of profits. We asked commenters to consider whether there are specific use cases for which actors' profits should be limited or prohibited for purposes of meeting the exception (84 FR 7539).

We also asked commenters to consider alternate approaches to the exception that would also achieve the goal of allowing actors to recover certain types of costs that would promote innovation, competition and consumer welfare and that are unlikely to present information blocking concerns. In assessing other potential approaches to this exception, we encouraged commenters to contemplate such considerations as enforceability, potential burden on the parties, and overall effectiveness in meeting the above stated goals (84 FR 7539).

Comments. We received several comments regarding our proposed approach for cost recovery and profits. Some commenters supported our proposed approach. A couple of commenters recommended that we prohibit all profits under the exception to ensure that actors cannot continue rent-seeking and exclusionary pricing practices. Several commenters requested clarification regarding the profits that would be allowed under the exception and expressed concern that the regulation text does not clearly state that profits are allowed under the exception. Several other commenters, primarily health IT developers, disagreed with the proposed cost recovery approach and limits on profits, expressing concern that ONC's proposals will serve as a barrier to innovation, competition, and interoperability. Some commenters stated that ONC's proposals regarding fees and profits go beyond the congressional intent in the Cures Act and questioned whether ONC has regulatory authority to regulate costs and profits.

We received some comments that recommended we take a different approach for assessing whether an actor's costs recovered are reasonable. Commenters recommended using an approach that distinguishes, as appropriate, between: (1) Pure cost or expense recovery, with no provision for margin or profit; (2) ''cost-based pricing'' or ''cost plus accounting,'' where margin or profit is allowed; and (3) ''market-based pricing,'' where there

are no restrictions on pricing. A couple of commenters recommended that where a cost-based pricing mechanism is required, the method for assessing the cost basis should be reasonably associated with the complexity or cost of providing the capabilities. Such methods could include reasonable heuristics, estimates, or other commonly used methods.

Commenters recommended that we distinguish ''basic access'' (with no profits or limited profits) from ''value-added'' access, exchange, or use (which would allow for increased profits). A couple of commenters recommended that allowed fees for ''basic access'' be on a pure direct cost recovery basis only. Those commenters recommended that the cost to develop and/or map to standards should not be part of the cost basis for fees for ''basic access;'' rather any such costs should be a part of the fees for the health IT. The commenters recommended that when the outputs of value-added services are incorporated into, or from, an essential part of the legal medical record, or are routinely used for decision making, they constitute part of the set to which basic access is required. The commenters also recommended that we distinguish between intellectual property (IP) rights that are essential to access EHI and IP rights that allow for value-added services.

Response. We thank commenters for their support of our proposals and for the thoughtful comments on this aspect of the exception. We appreciate that commenters were concerned both about the elimination of rent-seeking, opportunistic fees, and exclusionary pricing practices that interfere with the access, exchange, and use of EHI as well as the importance of finalizing policies that support and promote innovation. We have finalized the proposed approach for determining whether the basis for fees charged is acceptable under this exception, with some clarifications and updates detailed below.

As we discussed in the Proposed Rule, we believe our approach will provide actors that seek to meet this exception certainty that charging fees to recover certain costs reasonably incurred for the access, exchange, or use of EHI will not implicate the information blocking provision, provided the actor's practice meets the conditions of the exception. We reiterate that an actor who seeks to comply with the conditions of this exception will *not* be prevented from making a reasonable profit in connection with the access, exchange, or use of EHI, provided that all applicable conditions are met. We emphasize that our intention with this exception is not to set any particular costs that would be considered ''reasonably incurred,'' but rather to allow the market to define the appropriate price so long as certain methods are followed and certain criteria are met as established by the conditions. To be responsive to comments, we have added text in the introductory sentence of this exception that clarifies that fees that result in a reasonable profit margin will be covered by this exception so long as they are in compliance with the conditions in the exception (§ 171.302).

We also appreciate the comments that encouraged us to prohibit all profits under this exception. We considered this approach, but believe that actors should be able to make a reasonable profit margin, subject to the conditions in this exception. The allowance of a reasonable profit margin is necessary to incentivize innovation and allow innovators to earn returns on the investments they have made to develop, maintain, and update innovations that ultimately improve health care delivery and benefit patients. We believe the finalized approach strikes the appropriate balance of addressing the rent-seeking and exclusionary pricing practices noted by the commenters while enabling and supporting innovation. However, to be responsive to these comments related to limiting profits, we added a provision in § 171.302(a)(1)(iv) that the fees an actor charges must be based on costs not otherwise recovered for the same instance of service to a provider and third party. The intent of this provision is that the exception will not apply to practices where an actor charges twice for the same exact service. For example, the exception likely would not apply where an actor charges a hospital for providing a third party that the hospital contracts with access to certain EHI, and then charges that same third party an additional fee for access to the same EHI. This condition creates a necessary guardrail to address potential misuse of this exception that could result in a windfall for certain actors who charge fees for the same services multiple times.

We have also modified other aspects of this final rule that address commenter concerns regarding this exception. First, as discussed previously in this section and in more detail in section VIII.C.3 of this preamble, we have focused the scope of the EHI definition. This change addresses commenters' concerns regarding potential ambiguity regarding the types of information for which profits could be realized. Actors seeking certainty about their practices related to charging fees only need to comply with this exception if their practices interfere with the access, exchange, and use of EHI. We emphasize that we are not limiting the fees and/or profits related to the access, exchange, or use of information outside the scope of EHI. We refer readers to section VIII.C.3 of this preamble for a detailed discussion of focused scope of the EHI definition.

Second, under the finalized information blocking definition, for up to 18 months after the six-month delayed compliance date of the information blocking section of this final rule (part 171) (a total of 24 months after the publication date of this final rule), EHI for purposes of part 171 is limited to the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213 (see (§ 171.103(b)). The fees an actor charges during that time will only be limited pursuant to the conditions in this exception for that subset of EHI.

We note that we revised § 171.302(a)(1)(i) for clarity by limiting the requirement to ''objective and verifiable criteria that are uniformly applied for all *similarly situated* classes of persons and requests'' instead of ''objective and verifiable criteria that are uniformly applied for all *substantially similar or similarly situated* classes of persons and requests.'' We believe the final standard achieves the same goal as the proposed standard and provides a clearer condition for the regulated community to follow. We updated § 171.302(a)(2)(ii) by removing the illustrative language regarding the ''secondary use of such information'' and by removing the proposed language about exceeding the actor's reasonable costs for providing access, exchange, or use of EHI (see 84 FR 7539). The provision finalized in § 171.302(a)(1)(ii)—that an actor's fees must be reasonably related to the actor's costs of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged—achieves the same purpose of limiting fees to those necessary to recover the costs reasonably incurred.

We removed the ''secondary use'' language because it seemed superfluous to include in the regulation text; however, we emphasize that we maintain that the fees an actor charges must *not* be based on the sales, profit, revenue or other value that the requestor or other persons derive or may derive from the subsequent use of EHI. Our policy on this point has not changed from the Proposed Rule. Practices that use this method to recover costs will not

benefit from this exception and may implicate the information blocking provision. Last, we note that we have added ''or entities'' to follow ''person'' to align with the language in § 171.302(a)(1)(ii).

We note, with regard to the ''basis for fees'' and ''excluded fees'' conditions (§ 171.302(a) and (b), respectively), that each provision under these conditions was proposed in the Proposed Rule with the exception of two new provisions: (1) The fees an actor charges must be based on costs not otherwise recovered for the same instance of service to a provider and third party (§ 171.302(a)(1)(iv)); and (2) the fees an actor charges must not be based on any costs that led to the creation of IP, if the actor charged a royalty for that IP pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property (§ 171.302(a)(2)(vi)). We discuss each of these additions in the discussion below. Regarding the conditions that were included in the proposed exception, we note that some of the conditions were in different subsections of the proposed exception and/or have been updated for clarity and consistency with other sections of this final rule. We describe all the substantive changes to these provisions in this preamble, but refer readers to the proposed exception to review the full scope of structural changes and clarifications we have made (see 84 FR 7603).

Comments. We received some comments regarding the scaling of fees and the proposed condition that the method by which the actor recovers its costs must be reasonably allocated among all customers to whom the technology or service is supplied or for whom the technology is supported. Some commenters stated that the notion that costs can be evenly divided among clients is flawed. Commenters requested that ONC allow a fee scale as opposed to a blanket fee structure. Commenters noted that a sliding scale structure would ensure that smaller entities would not be limited by a restrictive pricing application that threatens their operating costs, which may exist on a slim margin. A couple of commenters requested that ONC recognize that for many organizations, especially non-profits, it is common and appropriate for fees to scale with the size of a member/participant organization.

Several HIEs and HINs expressed concern that the proposed condition regarding the reasonable allocation of costs could have the unintended effect of prohibiting the fee structure of many public HIEs/HINs. Commenters noted that many HIEs/HINs choose to charge fees to only a subset of their participants. However, as proposed, the condition that costs be reasonably allocated among all customers could undercut this ability. Commenters emphasized that the ability to offer free services to smaller providers, particularly as HIEs/HINs work to engage providers across the care continuum, is an important flexibility for such organizations. Commenters requested that HIE/HIN membership/participation costs and subscription fees not be considered restricted fees under the information blocking provision.

Response. We thank commenters for these thoughtful comments. We maintain that the condition regarding reasonable allocation of costs in § 171.302(a)(iii) is necessary to ensure that actors do not allocate fees in an arbitrary or anti-competitive manner. The final condition requires that an actor allocate its costs in accordance with criteria that are reasonable and between only those customers that either cause the costs to be incurred or benefit from the associated supply or support of the technology. We have finalized this condition with a modification discussed below.

We agree with commenters that there may be situations when it would be reasonable for an actor to allocate costs differently for different classes of customers. In response to these comments, we have revised the condition in § 171.302(a)(1)(iii) so that the fees an actor charges must be reasonably allocated among all *similarly situated* customers to whom the technology or service is supplied, or for whom the technology is supported. This addition addresses commenters' concerns by providing actors with the discretion to allocate costs differently for different classes of customers, while ensuring that any differences in cost allocation are based on actual differences in the class of customer. For instance, under this provision, fees must be reasonably allocated among all similarly situated large hospital systems (above a certain established size threshold) to whom a technology or service is supplied, or for whom the technology is supported. However, the allocation of fees for the same technology or service could be quite different for a small, non-profit, rural health clinic.

We also note that we have replaced ''customers'' with ''persons or entities'' in § 171.302(a)(1)(iii) in order to align the language with § 171.302(a)(1)(i) and (ii). We believe aligning the provisions within § 171.302(a) will strengthen the exception and provide actor's with clarity regarding what is necessary to meet the exception.

Comments. We received many comments, primarily from providers and provider organizations, regarding the potential financial burden the proposed exception will place on actors. Commenters recommended that ONC carefully consider the downstream financial impact of new requirements, especially that providers, including providers without certified health IT and who do not participate in CMS programs, will bear the brunt of the financial burden of these policies. More specifically, commenters expressed concern regarding potential recordkeeping and administrative burden caused by this exception. Commenters explained that actors may need to retain extensive records to document all of the costs that the actor incurred so that it can prove that its fees only constitute those costs plus a reasonable profit. Further, commenters stated that the administrative burden required to assess and monitor this exception would be significant and not sustainable. Commenters explained that cost accounting is challenging for even very large and well-resourced organizations and there is concern that the exception will result in unintended negative consequences for many actors.

Response. We appreciate these comments. We reiterate that actors may choose to satisfy the conditions of this exception to be certain that the fees they charge for the access, exchange, or use of EHI do not implicate the information blocking provision. We also reiterate that failure to meet the exception does not mean that an actor's practice related to charging fees meets the information blocking definition. However, as we explained in the Proposed Rule, we interpret the broad definition of information blocking in section 3022(a) of the PHSA to encompass *any* fee that is likely to interfere with the access, exchange, or use of EHI (84 FR 7521). Fees that do not meet this exception may implicate the information blocking provision and will have to be assessed on a case-by-case basis to determine, for example, the actor's intent and whether the practice rises to the level of an interference. This exception, as well as the other finalized exceptions, strike a balance by identifying, as the Cures Act requires, activities that interfere with access, exchange, or use of EHI but which are reasonable and necessary.

We believe the overwhelming benefits of the information blocking provision and the exceptions to the information blocking definition—which enable patients to access, exchange, and use their EHI where and when it is

needed—far outweigh the potential burden on actors. We believe the revisions we have made to this exception, the addition of paragraph (b) in the information blocking definition (see § 171.103(b)) and the discussion in section VIII.C of this preamble), the addition of the Content and Manner Exception, as well as the revisions we have made to the other exceptions and relevant terms will have the overall effect of reducing burden on actors. The fact the information blocking section of this rule (part 171) has a 6-month delayed compliance date from the publication date of this final rule will also relieve the burden on actors and give them time to prepare for administrative changes.

Comments. We received comments about the interplay and potential overlap between the proposed Fees Exception and Licensing Exception. Some commenters suggested that we combine the two exceptions for clarity. Some commenters requested clarification as to whether an actor may charge both a fee to recover reasonable costs associated with EHI services and a reasonable royalty for licensing interoperability elements. One commenter expressed concern that the overlap between the two exceptions creates the potential for actors to recover the same costs twice. The commenter explained that licensing of IP is intended to recoup the costs of development of that IP, so where the IP is an interoperability element, the costs reasonably incurred for its development should be incorporated into the royalty rate. The commenter recommended that we should be clearer that, in these circumstances, only a single recovery is permitted.

Response. We thank commenters for the thoughtful feedback and agree that the distinction between the Fees Exception and the Licensing Exception (§ 171.303) must be clear. We emphasize that both exceptions deal with the fees actors may charge regarding the access, exchange, or use of EHI and under both exceptions actors use interoperability elements (as defined in § 171.102) to facilitate the access, exchange, or use of EHI. The exception for recovering costs reasonably incurred enables actors to recover their costs to develop technologies and provide services that enhance interoperability. On the other hand, the exception for licensing interoperability elements specifically addresses circumstances when it is necessary for an actor to *license* interoperability elements in order fulfill a request to access exchange, or use EHI. The Licensing Exception deals with the requisite licensing conditions. We believe there should be a distinction made between these two exceptions, and have therefore decided not to combine the two exceptions.

We agree with the commenter that actors should *not* be able to recover the same costs twice and have added a provision in § 171.302(a)(2)(vi) that the fees an actor charges must not be based on any costs that led to the creation of IP, if the actor charged a royalty for that IP pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.

Excluded Fees Condition

We proposed that certain costs should be explicitly excluded from the exception regardless of the method for recovering the costs (84 FR 7540).

Comments. We did not receive comments regarding the overall proposed approach of excluding certain costs from this exception.

Response. We have finalized the structure of this exception to exclude certain fees with the changes described in the discussions above and below. We note that we have substituted the ''or'' that preceded the final excluded fee in the proposed exception (see 84 FR 7603) with an ''and'' in the final exception. This is not a substantive change, as our intent has always been that the exception does not apply to *each* of ''excluded fees.'' This revision clarifies that point.

Costs Due to Non-Standard Design or Implementation Choices

We proposed that this exception would not permit the recovery of any cost that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI. To the extent that such costs can be reasonably avoided, we stated that we believe that actors should internalize the costs of such behaviors, which do not benefit consumers, and which create unnecessary impediments to access, exchange, and use of EHI. We requested comments on the proposed exclusion of these types of costs from the exception (84 FR 7540).

Comments. We received several comments regarding the proposed exclusion of costs due to non-standard design or implementation choices from this exception. A couple of commenters expressed support for the proposal. A couple of other commenters disagreed with the proposal and recommended that actors should be able to recover all reasonable implementation costs independent of design decisions. One commenter requested additional clarity about what ''non-standard'' means. A couple of commenters noted that requestors may prefer information in a non-standard manner to meet their business purposes, due to their own constraints, or for other reasons.

Response. We thank commenters for their support of this proposal, as well as the constructive feedback. We emphasize that the problematic nature of non-standard implementation choices was identified by Congress in the Cures Act. Section 3022(a)(2)(B) of the PHSA states that information blocking may include implementing health IT in non-standard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI. Due to Congress's clear objective to restrict these practices, along with our continued concern that these practices will lead to unnecessary complexity and burden related to the access, exchange, or use of EHI, we have finalized the proposed provision regarding non-standard design and implementation choices. We have updated § 171.302(a)(2)(iii) to address comments indicating that requestors may prefer information in a non-standard manner to meet their business purposes, due to their own constraints, or for other reasons. We agree with commenters that in those situations—when the requestor requests access, exchange or use of EHI in the non-standard way—the exception should allow the actor to charge fees for the reasonable costs associated with the requested non-standard design or implementation. We emphasize, however, and make clear in § 171.302(a)(2)(iii), that such fees related to non-standard design or implementation are *only* covered by the exception when the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use EHI. We note that this provision was proposed as an ''excluded cost'' but has been finalized within the ''Basis for fees condition'' for clarity and to align with the revised structure of this exception.

We also note that the new Content and Manner Exception in § 171.301 further addresses commenter concerns because it provides actors with clear procedures regarding the manner in which they may provide access, exchange, or use of EHI if they are technically unable to respond in the manner requested or the manner requested requires the actor to license intellectual property and the actor cannot reach agreeable terms with the requestor (discussed in section VIII.D.2.a of this preamble). If an actor

meets that exception, its practice would not implicate the information blocking provision. For instance, if a requestor requested that the actor provide EHI in a non-standard manner, but the actor is technically unable to provide the EHI in the manner requested, the actor's response to the request would not implicate the information blocking provision if it provides the EHI via an alternative manner in accordance with § 171.301(b). The actor could also potentially seek coverage under the Infeasibility Exception if the request is infeasible and the actor meets all the conditions in § 171.204.

Regarding the comment concerning additional clarity about what ''non-standard'' means, we explained and provided examples in the Proposed Rule of practices related to implementing health IT in non-standard ways that substantially increase the complexity or burden of accessing, exchanging, or using EHI, and therefore implicate the information blocking provision (84 FR 7521). In addition, the Cures Act specifically describes information blocking practices to include implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information (see section 3022(a)(2)(B) of the PHSA). Therefore, the Proposed Rule discussion regarding non-standard ways of implementing health IT also applies for purposes of the Fees Exception. As explained in the Proposed Rule, non-standard implementation of health IT may arise where an actor chooses not to adopt, or to materially deviates from, relevant standards, implementation specifications, and certification criteria adopted by the Secretary under section 3004 of the PHSA (84 FR 7521). Even where no federally adopted or identified standard exists, if a particular implementation approach has been broadly adopted in a relevant industry segment, deviations from that approach will be suspect unless strictly necessary to achieve substantial efficiencies. For further discussion regarding our rationale for this provision, as well as specific, non-exhaustive examples of conduct that would be likely to interfere with the access, exchange, or use of EHI, we refer readers to the Proposed Rule (84 FR 7521).

Subjective or Speculative Costs

We proposed to limit this exception to the recovery of costs that an actor *actually* incurred to provide the relevant interoperability element or group of elements (which may comprise either products or services). We proposed that the exception would not permit the recovery of certain types of costs that are subjective or speculative. We noted two important examples of this limitation. First, we proposed that an actor would not be permitted to recover any costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets. For example, an actor could not charge a customer a fee based on the purported ''cost'' of allowing the customer to use the actor's patented technology, computer software, databases, trade secrets, copyrighted works, and the like. We noted that the customer's use of the asset could be considered a ''cost'' in the sense that, were it not for the information blocking provision, the actor could charge a royalty or other fee for the use of its intangible assets. For this reason we proposed to permit an actor to license most interoperability elements on reasonable and non-discriminatory terms, subject to certain conditions. For purposes of this more general exception, however, we explained that it would be inappropriate to permit an actor to charge a fee based on these considerations, which are inherently subjective and could invite the kinds of rent-seeking and opportunistic pricing practices that fall squarely within the definition of information blocking. We proposed that an actor's practices could qualify for both this exception (Fees Exception) and the Licensing Exception (finalized in § 171.303). In that case, the actor could recover costs under both exceptions (84 FR 7540).

Second we stated the exception would not apply to ''opportunity costs,'' such as the revenues that an actor could have earned had it not provided the interoperability elements. We clarified that the exclusion of opportunity costs would not preclude an actor from recovering its reasonable forward-looking cost of capital (84 FR 7540).

Comments. We did not receive any comments on our proposals regarding subjective or speculative costs.

Response. We have finalized this provision as proposed with some modifications for clarity. We have modified the provision regarding intangible assets in § 171.301(a)(2)(iv) by removing the parenthetical that noted that such costs include the depreciation or loss of value. The parenthetical was illustrative and was not necessary in the regulation text, as it is just one of the many types of intangible assets on which a fee must not be based. We have also modified the provision regarding opportunity costs in § 171.301(a)(2)(v) by clarifying that the specific opportunity costs on which a fee must *not* be based are those *unrelated* to the access, exchange, or use of EHI instead of the proposed qualifying language of ''except for the reasonable forward-looking cost of capital'' (see 84 FR 7603). We believe this finalized language is clearer than the proposed language. In addition, it is more precise than the proposed language because it creates a connection to the information blocking definition. We note that we proposed these provisions as ''excluded costs'' (see 84 FR 7603) but have finalized them within the ''Basis for fees condition'' for clarity.

Fee Prohibited by 45 CFR 164.524(c)(4)

We also proposed that the exception would not apply to fees prohibited by 45 CFR 164.524(c)(4). We noted in the Proposed Rule that the HIPAA Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) Labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (*e.g.,* CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual (45 CFR 164.524(c)(4)). The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law (84 FR 7540).

Comments. We received a couple of comments regarding copying fees allowed under the HIPAA Privacy Rule. One commenter stated that reasonable, cost-based fees for certain costs, consistent with the HIPAA Privacy Rule individual access provisions, should not be allowed under the exception. One commenter requested that ONC harmonize the exception with the HIPAA Privacy Rule provisions that govern the charging of fees for electronic copies of medical records.

Response. We appreciate these comments. We have decided to finalize the provision as proposed, which harmonizes this part of the exception (§ 171.302) with those provisions of the HIPAA Privacy Rule. The exception does not apply to fees prohibited by 45 CFR 164.524(c)(4). Consistent with the

HIPAA Privacy Rule's individual access fee implementation specification, an actor can charge a reasonable, cost-based fee related to certain costs (described above) if a patient requests a copy of her records.

Individual Electronic Access

We proposed that the exception would not apply if the actor charged a fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's EHI. We stated that such fees are distinguished from the cost-based fees that a covered entity is permitted to charge individuals for the provision of copies of ePHI under the HIPAA Privacy Rule access provisions (45 CFR 164.524(c)(4)), and similar allowable costs under State privacy laws, which would *not* be excluded from the costs recoverable under the exception. We clarified that access to EHI that is provisioned by supplying some form of physical media, such as paper copies (where the EHI is printed out), or where EHI is copied onto a CD or flash-drive, would not be a practice that implicated the information blocking provision provided that the fee(s) charged for that access complied with the HIPAA Privacy Rule access provisions (45 CFR 164.524(c)(4)) (84 FR 7540).

We stated that a fee based on electronic access by an individual or their personal representative, agent, or designee to the individual's EHI, in contrast, would arise if an actor sought to impose on individuals, or their personal representatives, agents, or designees, a fee that operated as a toll to electronically access, exchange, or use EHI. For example, a health care provider that charges individuals a fee in order for the individuals to receive access to their EHI via the health care provider's patient portal or another internet-based method, would not be able to benefit from this exception. Similarly, where an individual authorizes (approves) a consumer-facing app to receive EHI on the individual's behalf, the exception would not apply to practices where an actor charges the app or its developer a fee to access or use APIs that enable an individual's access to the individual's EHI. We explained that this would be true whether the actor is a supplier of the API technology or an individual or entity that has deployed the API technology, such as a health care provider (84 FR 7540).

Comments. Commenters expressed overwhelming support for our proposal regarding individual electronic access. Commenters from across stakeholder groups emphasized that patients have a fundamental right to access their data and should be able to access, exchange, and use their EHI at no charge. Commenters emphasized that the EHI belongs to the patient, and neither health care providers, EHR developers, nor payers should profit from the sale of EHI, as that will only serve to limit data transfer, increase health care costs, and adversely affect patient care.

Commenters strongly supported our proposal (within the API Condition of Certification) that API fees should not be a barrier in allowing patient access to their EHI (see proposed § 170.404 and 84 FR 7487 through 7491). They stressed that neither individuals nor app developers (*i.e.,* API Users) should be charged a fee for API uses that are associated with the access, exchange, and use of EHI by patients or their applications, technologies, or services. Several commenters supported our efforts to bolster patient access, noting that the capacity to offer a patient access to EHI, through an API, without cost, is well-supported in the Proposed Rule. One commenter requested that we differentiate between an individual electronically accessing EHI and third parties, at the direction of the individual, electronically accessing EHI.

Response. We thank commenters for the support and have finalized this provision as proposed with a slight modification to the text in § 171.302(b)(2) and clarification of the meaning of electronic access, which we have codified in § 171.302(d). We have reordered the language for clarity and, in order to clarify the terms ''agent'' and ''designee,'' we have replaced them with ''another person or entity designated by the individual.'' These other individuals or entities (*e.g.,* a third-party app) receive access to EHI at the direction of the individual and individuals control whether the third-party receives access to the individual's EHI. This modification is merely a clarification of our proposal and is not a substantive change as we clearly stated in the Proposed Rule that, as summarized above, this exception would not apply to practices where an actor charges the *app or its developer* a fee to access or use APIs that enable access to the individual's EHI. Fees can be a method of interfering with the access, exchange, and use of EHI, as we have emphasized in the Proposed Rule and this final rule. When it comes to an individual's electronic access to their EHI, we believe that any fee, whether direct or indirectly passed on through a fee charged to a third-party app that the individual has chosen to facilitate access to their EHI, could interfere with an individual's access and use of their EHI. ONC's implementation of the Cures Act is predicated on an understanding that access to EHI should not be treated as a commodity that should be traded or sold. ONC takes this approach because we view patients as having an overwhelming interest in EHI about themselves, and because we understand that the true value of EHI can only be realized if it is available where and when it is needed, including providing electronic access to patients. Patients have already effectively paid for their health information, either directly or through their employers, health plans, and other entities that negotiate and purchase health care items and services on their behalf. We have codified this provision in § 170.302(b)(2) to not permit ''[a] fee based in any part on the electronic access of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual.''

For purposes of the Fees Exception, we define electronic access to mean an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request (§ 171.302(d)). We discussed the meaning of ''electronic access'' in the Proposed Rule (see 45 FR 7540). We have defined ''electronic access'' in § 171.302(d) in this final rule consistent with the Proposed Rule, including distinguishing it from the methods and efforts we cited in the Proposed Rule that we did not consider electronic access and for which a fee could be charged (see 45 FR 7540). We have chosen ''internet-based method'' in lieu of the proposed ''web-based delivery'' because it more technically aligns with the concept we were attempting to convey in the Proposed Rule. Such methods would be, as described in part in the Proposed Rule, access via an API, patient portal, or other internet-based means. To note, the 2015 Edition ''view, download, and transmit to 3rd party'' certification criterion uses this same concept of ''internet-based'' to convey that ''patients (and their authorized representatives) must be able to use *internet-based technology* to view, download, and transmit. . . .'' In terms of fulfilling a request without manual effort, we clarify that it entails the completion of the process where there is *no* manual effort involved to meet the request at the time of the request. To illustrate the inverse, we recognize that there are times that manual effort may be involved in collating or assembling EHI from various systems in response to a request. In such instances, this provision (§ 170.302(b)(2)) would not

apply to the costs of those efforts because the efforts would not fall under the definition of ''electronic access.''

We reaffirm that this exception would not apply to an actor that charges individuals a fee in order for the individuals to receive access to their EHI using an internet-based delivery method, including where an individual uses consumer-directed technology (*e.g.,* patient-chosen apps, personal health apps, standalone/untethered personal health records (PHR), email) to request and/or receive their EHI. This includes sharing it with an entity designated by the individual (*e.g.,* allowing individuals to donate/share EHI with a biomedical research program of the individual's choice). Practices that involve an actor charging an individual (or the individual's personal representative or another person or entity designated by the individual) a fee to access, exchange, or use their EHI would be inherently suspect and would be extremely likely to implicate the information blocking provision. We emphasize that practices that do not meet this condition, or any other conditions in the Fees Exception, would be subject to case-by-case review (unless another exception applies). We further refer readers to our discussion of ''interfere with'' or ''interference,'' including examples of practices that would likely interfere with access, exchange, and use of EHI (section VIII.C.6).

Export and Portability of EHI Maintained in EHR Systems

We explained in the Proposed Rule that the definition of information blocking specifically mentions transitions between health IT systems and the export of complete information sets as protected forms of access, exchange, and use (see section 3022(a)(2)(C)(i) of the PHSA). We noted that in our experience, health care providers frequently encounter rent-seeking and opportunistic pricing practices in these and other contexts in which they are attempting to export EHI from their systems for use in connection with other technologies or services that compete with or could reduce the revenue opportunities associated with an EHR developer's own suite of products and services. We explained that most EHI is currently maintained in EHRs and other source systems that use proprietary data models or formats; this puts EHR developers in a unique position to block the export and portability of EHI for use in competing systems or applications, or to charge rents for access to the basic technical information needed to facilitate the conversion or migration of data for these purposes. We emphasized that our concerns are compounded by the fact that EHR developers rarely disclose in advance the fees they will charge for data export and data portability services (see 80 FR 62719; 80 FR 16880 and 81).

For these reasons, we proposed that fees charged for the export, conversion, or migration of data from an EHR technology would not qualify for this exception unless they also meet two additional conditions. First, we proposed that health IT developers of certified health IT would, for purposes of the exception, be precluded from charging a fee to perform an export of EHI via the capability of health IT certified to the proposed 2015 Edition ''EHI export'' certification criterion for the purposes of supporting single patient EHI export upon a valid request from that patient or a user on the patient's behalf, or supporting the export of all EHI when health care provider chooses to transition or migrate information to another health IT system. We stated that, as part of the ''Assurances'' Condition of Certification, health IT developers that produce and electronically manage EHI would need to be certified to the criterion and provide the functionality to its customers. We stated that fees or limitations associated with the *use* of the ''EHI export'' certification criterion (as distinguished from deployment or other costs reasonably incurred by the developer) would not receive protection under the exception and may be suspect under the information blocking provision (84 FR 7541).

We clarified that the condition would not preclude a developer from charging a fee to deploy the ''EHI export'' certification criterion in a health care provider's production environment, or to provide additional services in connection with this capability other than those reasonably necessary to enable its intended use. For example, we explained that this condition would not preclude a developer from charging a fee to perform an export of EHI via the capability of health IT certified to the proposed § 170.315(b)(10) for a third-party analytics company. We noted in the Proposed Rule that, because the certification criterion provides only a baseline capability for exporting data, we anticipated that health IT developers of certified health IT will need to provide other data portability services to facilitate the smooth transition of health care providers between different health IT systems. We proposed that such fees may qualify for protection under the exception, but only if they meet the other conditions described above and in proposed § 171.205(a).

Second, we proposed that the exception would not apply to a fee to export or convert data from an EHR technology unless such fee was agreed to in writing at the time the technology was acquired, meaning when the EHR developer and the customer entered into a contract or license agreement for the EHR technology (84 FR 7541).

Comments. A commenter requested clarification regarding the proposal to exclude from the exception costs related to fees to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired. The commenter asked that ONC clarify if this provision is applicable to export or the conversion of EHI from certified health IT or if it is applicable to any export or conversion of EHI from any health IT. The commenter also requested that ONC clarify if this provision is prospective in nature, meaning it would only apply to agreements entered into after the effective date of a final rule. The commenter recommended that ONC change the focus of this proposal so that it only requires that the parties agree in writing that fees of a particular nature may be charged for the export of EHI.

Response. We appreciate this comment. In response to the comment, we clarify that this exclusion from the exception is not limited to the export of EHI from certified health IT. Instead, this provision applies to the export or conversion of any EHI from an actor's technology(ies). As we discuss elsewhere in this Final Rule, we interpret the information blocking provision broadly such that practices of a health IT developer of certified health IT that do not pertain specifically to certified health IT may implicate the information blocking provision. Consistent with this interpretation of the information blocking provision, the exception will not protect practices where an actor charges fees to export or convert data from any EHR technology, unless such fee was agreed to in writing at the time technology was acquired. Further, we clarify that if a fee to export or convert data is not subject to this exclusion in § 171.302(b)(4) because it was agreed to in writing, it still must meet the other applicable conditions in § 171.302 to be covered by the Fees Exception.

Without this exclusion, actors may seek to take advantage of the exception and enable rent-seeking or opportunistic pricing practices. Thus, we have decided not to limit the condition so that it only requires that the parties

agree in writing that fees of a particular nature may be charged for the export of EHI as suggested by the commenter. Only requiring the parties to agree to the fee in writing (without applying the other conditions in this exception), may allow an actor to charge an unreasonable fee or engage in a practice that is likely to interfere with the access, exchange, or use of EHI. While a party may agree to pay a fee under specific circumstances, that agreement does not change the fact that the fee must be reasonably related to the actor's costs or may otherwise interfere with the access, exchange, or use of EHI.

We have finalized these provisions as proposed with a slight modification. We changed the condition from ''A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired'' (see 84 FR 7603) to ''A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired'' (§ 171.302(b)(4)). We made this change for clarity based on the change we made to the introductory language in the exception, that a practice will not be considered information blocking when the practice meets the conditions in paragraph (a), does not include any of the excluded fees in paragraph (b), and, as applicable, meets the condition in paragraph (c). This modification does not change the substance of this condition in any way.

Compliance With the Conditions of Certification

We stated in the Proposed Rule that health IT developers of certified health IT subject to the API Condition of Certification may not charge certain types of fees and are subject to more specific cost accountability provisions than apply generally under this proposed exception. We noted that the failure of developers to comply with these additional requirements would impose impediments to consumer and other stakeholder access to EHI without special effort and would be suspect under the information blocking provision. We proposed, therefore, that a health IT developer of certified health IT subject to the API Condition of Certification must comply with all requirements of that condition for all practices and at all relevant times in order to qualify for the exception (84 FR 7541).

We also stated that a health care provider that acts as an API Data Provider should be subject to the same constraints. We noted that the API Condition of Certification prohibits a health IT developer from charging a usage fee to patient-oriented apps. We noted that information blocking concerns would arise if a provider were to charge such a fee, notwithstanding the fact that the provider is not subject to the certification requirements. For this reason, we proposed that, if the actor is an API Data Provider, the actor would only be permitted to charge the same fees that an API Technology Supplier would be permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification (84 FR 7541).

Comments. We did not receive comments on these proposals.

Response. We have finalized the first provision detailed above as proposed with a slight modification for clarity. The final provision in § 171.302(c) states: Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4), § 170.404, *or both* of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times. We added ''or both'' into the final language because a health IT developer could be subject to both § 170.402(a)(4) and § 170.404 and in such instances would be covered by this provision.

We have removed the second provision detailed above regarding a health care provider that acts as an API Data Provider (see the Proposed Rule at 84 FR 7603) for clarity, as not all of the permitted fees specified in the API Condition of Certification (§ 170.404) are applicable for API Data Providers.

Application of the Exception to Individual Practices

We stated in the Proposed Rule that the conditions of this exception, including those governing the methodology and criteria by which an actor calculates and distributes its costs, must be satisfied for *each and every* fee that an actor charges to a customer, requestor, or other person for accessing, exchanging, or using EHI. All applicable conditions of the exception must be met at all relevant times for each practice (84 FR 7541).

Comments. We did not receive any comments on this proposed policy.

Response. We have finalized this policy as proposed.

c. Licensing Exception—When will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?

We proposed in the Proposed Rule in § 171.206 to establish an exception to the information blocking provision that would permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, provided that certain conditions are met. We proposed that the information blocking provision would be implicated if an actor were to refuse to license or allow the disclosure of interoperability elements to persons who require those elements to develop and provide interoperable technologies or services—including those that might complement or compete with the actor's own technology or services (84 FR 7544). Moreover, we proposed that the information blocking provision would be implicated if the actor licensed such interoperability elements subject to terms or conditions that have the purpose or effect of excluding or discouraging competitors, rivals, or other persons from engaging in these pro-competitive and interoperability-enhancing activities. Thus, we proposed the Licensing Exception would apply in both vertical and horizontal relationships and provided an example emphasizing that point in the Proposed Rule (see 84 FR 7544).

We noted in the Proposed Rule that some licensees do not require interoperability elements to develop products or services that can be interoperable with the actor's health IT. We explained that there may be firms that simply want to license the actor's technology for use in developing their own interoperability elements. Their interest would be for access to the technology itself—*not* for the use of the technology to interoperate with either the actor or its customers to enable the access, exchange, or use of EHI. We emphasized that in such cases, the actor's licensing of its intellectual property (IP) in such a context would *not* implicate the information blocking provision (in other words, would not be in scope for information blocking). For a non-exhaustive list of examples of situations that *would* implicate the information blocking provision, see the Proposed Rule (84 FR 7544–45).

In our experience, contractual and IP rights are frequently used to extract unreasonable rents for access to EHI or to prevent competition from developers of interoperable technologies and services. These practices frustrate access, exchange, and use of EHI and stifle competition and innovation in the health IT sector. As a case in point, we noted in the Proposed Rule that even following the enactment of the Cures Act, some health IT developers had been selectively prohibiting—whether expressly or through commercially unreasonable terms—the disclosure or

use of technical interoperability information required for third-party applications to access, exchange, and use EHI maintained in EHR systems. We noted that such practices limit health care providers' use of the EHI maintained on their behalf to the particular capabilities and use cases that their EHR developer happens to support. More than this, by limiting the ability of providers to choose what applications and technologies they can use with their EHR systems, we indicated that these practices close off the market to innovative applications and services that providers and other stakeholders need to deliver greater value and choice to health care purchasers and consumers (84 FR 7545).

Despite these serious concerns, we recognized in the Proposed Rule that the definition of information blocking may be broader than necessary and could have unintended consequences. We proposed that it is generally appropriate for actors to license their IP on RAND terms that do not interfere with access, exchange, or use of EHI provided certain conditions were met. We explained that these practices would further the goals of the information blocking provision by allowing actors to protect the value of their innovations and earn returns on the investments made to develop, maintain, and update those innovations. We explained that this would protect future incentives to invest in, develop, and disseminate interoperable technologies and services. Conversely, we explained that if actors cannot (or believe they cannot) protect and commercialize their innovations, they may not engage in these productive activities that improve access, exchange, and use of EHI (84 FR 7545).

We proposed that the exception would be subject to strict conditions to ensure, among other things, that actors license interoperability elements on RAND terms and that actors do not impose collateral terms or engage in other practices that would impede the use of the interoperability elements or otherwise undermine the intent of the exception (84 FR 7545). We acknowledged that preventing IP holders from extracting rents for access to EHI may differ from standard IP policy. We proposed that absent specific circumstances, IP holders are generally free to negotiate with prospective licensees to determine the royalty to practice their IP, and this negotiated royalty frequently reflects the value the licensee would obtain from exercising those rights. However, in the context of EHI, we proposed that a limitation on rents is essential due to the likelihood that rents will frustrate access, exchange, and use of EHI, particularly because of the power dynamics that exist in the health IT market (84 FR 7545).

We also emphasized that actors are not required to seek the protection under this (or any other) exception. We explained that if an actor does not want to license a particular technology in accordance with the exception, it may choose to comply with the information blocking provision in another way, such as by developing and providing alternative means of accessing, exchanging, and using EHI that are similarly efficient and efficacious (84 FR 7545).

Comments. We received many comments in support of this proposed exception. One commenter highlighted the significance of the exception, noting that data is often locked in proprietary software systems, at times preventing providers from being able to connect and exchange information. Some commenters requested additional examples and that ONC issue guidance to assist actors in understanding how they can determine whether a request to license is valid, when this exception would apply, and what steps actors would be required to take to attain coverage under the exception. A couple of commenters suggested that there should be a distinction between requests to license interoperability elements to facilitate a patient's treatment or individual access versus requests that are simply for the requestor's own business purposes, such as commercializing a competing product. A couple of commenters requested additional provisions in the final rule to improve transparency regarding licensing of interoperability elements. Commenters recommended that ONC require regulated actors who engage in RAND licensing of interoperability elements to publish either standard licensing rate offers or actual licenses.

Response. We thank commenters for their support for this exception as well as the constructive feedback. We may consider developing materials in the future regarding the application of the exceptions should the need arise. However, we believe the final rule clearly describes the conditions actors must meet in order to be covered by each exception, and informational materials are not necessary at this time.

We appreciate the comments that recommended that there should be a distinction between requests for licensing of interoperability elements to facilitate a patient's treatment or individual access versus requests that are simply for the requestor's own business purposes. We emphasize that we made such a distinction in the Proposed Rule and we reiterate that distinction here in the final rule. In order for an actor to consider licensing its interoperability elements under this exception, the requestor would need to have a claim to the underlying, existing EHI for which the interoperability element would be necessary for access, exchange, or use (see the Privacy Exception discussion in VIII.D.1.b). An actor will not implicate the information blocking provision and does not need to seek coverage under this exception in circumstances where the entity requesting to license or use the interoperability element is not seeking to use the interoperability element to interoperate with either the actor or the actor's customers in order for EHI to be accessed, exchanged, or used. For instance, an actor would not need to consider licensing its interoperability elements in accordance with this exception to a firm that requested a license solely for that firm's use in developing its own technologies or business when *no* EHI is sought to be accessed, exchanged, or used. In other words, if there is no nexus between a requestor's need to license an interoperability element and existing EHI on one or more patients, an actor does *not* need to consider licensing the interoperability element requested in accordance with this exception. For example, if a developer of certified health IT included proprietary APIs in its product to support referral management, it would *not* need to license the interoperability element(s) associated with those referral management APIs simply because a requestor ''knocked on the actor's door'' and asked for a license with no EHI involved. The license request from a requestor *must always be based on a need* to access, exchange, or use EHI at the time the request is made—*not* on the requestor's prospective intent to access, exchange, or use EHI at some point in the future.

We appreciate the recommendation that ONC should require regulated actors who license interoperability elements to publish either standard licensing rate offers or actual licenses. However, we have decided not to finalize such a requirement because we believe actors should have discretion to decide whether to publish their licensing rates and/or licenses. We believe this exception will still effectively regulate the licensing of interoperability elements even if it does not require the publication of such rates and licenses. Nonetheless, we commend

commenters' desire to enhance transparency in the final rule and will continue to consider steps to further promote transparency regarding our information blocking policies in future rulemakings.

We note that we have changed the title of this exception from ''Exception—Licensing of interoperability elements on reasonable and non-discriminatory terms'' to ''When will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?'' Throughout this final rule preamble, we use ''Licensing Exception'' as a short form of this title, for ease of reference. As stated in Section VIII.D of this final rule preamble, we have changed the titles of all of the exceptions to questions to improve clarity. We have also edited the wording of the introductory text in § 171.303, in comparison to that proposed (84 FR 7602), so that it is consistent with the finalized title in § 171.303. We believe these conforming changes in wording of the introductory text also improve clarity in this section.

Comments. We received many comments requesting greater clarity and precision regarding key terms within the proposed exception in order to clarify the scope and application of the exception.

Response. We appreciate these comments and agree with commenters that it is essential that our final policies are clear, administrable, and actionable. Accordingly, we have made several updates to this exception as well as to terms and concepts that apply broadly throughout the information blocking section. Notably, we have: (1) Revised the definition of interoperability element (see section VIII.C.3.b); (2) clarified the process and timeframe for negotiating a license (see the discussion later in this section of the preamble); (3) removed the ''RAND'' framework, which commenters noted was confusing (see the discussion later in this section of the preamble); and (4) clarified the relationship between this exception and the Fees Exception (see § 171.302 and the discussion later in this section of the preamble).

Comments. A few commenters requested clarification regarding whether the information blocking provision, and particularly this exception, applies to all licensing agreements already in effect; only licensing agreements that were entered into following the effective date of the Cures Act; or only those licensing agreements entered into after the effective date of ONC's final rule. Commenters recommended that licensing agreements that were entered into prior to the effective date of the final rule should be considered valid and effective. Commenters also recommended that all negotiations and licensing agreements entered into after the effective date of ONC's final rule should comply with the requirements of the final rule. Commenters requested that if ONC plans to enforce provisions of the final rule retroactively, ONC should allow actors to review and renegotiate licensing agreements for compliance with the terms at the request of the licensee.

Response. We thank commenters for these comments. We emphasize that actors are expected to be in full compliance with the information blocking provision when this rule becomes effective. We note that the information blocking section of this final rule (part 171) will not become effective until 6 months after the publication date of the final rule. We believe this delayed compliance date will provide actors with adequate time to assess their existing licensing contracts or agreements and make appropriate changes and amendments to comply with this final rule.

OIG and ONC are coordinating timing of the compliance date of the information blocking section of this final rule (45 CFR part 171) and the start of information blocking enforcement. We are providing the following information on timing for actors. Enforcement of information blocking CMPs in section 3022(b)(2)(A) of the PHSA will not begin until established by future notice and comment rulemaking by OIG. As a result, actors would not be subject to penalties until CMP rules are final. At a minimum, the timeframe for enforcement would not begin sooner than the compliance date of this final rule and will depend on when the CMP rules are final. Discretion will be exercised such that conduct that occurs before that time will not be subject to information blocking CMPs.

We are aware that some actors may currently have in place licensing agreements that contravene the information blocking provision and do not meet the requisite conditions for this exception. We expect actors in these situations to take immediate steps to come into compliance with the information blocking provision by amending their contracts or agreements to eliminate or void any clauses that contravene the information blocking provision. We emphasize that an existing license is no excuse or justification for information blocking. One of the ways we have heard that actors interfere with the access, exchange, and use of EHI is through formal restrictions, such as discriminatory licensing agreements, and this final rule, as well as this exception, seek to address those very circumstances and situations.

Comments. One commenter expressed concern about this exception on privacy and security grounds. The commenter noted that a proliferation of EHI to a multitude of entities who have not and cannot be vetted is likely to increase the risks to the privacy and security of such data and create secondary and tertiary markets for such data without clear regulation and oversight.

Response. We appreciate this comment and understand that the secondary use of data creates privacy and security challenges in the health care industry and beyond. We refer readers to section VIII.C.6 of this preamble for a detailed discussion of how we are addressing this issue in this rule.

i. Responding to Requests

We proposed that, upon receiving a request to license or use interoperability elements, an actor would be required to respond to the requestor within 10 business days from receipt of the request. We noted that the request could be made to ''license'' or ''use'' the interoperability elements because a requestor may not always know that ''license'' is the legal mechanism for ''use'' when making the request (84 FR 7546).

In order to meet this condition, we proposed that the actor would be required to respond to the requestor within 10 business days from the receipt of the request by: (1) Negotiating with the requestor in a RAND fashion to identify the interoperability elements that are needed; and (2) offering an appropriate license with RAND terms, consistent with its other obligations under the exception. We emphasized that, in order to qualify for the proposed exception, the actor would only be required to *negotiate* with the requestor in a RAND fashion and to *offer* a license with RAND terms. We proposed that the actor would not be required to *grant* a license in all instances. We did not propose a set timeframe for when the negotiations must be resolved (84 FR 7546).

We requested comment on whether 10 business days is an appropriate amount of time for the actor to respond to the requestor. We noted that we considered proposing response timeframes ranging from 5 business days to 15 business days. We also considered proposing two separate timeframes for: (1) Negotiating

with the requestor; and (2) offering the license. We stated that if commenters prefer a different response timeframe or approach than proposed, we requested that commenters explain their rationale with as much detail as possible. In addition, we requested comment on whether we should create set limits for: (1) The amount of time the requestor has to accept the actor's initial offer or make a counteroffer; (2) if the requestor makes a counteroffer, the amount of time the actor has to accept the requestor's counteroffer or make its own counteroffer; and (3) an allowable number of counteroffers in negotiations (84 FR 7546).

Comments. We received many comments regarding the proposed framework and timeframe for responding to requests to license or use interoperability elements. Some commenters were supportive of our proposal and stated that 10 business days is an appropriate amount of time for the actor to respond to the requestor. Other commenters disagreed with the proposed timeframe, explaining that 10 business days is insufficient time to begin a license negotiation. Commenters suggested various alternate timeframes ranging from 20 to 90 business days. One commenter requested that ONC consider differentiating the timeline expected for making an offer predicated on an interoperability element being available as an existing capability, as opposed to an interoperability element requiring new formal licensure or requiring one off ''custom'' or ''spec'' development. Another commenter recommended that the process be divided into a series of steps with a requirement that a request for information be acknowledged and negotiations begin within 10 business days and completed within 20 business days. One commenter recommended that the 10-day timeframe be for beginning negotiations with the intent to furnish a quotation for a license. Some commenters stated that timeframes should not be set, as the license negotiation process is highly variable based on the specific requestor and circumstances. One commenter expressed concern that the proposed exception would increase the administrative burden on covered entities, particularly regarding the response timeframe and the actor's inability to review and/or vet the appropriateness of a request before responding.

Response. We thank commenters for these thoughtful comments. To be responsive to comments, we have updated the response and license negotiation framework and timeframe. The finalized provision in § 171.303(a) states that, upon receiving a request to license an interoperability element for the access, exchange, or use of EHI, the actor must: (1) Begin license negotiations with the requestor within 10 business days from receipt of the request (§ 171.303(a)(1)); and (2) negotiate a license with the requestor, subject to the licensing conditions in paragraph (b) of the exception, within 30 business days from receipt of the request (§ 171.303(a)(2)). We note that the expectation in (2) above is that the actor will negotiate with the requestor in good faith. If it is determined that the negotiation is not in good faith, the actor would not qualify for this exception. These provisions create a clear and administrable timeline for actors to follow that is informed by stakeholder comments and will reduce potential burden on actors. Further, it provides actors with appropriate flexibility for negotiating a good faith license, taking into consideration the potential complexity and variability associated with negotiations for licensing interoperability elements.

In instances when an actor is unable to negotiate a good faith license subject to the requirements in § 171.303(a)(2), the actor may not meet the conditions of this exception. As part of an information blocking investigation, ONC and OIG may consider documentation or other writings maintained by the actor around the time of the request that indicate why the actor was unable to meet the conditions. This would not permit the actor to be covered by this exception, but discretion in determining whether to enforce the information blocking provision may be exercised.

We note that we have revised paragraph § 171.303(a) by changing ''a request to license *or use*'' to ''a request to license'' for clarity. We emphasize, however, that this change does not alter the meaning or application of the provision. We reiterate, as we proposed, that the request could be made to ''license'' or ''use'' the interoperability elements because a requestor may not always know that ''license'' is the legal mechanism for ''use'' when making the request (see 84 FR 7546). We believe it is unnecessary to include ''or use'' in the regulation text because actors should know that a request to ''use'' would be synonymous with a request to ''license'' and would thus be covered by this exception. Further, the inclusion of ''or use'' could be confusing since ''use'' is a defined term in the context of ''access, exchange, or use'' of EHI, but would carry different meaning in the context of ''using'' an interoperability element, as opposed to ''using'' EHI.

ii. Licensing Conditions

We proposed to require, as a condition of this exception, that any terms upon which an actor licenses interoperability elements must be reasonable and non-discriminatory (RAND). We recognized in the Proposed Rule that strong legal protections for IP rights can promote competition and innovation. Nevertheless, IP rights can also be abused in ways that undermine these goals. We explained that we believe this potential for abuse is heightened when the IP rights pertain to functional aspects of technology that are essential to enabling interoperability. We emphasized that to the extent that the interoperability elements are essential to enable the efficient access, exchange, or use of EHI by particular persons or for particular purposes, any practice by the actor that could impede the use of the interoperability elements for that purpose—or that could unnecessarily increase the cost or other burden of using the elements for that purpose—would give rise to an obvious risk of interference with access, exchange, or use of EHI under the information blocking provision (84 FR 7546).

We explained that our goal was to balance the need for IP protections with the need to ensure that this proposed exception does not permit actors to abuse their IP or other proprietary rights in inappropriate ways that would block the development, adoption, or use of interoperable technologies and services. The abuse of IP rights in such ways is incompatible with the information blocking provision, which protects the investments that taxpayers and the health care industry have made to adopt technologies that will enable the efficient sharing of EHI to benefit consumers and the health care system. We emphasized that while actors are entitled to protect and exercise their IP rights, to benefit from the exception to the information blocking provision they must do so on terms that do not undermine these efforts and prevent the appropriate flow of EHI. We proposed that these requirements would apply to both price terms (such as royalties and license fees) and other terms, such as conditions or limitations on access to interoperability elements or the purposes for which they can be used (see 84 FR 7546).

Comments. Several health IT developers strongly disagreed with the framework and conditions of this exception. These commenters stated that compulsory licensing of health IT on RAND terms is inconsistent with the usual use of RAND with regards to

standards development. The commenters opined that the proposed exception is a significant overstep that exceeds Congressional intent in the Cures Act and would have a detrimental effect on innovation in the industry. Commenters stated that IP rights would not be adequately protected under the exception, as the exception would allow unprecedented access to IP, and requested that ONC better protect IP rights in the final rule. One commenter recommended that ONC make clear that there are other ways for actors to be in compliance with the information blocking provision besides licensing interoperability elements to all.

Response. We appreciate these comments. Responsive to these comments, we have removed all references to ''RAND.'' However, we have finalized the majority of the substantive conditions for the licensing of interoperability elements under this exception (§ 171.303(b)) as proposed (*i.e.,* the sections on scope of rights, reasonable royalty, non-discriminatory terms, collateral terms, and non-disclosure agreement), with slight modifications discussed below.

In response to comments regarding compulsory licensing, we emphasize that we do not view this exception as constituting compulsory licensing. Each exception is voluntary and actors may choose whether or not they want to seek coverage under an exception. The exceptions operate to the benefit of actors and are intended to provide actors with certainty that certain practices that would normally constitute information blocking will not be considered information blocking, provided the actor's practice meets the conditions of the exception. The fact that a practice to license interoperability elements does not meet the conditions of an exception does *not* mean that the practice would necessarily constitute information blocking. As a result, practices that do not meet the exception will have to be reviewed on a case-by-case basis in order to assess the specific facts and circumstances and to determine, for example, the actor's intent and whether the practice rises to the level of an interference.

In addition, under the Content and Manner Exception (§ 171.301), we establish that an actor is not required to respond to a request to access, exchange, or use EHI in the manner requested if the actor would be required to license IP and cannot reach agreeable terms for the license with the requestor (§ 171.301(b)(1)(ii)). This provision allows actors who do not want to license their IP to respond in an alternative manner that does not require the licensing of proprietary IP. Further, if the actor chooses to respond in the manner requested, and such manner requires the licensing of an interoperability element(s), the actor could license the interoperability elements(s) with whatever terms the actor chooses, so long as the actor is able to reach agreeable terms with the requestor. We refer readers to the discussion in the Content and Manner Exception in VIII.D.2.a, which highlights how the Content and Manner Exception supports an actor's ability to protect their IP.

We understand and appreciate that health IT developers and other entities have invested significant resources to innovate and our policies aim to support these innovations and advancements regarding the access, exchange, and use of EHI. We stress that this exception was drafted with innovation in mind and operates to benefit health IT developers and other actors by allowing them to obtain remuneration for their IP. The Cures Act did *not* create a specific carve out to the information blocking provision for IP rights, but did provide HHS with the authority to establish reasonable and necessary exceptions that do not constitute information blocking. We interpret the definition of information blocking in the Cures Act (section 3022(a) of the PHSA) to encompass *any* fee that materially discourages or otherwise inhibits the access, exchange, or use of EHI, so long as the actor has the requisite intent in the statute. Thus, without clarifying this exception, an actor could implicate the information blocking provision whenever it charged any royalty to license its interoperability elements. We believe this broad interpretation of the information blocking provision would have a detrimental effect of innovation, competition, and consumer welfare. As such, we established this exception to provide assurances to actors that licensing of interoperability elements for access, exchange, or use will not be considered information blocking, *so long as* the actor's practice meets all conditions in the exception. We reiterate that the actor would also need to have the requisite intent, as set forth in the statute. We emphasize that actors are able to make reasonable profits from the licensing of interoperability elements, so long as such profits comply with the ''reasonable royalty'' provision in this exception in § 171.303(b)(2). We also note that the non-disclosure agreement provision in § 171.303(b)(5) establishes additional IP protections.

We emphasize that, in the context of information blocking, control of interoperability elements is often a proxy for control of access, exchange and use of EHI. For example, where EHI is stored in a proprietary format, the EHI cannot be accessed or used if information about the proprietary format does not accompany the EHI. Similarly, when EHI is stored electronically, a technological solution must exist to make the EHI available for use by others. We clarify that health IT developers are *not* required to license *all* of their IP. As discussed earlier in this section, an actor would not need to seek coverage under this exception if the actor's practice is not likely to interfere with the access, exchange, or use of *actual EHI.* Thus, an essential element of the information blocking provision is that there is actual EHI at stake. Further, as discussed above, there would also need to be a nexus between a requestor's need to license an interoperability element and the existing EHI. If there is not such a nexus, the actor would *not* need to seek coverage under this exception (see the Privacy Exception discussion in VIII.D.1.b).

We clarify that, if an actor licenses an interoperability element to one requestor, the actor must license that same interoperability element to future similarly situated requestors with the same terms. Once an actor has granted a license for a particular interoperability element, an actor *cannot* choose to license an interoperability element to one requestor and then refuse or use different terms to license the same interoperability element to a second similarly situated requestor, even if the actor offers to provide the EHI via an alternative manner in accordance with the Content and Manner Exception in § 171.301. In other words, an actor cannot pick and choose who can license a given interoperability element or who gets favorable license terms based on the actor's relationship with the requestor.

Comments. A couple of commenters noted that there is a wide-spectrum of perspectives among stakeholders of common license agreement terms such as limitations on liability and indemnification, which may make reasonableness and non-discriminatory aspects challenging to interpret.

Response. We appreciate these concerns and understand that there is the potential for significant variability in the terms included in license agreements, particularly for licensing interoperability elements. We believe the conditions adopted in this final exception are clear, equitable, and implementable. We emphasize that each information blocking case will turn on its own unique facts and circumstances.

This fact-based approach is appropriate for this exception particularly due to the potential variability in interoperability elements and licensing terms noted by the commenters.

Scope of Rights

To qualify for the proposed exception, we proposed that the actor must license the requested interoperability elements with all rights necessary to access and use the interoperability elements for the following purposes, as applicable:

- All rights necessary to access and use the interoperability elements for the purpose of developing products or services that are interoperable with the actor's health IT or with health IT under the actor's control and/or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control. These rights would include the right to incorporate and use the interoperability elements in the licensee's own technology to the extent necessary to accomplish this purpose.
- All rights necessary to market, offer, and distribute the interoperable products and services described above to potential customers and users, including the right to copy or disclose the interoperability elements as necessary to accomplish this purpose.
- All rights necessary to enable the use of the interoperable products or services in production environments, including using the interoperability elements to access and enable the exchange and use of EHI (84 FR 7546 and 7547).

We requested comment on whether these rights are sufficiently inclusive to support licensees in developing interoperable technologies, bringing them to market, and deploying them for use in production environments. We also requested comment on the breadth of these required rights and if they should be subject to any limitations that would not interfere with the uses we have described above (84 FR 7547).

Comments. We received a couple of comments regarding the scope of rights under this exception. One commenter recommended that ONC specify that actors can require that licensees of the proprietary IP embodied in an interoperability element use that IP only for the licensed purpose, or ONC should allow actors to decline to license that IP at all. One commenter suggested that we broaden the scope of rights regarding the development of products or services that are interoperable so that interoperability does not need to be tied to the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

Response. We thank commenters for these thoughtful comments. We have streamlined the ''scope of rights'' section of this exception for clarity and to align with the overarching goal throughout the information blocking section of enabling the access, exchange, and use of EHI. The finalized ''scope of rights'' section in § 171.303(c)(1) states that the license must provide all rights necessary to: (1) Enable the access, exchange, or use of EHI; and (2) achieve the intended access, exchange, or use of EHI via the interoperability element(s). These rights replaced the rights we proposed in the ''scope of rights'' section (see proposed § 171.206(b)(1)(i)–(iii) and 84 FR 7546 and 7547) because they more clearly and succinctly explain the scope of rights we were trying to convey in the Proposed Rule. The proposed scope of rights included examples that are not necessary in the regulatory text.

Regarding the comment that we should specify that actors can require that licensees of the proprietary IP embodied in an interoperability element use that IP only for the licensed purpose, or ONC should allow actors to decline to license that IP at all, we clarify that actors may require that licensees of the proprietary IP embodied in an interoperability element only use that IP for the licensed purpose, so long as such limits are in compliance with all the conditions in § 171.303, including the scope of rights provisions in § 171.303(c)(1). For instance, an actor could place a limitation in the license that the license only covers a one-time use of the interoperability element for accessing and exchanging certain EHI. In this scenario, this limitation *could* be allowed under the exception if: (1) Despite the limitation, the licensee's request for access, exchange, or use of EHI is met; and (2) the limitation complies with the conditions in § 171.303. Similarly, if an app developer requests to license a health IT developer's interoperability element in order to enable the exchange of EHI by integrating the app developer's CDS software into Provider A's EHR, the health IT developer could scope the rights in the license to restrict the app developer from using the license to complete the same integration for Provider B, so long as the license complies with the conditions in § 171.303. We also emphasize that under the Content and Manner Exception (§ 171.301), actors are decline to license their proprietary IP so long as they are able to respond to the request to access, exchange, or use EHI through an alternative manner specified in § 171.301(b)(2)(ii)(A)–(C).

We have decided not to broaden the scope of rights regarding the development of products or services that are interoperable as suggested by the commenter because we believe this provision, as proposed, is appropriately tailored to addresses information blocking and *should* be focused on health IT under the actor's control or any third party who currently uses the actor's interoperability elements to interoperate with health IT under the actor's control.

Reasonable Royalty

As a condition of this exception, we proposed that if an actor charges a royalty for the use of interoperability elements, the royalty base and rate must be reasonable. Importantly, we proposed that the reasonableness of any royalties would be assessed solely on the basis of the independent value of the actor's technology to the licensee's product, *not* on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using EHI (84 FR 7547).

In evaluating the actor's assertions and evidence that the royalty was reasonable, we proposed that ONC may consider the following factors:

- The royalties received by the actor for the licensing of the proprietary elements in other circumstances comparable to RAND-licensing circumstances.
- The rates paid by the licensee for the use of other comparable proprietary elements.
- The nature and scope of the license.
- The effect of the proprietary elements in promoting sales of other products of the licensee and the licensor, taking into account only the contribution of the elements themselves and not of the enhanced interoperability that they enable.
- The utility and advantages of the actor's interoperability element over the existing technology, if any, that had been used to achieve a similar level of access, exchange, or use of EHI.
- The contribution of the elements to the technical capabilities of the licensee's products, taking into account only the value of the elements themselves and not the enhanced interoperability that they enable.
- The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the proprietary elements or analogous

elements that are also covered by RAND commitments.

- The portion of the realizable profit that should be credited to the proprietary elements as distinguished from non-proprietary elements, the manufacturing process, business risks, significant features or improvements added by the licensee, or the strategic value resulting from the network effects, switching costs, or other effects of the adoption of the actor's technology.
- The opinion testimony of qualified experts.
- The amount that a licensor and a licensee would have agreed upon (at the time the licensee began using the elements) if both were considering the RAND obligation under the exception and its purposes, and had been reasonably and voluntarily trying to reach an agreement (84 FR 7547).

We noted that these factors mirror those used by courts that have examined the reasonableness of royalties charged pursuant to a commitment to a standards developing organization to license standard-essential technologies on RAND terms (*see Microsoft Corp.* v. *Motorola, Inc.;*[187] In re *Innovatio IP Ventures, LLC Patent Litig.;*[188] and *Realtek Semiconductor Corp.* v. *LSI Corp.*[189]). We noted, however, that we adapted the factors to the information blocking context (84 FR 7547).

We proposed that the RAND inquiry should focus on whether the royalty demanded by the actor represents the independent value of the actor's proprietary technology. We proposed that if the actor has licensed the interoperability element through a standards developing organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on RAND terms, the actor may charge a royalty that is consistent with such policies. We proposed that we would ask whether the actor is charging a royalty that is not based on the value of its technology (embodied in the interoperability elements) but rather includes the strategic value stemming from the adoption of that technology by customers or users. We proposed that we would consider the technical contribution of the actor's interoperability elements to the licensee's products—such as any proprietary capabilities or features that the licensee uses in its product—but would screen out any functional aspects of the actor's technology that are used only to establish interoperability and enable EHI to be accessed, exchanged, and used. Additionally, we proposed that to address the potential risk of royalty stacking, we would need to consider the aggregate royalties that would apply if owners of other essential interoperability elements made royalty demands of the implementer. Specifically, we proposed that, to qualify for the exception, the actor must grant licenses on terms that are objectively commercially reasonable taking into account the overall licensing situation, including the cost to the licensee of obtaining other interoperability elements that are important for the viability of the products for which it is seeking to license interoperability elements from the actor (84 FR 7547 and 7548).

We clarified that this condition would not preclude an actor from licensing its interoperability elements pursuant to an existing RAND commitment to a standards developing organization. We also noted that, in addition to complying with the requirements described above, to meet this proposed condition, any royalties charged must meet the condition, proposed separately below, that any license terms be non-discriminatory (84 FR 7548).

We requested comment on these aspects of the proposed exception. We encouraged commenters to consider, in particular, whether the factors and approach we described will be administrable and appropriately balance the unreasonable blocking by actors of the use of essential interoperability elements with the need to provide adequate assurance to investors and innovators that they will be able to earn a reasonable return on their investments in interoperable technologies. Further, we noted that if our proposed approach did not adequately balance these concerns or would not achieve our stated policy goals, we asked that commenters suggest revisions or alternative approaches. We asked that such comments be as detailed as possible and provide rigorous economic justifications for any suggested revisions or alternative approaches (84 FR 7548).

Comments. We received many comments regarding reasonable royalties and the ability of actors to make a profit. Some commenters supported the proposed framework. A couple of commenters recommended that we not allow *any* royalty for licensing interoperability elements. One of those commenters suggested we require ''RAND-Zero'' licensing, by which the copyright holder may still impose non-discriminatory licensing terms on the licensee but may not charge a royalty. The commenter also expressed concern that the overlap between this exception and the exception for recovering costs reasonably incurred creates the potential for actors to earn a double recovery. The commenter explained that licensing of IP is intended to recoup the costs of development of that IP, so where the IP is an interoperability element, the costs reasonably incurred for its development should be incorporated into the royalty rate. The commenter recommended that we be clearer that in these circumstances, only a single recovery is permitted. Provider and registry organizations were concerned that the ability to charge reasonable royalties to license interoperability elements may present an opening for health IT developers to charge unreasonably high fees for exchanging information with provider groups and registries. As such, the commenters recommended that ONC require actors to disclose the methodology behind their fees.

Alternatively, other commenters, consisting primarily of health IT developers, expressed concern that the proposals regarding reasonable royalties were too restrictive. Commenters were concerned that the exception, as proposed, would have a detrimental effect on innovation in the industry as it provides disincentives for established companies to develop new, forward-leaning solutions. A few commenters recommended that the value of the actor's technology must be constructed on a ''fair market'' basis. Commenters stated that ONC should not set or determine the reasonableness of royalties. However, if ONC decided to set or define the reasonableness of royalties, the primary factor for such a determination should be the willingness of licensees to agree to a given royalty rate. A couple of commenters requested clarification regarding ONC's approach for calculating reasonable royalties and ONC's basis for determining whether a royalty is ''reasonable.''

Response. We thank commenters for these thoughtful comments. First, we note, as discussed previously in this section, we have removed all references to ''RAND.'' However, we have finalized this reasonable royalty provision (§ 171.303(c)(2)) as proposed, with a slight modification for consistency and the addition of a paragraph in § 171.303(c)(2)(iv). The slight modification was made to § 171.303(c)(2)(iii), in which we deleted ''on reasonable and non-discriminatory terms'' in order to align with the overall approach of removing ''RAND''

[187] Case No. 10–cv–1823 JLR, 2013 WL 2111217 (W.D.Wash. Apr. 25, 2013).

[188] MDL 2303, 2013 WL 5593609 (N.D.Ill. Oct. 3, 2013).

[189] Case No. 5:12–cv–03451–RMW, 2014 WL 46997 (N.D.Cal. Jan. 6, 2014).

throughout the exception. In response to comment, we added a paragraph in § 171.303(c)(2)(iv) to address the potential for double recovery in this exception and the Fees Exception (§ 171.302). The new paragraph states that an actor may *not* charge a royalty for IP if the actor recovered any development costs pursuant to § 171.302 that led to the creation of the IP.

In response to the commenters who expressed concern that our approach for allowing reasonable royalties is too restrictive and could slow innovation, we emphasize that our regulatory approach to implementing the information blocking provision of the Cures Act is informed by years of research and stakeholder engagement indicating that information blocking undermines public and private sector investments in the nation's health IT infrastructure and frustrates efforts to use modern technologies to improve health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care consumers. In our experience, contractual and IP rights are frequently used to extract rents for access to EHI or to prevent competition from health IT developers of interoperable technologies and services. These practices frustrate access, exchange, and use of EHI and stifle competition and innovation in the health IT sector.

We believe the general claim that the limits on licensing royalties within this exception would inhibit innovation misstates the experiences many stakeholders face today. Our experience in the health IT industry has highlighted that innovation has struggled under current market practices, in which there is no limit on fees and royalties for access and use of interoperability elements. In fact, the ability of large entities with significant market power to prevent access and use of essential interoperability elements has prevented and continues to prevent large amounts of potential investment in innovative solutions for the United States health care market. We also refer readers to the Content and Manner Exception (§ 171.301), where we further address commenter concerns regarding protections for their proprietary IP.

We also appreciate the comments that suggested we not allow *any* royalty for licensing interoperability elements because allowing a royalty could create an opening for actors to continue to charge unreasonably high fees for the exchange of EHI. We have decided to allow reasonable royalties that must meet certain requirements (see § 171.303(b)(2)) because the allowance of such royalties will promote competition, consumer welfare, and investment in innovation. The conditions we have finalized in § 171.303(b)(2) are specifically tailored to address the type of abuse about which commenters expressed concern. Under the finalized reasonable royalty provision, it would generally be appropriate for actors to license their IP on terms that are non-discriminatory and do not interfere with the access, exchange, or use of EHI so long as the actor meets all of the conditions in § 171.303. We emphasize that actors are able to make reasonable profits from the licensing of interoperability elements, so long as such profits comply with § 171.303(b)(2). These licensing practices will further the goals of the information blocking provision by allowing actors to protect the value of their innovations and earn returns on the investments they have made to develop, maintain, and update those innovations. This approach will also protect future incentives to invest in, develop, and disseminate interoperable technologies and services that could improve the lives and safety of patients nationwide.

We acknowledge that limiting the royalties IP holders can charge for access, exchange, or use of EHI departs from IP policy. Absent specific circumstances, IP holders are generally free to negotiate with prospective licensees to determine the royalty to practice their IP, and this negotiated royalty frequently reflects the value the licensee would obtain from exercising those rights. However, in the context of EHI, a limitation on royalties is essential due to the likelihood that unreasonable royalties would frustrate access, exchange, and use of the EHI, particularly because of the imbalanced power dynamics that currently exist in the health IT market.

In response to commenters who requested clarification regarding ONC's approach for calculating reasonable royalties, we emphasize that each case of potential information blocking, as well as the ''reasonableness'' of a royalty, will hinge on the specific facts and circumstances of the case. We explained in the Proposed Rule that the actor would need to show that the royalty base was reasonable and that the royalty was within a reasonable range for the interoperability elements at issue. Importantly, we explained that the reasonableness of any royalties would be assessed solely on the basis of the independent value of the actor's technology to the licensee's product, *not* on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using EHI (84 FR 7547 and 7548). For additional clarification regarding the specific factors to be considered in evaluating an actor's assertion and evidence that a royalty was reasonable, we refer reader to the discussion above and the discussion in the Proposed Rule regarding reasonable royalties (see 84 FR 7547 and 7548).

Non-Discriminatory Terms

We proposed that for the exception to apply, the terms on which an actor licenses and otherwise provides interoperability elements must be non-discriminatory. We explained that this condition would apply to both price and non-price terms, and thus would apply to the royalty terms discussed immediately above as well as other types of terms that may be included in licensing agreements or other agreements related to the provision or use of interoperability elements (84 FR 7548).

We proposed that to comply with this condition, the terms on which the actor licensed the interoperability elements must be based on criteria that the actor applied uniformly for all substantially similar or similarly situated classes of persons and requests. In order to be considered non-discriminatory, such criteria would have to be objective and verifiable, not based on the actor's subjective judgment or discretion. We emphasized that this proposal does not mean that the actor must apply the same terms for all persons or classes of persons requesting a license. However, any differences in terms would have to be based on actual differences in the costs that the actor incurred or other reasonable and non-discriminatory criteria. Moreover, we proposed that any criteria upon which an actor varies its terms or conditions would have to be both competitively neutral—meaning that the criteria are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor—and neutral as to the revenue or other value that the requestor may derive from access, exchange, or use of the EHI obtained via the interoperability elements, including any secondary use of such EHI (84 FR 7548). For a detailed example regarding this proposed condition, see the Proposed Rule (84 FR 7548).

We noted that the foregoing conditions were not intended to limit an actor's flexibility to set different terms based on legitimate differences in the

costs to different classes of persons or in response to different classes of requests, so long as any such classification was in fact based on neutral criteria (in the sense described above) that are objectively verifiable and were applied in a consistent manner for persons and/or requests within each class. For instance, the proposed condition would not preclude an actor from pursuing strategic partnerships, joint ventures, co-marketing agreements, cross-licensing agreements, and other similar types of commercial arrangements under which it provides more favorable terms than for other persons with whom it has a more arms-length relationship. We explained that in these instances, the actor should have no difficulty identifying substantial and verifiable efficiencies that demonstrate that any variations in its terms and conditions were based on objective and neutral criteria (84 FR 7548).

We proposed that a health IT developer of certified health IT who is an ''API Technology Supplier'' under the Condition of Certification proposed in § 170.404 would not be permitted to offer different terms in connection with the APIs required by that Condition of Certification. We proposed that API Technology Suppliers are required to make these APIs available on terms that are no less favorable than provided to their own customers, suppliers, partners, and other persons with whom they have a business relationship (84 FR 7548 and 7549).

We requested comments on the foregoing conditions (84 FR 7549).

Comments. One commenter disagreed with the proposal that the terms must not be based in any part on revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements, including the secondary use of such EHI. The commenter stated that such information should be considered.

Response. We thank the commenter for this feedback, but have decided to finalize this provision as proposed, with slight modification. We continue to believe that license terms for licensing interoperability elements required for the access, exchange, or use of EHI should not be based in any part of the revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements, including the subsequent use of such EHI. The allowance of such terms could enable the type of opportunistic pricing and anti-competitive behavior that this exception seeks to address. We note that we have removed the proposed example about ''secondary use'' from the regulation text because such an example is not necessary in the regulation text (see 84 FR 7604). We emphasize, however, that we continue to maintain that the terms must *not* be based on revenue or other value derived from the subsequent use of EHI. Our policy on this point has not changed from the Proposed Rule. The terms and conditions *could* vary based on neutral, objectively verifiable, and uniformly applied criteria. These might include, for example, significantly greater resources consumed by certain types of apps, such as those that export large volumes of data on a continuous basis, or the heightened risks associated with apps designed to ''write'' data to the EHR database or to run natively within the EHR's user interface.

We emphasize that health IT developers that license interoperability elements in order for EHI to be accessed, exchanged, or used could *not* vary the license terms and conditions based on subjective criteria, such as whether it thinks an app will be ''popular'' or is a ''good fit'' for its ecosystem. Nor could developers offer different terms or conditions on the basis of objective criteria that are not competitively neutral, such as whether an app ''connects to'' other technologies or services, provides capabilities that the EHR developer plans to incorporate in a future release of its technology, or enables an efficient means for customers to export data for use in other databases or technologies that compete directly with the EHR developer. Similarly, the EHR developer could not set different terms or conditions based on how much revenue or other value the app might generate from the information it collects through the APIs, such as by introducing a revenue-sharing requirement for apps that use data for secondary purposes that are very lucrative and for which the EHR developer would like a ''piece of the pie.'' Such practices would disqualify the actor from this exception and would implicate the information blocking provision.

We note that we made a slight modification to § 171.303(c)(3)(i) in that we removed ''substantially similar.'' We believe ''similarly situated,'' without ''substantially similar'' is clearer, maintains the intended effect, and is consistent with language used in other exceptions.

Collateral Terms

We proposed five additional conditions that would reinforce the requirements of the proposed exception. We explained that these additional conditions would provide bright-line prohibitions for certain types of collateral terms or agreements that we believe are inherently likely to interfere with access, exchange, or use of EHI. We proposed that any attempt to *require* a licensee or its agents or contractors to do or agree to do any of the following would disqualify the actor from the exception and would be suspect under the information blocking provision (84 FR 7549).

First, we proposed that the actor must not require the licensee or its agents or contractors to not compete with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development. We explained that we are aware that such agreements have been used to either directly exclude suppliers of interoperable technologies and services from the market or to create exclusivity that reduces the range of technologies and options available to health care providers and other health IT customers and users (84 FR 7549).

Second, we proposed that the actor must not require the licensee or its agents or contractors to deal exclusively with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development (84 FR 7549).

Third, we proposed that the actor must not require the licensee or its agents or contractors to obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements. We explained that without this condition, we believe that an actor could require a licensee to take a license to additional interoperability elements that the licensee does not need or want, which could enable the actor to extract royalties that are inconsistent with its RAND obligations under this exception. We clarified that this condition would not preclude an actor and a willing licensee from agreeing to such an arrangement, so long as the arrangement was not *required* (84 FR 7549).

Fourth, we proposed that the actor must not condition the use of interoperability elements on a requirement or agreement to license, grant, assign, or transfer the licensee's own IP to the actor. We explained that it would raise information blocking concerns for an actor to use its control over interoperability elements as leverage to obtain a ''grant back'' of IP rights or other consideration whose value may exceed that of a reasonable royalty. We proposed that, consistent with our approach under other conditions of this exception, this condition would not preclude an actor

and a willing licensee from agreeing to a cross-licensing, co-marketing, or other agreement if they so choose. However, the actor could not *require* the licensee to enter into such an agreement. We proposed that the actor must offer the option of licensing the interoperability elements without a promise to provide consideration beyond a reasonable royalty (84 FR 7549).

Finally, we proposed that the actor must not condition the use of interoperability elements on a requirement or agreement to pay a fee of any kind whatsoever unless the fee meets either the narrowly crafted condition to this exception for a reasonable royalty, or, alternatively, the fee satisfies the separate exception in § 171.302, which permits the recovery of certain costs reasonably incurred (84 FR 7549).

We requested comment on these categorical exclusions. In particular, we encouraged commenters to weigh in on our assumption that these practices are inherently likely to interfere with access, exchange, or use of EHI. We also encouraged commenters to suggest any conceivable benefits that these practices might offer for interoperability or for competition and consumers that we might have overlooked. Again, we asked that to the extent possible commenters provide detailed economic rationale in support of their comments (84 FR 7549).

Comments. One commenter noted that situations exist where licensors do not have the ability to lawfully confer rights or licenses to information or products without the agreement of a third party. The commenter recommended that we add ''except as required by law'' to the collateral terms provisions in order to clarify that the expectation is not that an actor must obtain such rights on behalf of the requestor.

Response. We appreciate this comment, but have decided not to make the suggested edit because we do not believe such an addition is necessary. The collateral terms provisions do not address whether an actor is expected to obtain rights from a third party to lawfully confer rights or licenses to interoperability elements. Instead, the collateral terms provisions describe conditions that the actors must *not* require of the licensee or its agents or contractors to do because such conditions are inherently likely to interfere with access, exchange, or use of EHI. We note that we have revised the definition of ''interoperability element'' (see § 171.102) to clarify that in order to meet the definition, the element must be ''controlled by the actor,'' which addresses the commenter's concern. We have also defined ''controlled by the actor'' in § 171.102 in the context of the interoperability element definition for clarity. If the actor could not lawfully confer a right or authorization, the actor would not have the requisite ''control'' under the ''interoperability element.'' Last, we emphasize that in situations when an actor does not have the ability to lawfully confer rights or licenses to enable the access, exchange, or use of EHI, the actor could seek coverage under the Infeasibility Exception (see § 171.204(a)(3)) or the Content and Manner Exception (see § 171.301(b)).

Comments. We did not receive any other comments regarding the proposed collateral terms proposals except those noted in the comment summary above.

Response. We have finalized the collateral terms as proposed.

Non-Disclosure Agreement

We proposed that an actor would be permitted under this exception to require a licensee to agree to a confidentiality or non-disclosure agreement (NDA) to protect the actor's trade secrets, provided that the NDA is no broader than necessary to prevent the unauthorized disclosure of the actor's trade secrets. Further, we proposed that the actor would have to identify (in the NDA) the specific information that it claims as trade secrets, and that such information would have to meet the definition of a trade secret under applicable law. We noted that if the actor is a health IT developer of certified health IT, it may be subject to the Condition of Certification that prohibits certain health IT developer prohibitions and restrictions on communications about a health IT developer's technology and business practices. We emphasized that the exception would not in any way abrogate the developer's obligations to comply with that condition. We encouraged comment on this condition of the proposed exception (84 FR 7549).

Comments. We received a couple of comments regarding the proposed NDA provision. One commenter recommended that we state in the final rule that interoperability elements themselves may not be protected as trade secrets. Another commenter expressed concern that this exception acts to require NDAs in certain circumstances. The commenter also suggested edits to preamble language that would allow the actor to ''generally'' identify the information that it claims as trade secrets, as opposed to the proposed language of identifying the ''specific'' information that it claims as trade secrets.

Response. We thank commenters for these thoughtful comments. We clarify that interoperability elements may be protected as trade secrets. Trade secrets are a type of IP that consist of information and can include a formula, pattern, compilation, program, device, method, technique or process,[190] and could fall within the definition of ''interoperability element'' (see § 171.102). We note, as discussed in more detail in VIII.C.5.b, that we have leveraged the definition of ''health information technology'' from section 3000(5) of the PHSA for the definition of ''interoperability element'' in § 171.102, and that IP is included in that definition of ''health information technology.'' The PHSA defines ''health information technology'' as ''hardware, software, integrated technologies or related licenses, *intellectual property,* upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.''

In response to the commenter that expressed concern that this exception acts to require NDAs in certain circumstances, we emphasize that we are *not* requiring NDAs. We included this provision in order to help actors protect their IP and actors may draft the NDA in a manner that best suits their needs so long as the NDA meets the requisite conditions in § 171.303(b)(5). We have decided not to allow actors to ''generally'' identify the information that they claim as trade secrets because such a change could enable actors to make broad assertions of trade secret protection that exceed the *actual* trade secrets. The safeguards we have finalized in the NDA provision (*e.g.,* that the agreement is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets and the agreement states with particularity all information the actor claims as trade secrets) are necessary to ensure that the NDA is not used to impose restrictions or burdensome requirements that are not actually necessary to protect the actor's trade secrets and that impede the use of the interoperability elements. We emphasize that the use of an NDA for such purposes would preclude an actor from qualifying for this exception and would implicate the information blocking provision.

[190] USPTO, Trade Secret Policy, *https://www.uspto.gov/patents-getting-started/international-protection/trade-secrets-policy.*

iii. Additional Requirements Relating to the Provision of Interoperability Elements

We proposed that an actor's practice would need to comply with additional conditions that ensure that actors who license interoperability elements on RAND terms do not engage in separate practices that impede the use of those elements or otherwise undermine the intent of this exception. We explained that these conditions are analogous to the conditions described in our proposal concerning collateral terms but address a broader range of practices that may not be effected through the license agreements themselves or that occur separately from the licensing negotiations and other dealings between the actor and the licensee. Specifically, we proposed that an actor would not qualify for this exception if it engaged in a practice that had the purpose or effect of impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose; or the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand. We explained that the exception would not apply if the developer licensed its proprietary APIs for use by third-party apps but then prevented or delayed the use of those apps in production environments by, for example, restricting or discouraging customers from enabling the use of the apps, or engaging in ''gate keeping'' practices, such as requiring apps to go through a vetting process and then applying that process in a discriminatory or unreasonable manner. Finally, to ensure the actor's commitments under this exception are durable, we proposed one additional safeguard: An actor could not avail itself of this exception if, having licensed the interoperability elements, the actor makes changes to the elements or its technology that ''break'' compatibility or otherwise degrade the performance or interoperability of the licensee's products or services (84 FR 7549 and 7550).

We emphasized that this proposed condition would in *no way* prevent an actor from making improvements to its technology or responding to the needs of its own customers or users. However, to benefit from the exception, the actor's practice would need to be necessary to accomplish these purposes and the actor must have afforded the licensee a reasonable opportunity under the circumstances to update its technology to maintain interoperability (84 FR 7550).

Comments. One commenter stated that the proposed restriction regarding breaking compatibility or otherwise degrading the performance or interoperability of the licensee's products or services is too broad. The commenter suggested that ONC add procedural safeguards to avoid misuse and unpredictable enforcement. Specifically, the commenter recommended that ONC: (1) Institute a grace period for licensors to provide fixes where interoperability elements are inadvertently unavailable due to software changes; (2) permit health IT developers to maintain their existing processes to notify customers about upgraded standards on a reasonable timeframe; (3) allow, with a year's notice, retirement of functionality in future versions of the software; (4) acknowledge that the use of interoperability elements will always require some initial work and ongoing upkeep by the licensee, such as testing and continuous work to deploy technology at health systems with different workflows; and (5) the ONC-administered advisory opinion process should account for review of RAND licensing terms to provide clarity to the regulated actors.

Response. We agree with the commenter that it is critical that the final exceptions are transparent and cannot be misused. Each exception should clearly explain what conduct would be covered by the exception and what conduct falls outside the scope of the exception. In response to the commenter, we note that we have not prevented health IT developers from maintaining their existing processes to notify customers about upgraded standards on a reasonable timeframe, nor have we instituted any new policies regarding the retirement of functionality in future versions of software. Further, we acknowledge that the use of interoperability elements may require some initial work and ongoing upkeep by the licensee, such as testing and continuous work to deploy technology in health systems with different workflows. However, we emphasize that such initial work, ongoing upkeep, or any additional burden on licensees must meet all the conditions of this exception as all relevant times.

We have decided not to institute a grace period for licensors to provide fixes where interoperability elements are inadvertently unavailable due to software changes because we do not believe such a grace period is necessary. Having consulted with OIG, we note that OIG generally does not pursue civil monetary penalties for actors who make innocent mistakes or for accidental conduct. Future notice and comment rulemaking by OIG will provide more additional detail regarding information blocking enforcement.

We may consider developing materials in the future regarding the application of the exceptions should the need arise. However, we believe the final rule clearly describes the conditions actors must meet in order to be covered by each exception, and informational materials are not necessary at this time.

iv. Compliance With Conditions of Certification

As a final condition of the proposed exception, we proposed that health IT developers of certified health IT who are subject to the Conditions of Certification proposed in §§ 170.402, 170.403, and 170.404 must comply with all requirements of those Conditions of Certification for all practices and at all relevant times (84 FR 7550).

Comments. We did not receive any comments on this proposed condition.

Response. We have removed this proposed condition from the final rule for consistency with other exceptions and for clarity, as the condition is not necessary.

E. Additional Exceptions—Request for Information

1. Exception for Complying With Common Agreement for Trusted Exchange

In the Proposed Rule, we included a request for information (RFI) regarding whether we should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement (84 FR 7552). The most recent draft Trusted Exchange Framework and Common Agreement was released for public comment on April 19, 2019.[191]

Comments. We received over 40 comment submissions on this RFI expressing various viewpoints on the purpose, need, and structure of a TEFCA exception.

Response. We thank commenters for their feedback. As noted in the Proposed Rule, we may use this feedback to inform a future rulemaking.

2. New Exceptions

In the Proposed Rule, we included an RFI regarding any potential new exceptions we should consider for future rulemaking (84 FR 7552).

[191] ONC, *Draft 2 Trusted Exchange Framework and Common Agreement, https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf.*

Comments. We received a number of requests for a new exception to cover sensitive and/or privileged information. A health IT developer suggested a new exception to allow actors to withhold sensitive information. The commenter expressed concern that EHI at a certain data class or data element level will require health care providers to exert substantial manual effort to mediate disclosure. Health care providers and provider organizations suggested an exception that would exempt actors from the information blocking provision if they are protecting privileged information. One commenter expressed concern about providing access, exchange, or use of quality program and reporting data. A hospital suggested that requiring providers to waive privilege in order to avoid information blocking would have a detrimental effect on peer reviews and safety assessments that help providers resolve adverse events.

Response. We thank commenters for these suggestions. We first note that the health information must fall within the EHI definition, which aligns with the ePHI definition contained in the HIPAA Rules. We note that actors faced with a request to access, exchange, We note that actors faced with a request to access, exchange, or use sensitive and/or privileged information can seek coverage under the exceptions for preventing harm (§ 171.201), promoting the privacy of EHI (§ 171.202), promoting the security of EHI (§ 171.203), or infeasibility (§ 171.204), depending on the specific information at issue and the circumstances of the case. We refer readers to those exceptions, as well as the preamble discussions at sections VIII.D.1 (Preventing Harm Exception), VIII.D.2 (Privacy Exception), VIII.D.3 (Security Exception), and VIII.D.4 (Infeasibility Exception). We also note that an actor would not be required to share EHI if the interference with access, exchange, or use of the EHI is explicitly required by State or Federal law (see the discussion regarding ''required by law'' at section VIII.C.1 of this preamble). We emphasize that this final rule does *not* require actors to waive privilege provided by law.

*Comment*s. Some commenters expressed concern about the effect of the information blocking provision on research. Public health organizations proposed an exception to exclude research (as defined by 45 CFR 164.501) and non-direct clinical care conducted by public health authorities, from implicating the information blocking provision. A hospital requested that we establish a new sub-exception under the exception for preventing harm that would allow health care providers who conduct research at their institutions to require that other providers who request EHI are also collaborators in that research. One commenter suggested an exception for health care providers who cannot send data to a public health registry when the public health agency is not ready to onboard the provider due factors outside of the provider's control (*e.g.,* lack of resources or a backup in the onboarding queue).

Response. We thank commenters for these suggestions. We note that actors faced with a request to access, exchange, or use EHI related to research can seek coverage under the exceptions for promoting the privacy of EHI (§ 171.202) or infeasibility (§ 171.204), depending on the specific research being conducted and EHI at issue. We refer readers to those exceptions, as well as the preamble discussions at sections VIII.D.2 (Privacy Exception) and VIII.D.4 (Infeasibility Exception). We also note that an actor would not be required to share EHI if the interference with access, exchange, or use of the EHI is explicitly required by State or Federal law (see the discussion regarding ''required by law'' at section VIII.C.1 of this preamble).

Comments. Some commenters requested a new exception to protect actors who seek independent opinions from external validators regarding their business practices, in case one of those practices falls within the definition of information blocking.

Response. We appreciate this suggestion. With regard to private ''external validators,'' we note that we are not restricting an actor's ability to hire private companies to assess its business practices.

Comments. A commenter recommended an exception for standard business practices. The commenter explained that examples of such conduct include suspending the access of any health IT developer or e-prescribing application that is not compliant with State laws or uses the provider's technology platform for reasons that compromises the integrity of the provider's network (*e.g.,* using the network for commercial messaging).

Response. We appreciate this suggestion. While we would need more facts to properly assess these scenarios, we believe that such situations could likely be covered by either the exception for promoting the privacy of EHI (§ 171.202) or the exception for promoting the security of EHI (§ 171.203). We refer readers to those exceptions, as well as the preamble discussions at sections VIII.D.2 (Privacy Exception) and VIII.D.3 (Security Exception). We also note that the actor would not be required to share EHI if the interference with access, exchange, or use of the EHI is explicitly required by State or Federal law (see the discussion regarding ''required by law'' at section VIII.C.1 of this preamble).

F. Complaint Process

We explained in the Proposed Rule that section 3022(d)(3)(A) of the PHSA directs the National Coordinator to implement a standardized process for the public to submit reports on claims of information blocking (84 FR 7552). Section 3022(d)(3)(B) further requires that the complaint process provide for the collection of such information as the originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information.

In the Proposed Rule, we stated that we intend to implement and evolve the complaint process by building on existing mechanisms, including the process for providing feedback and expressing concerns about health IT that is currently available at *https://www.healthit.gov/healthit-feedback* (84 FR 7553). We requested comment on this approach and any alternative approaches that would best effectuate this aspect of the Cures Act. In addition to any other comments that the public may have wished to submit, we specifically requested comment on several specific questions. The scope of these questions was specific to the information blocking complaint submission process and the information collection necessary to enable effective investigations and safeguard the confidentiality of information submitted through the complaint process.

Comments. We received over 25 comment submissions that included suggestions for the information blocking complaint process. A few commenters responded to one or more of the specific questions in the Proposed Rule, offering suggestions for specific data elements that complainants should be able to enter as part of a complaint. Some commenters suggested specific features such as: A dedicated secure online portal for entry of information blocking complaints and any supporting documents; a dedicated email box or toll-free phone number for submission of information blocking complaints; the ability to batch multiple instances of potential information blocking activity by the same actor into one complaint submission; and a user interface of pick-lists to help submitters more easily categorize their concerns and/or mark specific portions of or attachments to

their complaints according to their level of sensitivity or requested confidentiality. Numerous commenters expressed support for the existence of a publicly available, user-friendly complaint process and recommended that the development and publication of the complaint process include robust educational and informational materials. A few commenters requested an opportunity for public comment on the complaint process's operational details prior to it going live.

Response. We note that the complaint process is not required by statute to be established through rulemaking and we did not intend to give an impression that it would by including the request for information about the complaint process in the Proposed Rule. Rather, as was the intended outcome, we have received thoughtful suggestions that have informed our initial rollout of the information blocking complaint process as well as have provided considerations for further evolution of the process.

We have identified several themes and specific suggestions in the comments that we will address below for the purposes of transparency and to inform stakeholders. We have developed a dedicated complaint process that is based upon and informed by our experience with our current health IT feedback process and the comments received on the Proposed Rule. We also plan to publish informational materials to accompany the rollout of this dedicated information blocking complaint process so that potential complainants across the affected stakeholder categories can successfully use it to submit complaints where they believe they have experienced or observed conduct that constitutes information blocking. While we do not anticipate publishing potential operational details of the complaint process and submission mechanism in advance of its rollout, we would like to amplify a point we noted in the Proposed Rule, which is that we intend to implement *and evolve* the complaint process. After we launch the information blocking complaint process, we anticipate using our own experience and users' feedback about the information blocking complaint process to identify opportunities to further evolve and enhance all aspects of the information blocking complaint process, including but not limited to its associated informational materials.

Comments. Several commenters requested that all information blocking complaints be publicly posted and available. Conversely, many commenters were in strong support of ONC ensuring adequate confidentiality for those who submit information blocking complaints.

Response. Section 3022(d)(2) of the PHSA exempts from public disclosure ''any information that is received by the National Coordinator in connection with a claim or suggestion of possible information blocking and that could reasonably be expected to facilitate identification of the source of the information'' except as may be necessary to carry out the purpose of PHSA section 3022. We believe the publishing of complaints could lead to the identification of the source of the information or reasonably facilitate identification of the source; therefore, we do not intend to make complaints publicly available. In specific reference to health IT developers of certified health IT, however, we note that we publish in the Certified Health IT Product List (CHPL) information about non-conformities with Program requirements, which would include any non-conformities with the Information Blocking Condition of Certification requirement. We also note that the information blocking complaint process offers the option for users to submit anonymously, explaining in multiple places types of submission information to exclude for those who would like to maintain confidentiality.

Comments. Several commenters requested that complainants be required to submit sufficient evidence of *intentional* information blocking in the complaint submission process. Another commenter suggested complainants be required to meet particular qualifications in order to submit a formal complaint.

Response. We thank commenters for their input. However, we do not believe requiring a complaint submission to include more than the minimum information necessary to understand the complainant's concern would best serve the purpose of the complaint process. We believe that requiring that a complainant meet a proof, evidentiary, or qualification standard as a pre-requisite to them submitting a complaint would inappropriately discourage or prevent many individuals and organizations who are subjected to conduct that may meet the definition of information blocking from sharing their concerns with us.

G. Disincentives for Health Care Providers—Request for Information

Section 3022(b)(2)(B) of the PHSA provides that any health care provider determined by OIG to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking. We requested comment on potential disincentives and whether modifying disincentives already available under existing Department programs and regulations would provide for more effective deterrents (84 FR 7553).

We also sought information on the implementation of section 3022(d)(4) of the PHSA, which provides that in carrying out section 3022(d) of the PHSA, the Secretary shall, to the extent possible, not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved as of the day before December 13, 2016—enactment of the Cures Act.

Comments. We received over 40 submissions on this RFI. We have organized and summarized the comments by topic below.

Need for Disincentives

Views on the need for additional disincentives generally diverged based on stakeholder type. Health care providers were generally opposed to additional disincentives. Provider organizations were opposed to any new disincentives. Nearly all these organizations stated that any additional disincentives would be duplicative of disincentives for information blocking put in place through the QPP and Promoting Interoperability Programs. In particular, hospitals noted concerns that they are already subject to a 75 percent negative adjustment to their market basket increase if they are unable to make the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA)-mandated attestation that they have not engaged in information blocking. However, a few provider organizations noted that any new disincentives would only be duplicative for providers that are eligible for these specific CMS-administered programs, recognizing that the existing disincentives under Medicare would not reach providers that do not participate in QPP or PI Programs.

Multiple provider organizations stated that additional disincentives would be duplicative of fines for HIPAA Rules violations and mentioned that the Office for Civil Rights (OCR) has expressed an intent to increase HIPAA Rules enforcement on providers.

A patient-facing app developer commented that the HIPAA Rule's disincentives, attestation, and public reporting are not enough to discourage information blocking.

Several health IT developers were neutral on the topic, stating that it was

unclear if additional disincentives would duplicate disincentives in other programs.

One payer, one patient advocacy organization, and one HIN were supportive of additional provider disincentives.

The HITAC recommended that ONC work with CMS to build information blocking disincentives into a broad range of CMS programs, and that ONC work with other Federal departments and agencies that contract with providers (*e.g.,* Veterans Health Administration, Department of Defense Military Health System, Indian Health Service, Centers for Disease Control and Prevention) to similarly build information blocking disincentives into contracting and other programs. The HITAC also recommended that providers be required to attest to compliance with requirements to avoid information blocking as part of Conditions of Participation, Conditions for Coverage, contracts, and other similar relationships, covering fee-for-service (FFS), value-based care, and direct payment relationships. The HITAC noted that such an attestation requirement could potentially allow for pursuit of serious penalties should OIG find the provider engaged in information blocking.

Magnitude of Penalties

While health care providers were generally opposed to disincentives, some did offer recommendations for keeping penalties to a minimum. About half of the provider organizations commenting stated that any fines for providers should not be at the same level as those levied against health IT developers, HINs, and HIEs. Other provider organizations had more specific recommendations, including a tiered approach to penalties. One provider organization recommended a two-tiered approach, with more significant financial penalties for large hospitals and health systems and public reporting or QPP score reductions for physicians. Another provider organization recommended a tiered approach that mimics the approach used under HIPAA (as modified by HITECH), in which penalties increase based on the nature and extent of the violation and resulting harm. Another provider organization recommended that organizations found to engage in information blocking be disqualified from the PI category in QPP.

Some health IT developers recommended significant penalties for providers. Several health IT developers recommended that ONC work with CMS to utilize and enhance existing disincentive mechanisms, with one developer specifically recommending utilization of the Conditions of Participation, Conditions for Coverage, and Requirements for Participation. One app developer recommended that fines for information blocking be substantial and per record blocked. The HITAC stated that fines should be significant enough to discourage problematic behavior, encourage compliance, and incent providers to address and remediate problematic behavior. A payer commented that fines should be consistent with those levied against developers, HINs, and HIEs.

Enforcement

Most health care providers and provider organizations recommended that providers be given the opportunity to become compliant before being subject to any fines, except in instances of clear, egregious violations. Some provider organizations recommended that there be an appeals process for disincentives or findings that health care providers had violated the information blocking provision, with one organization noting that an appeals process is especially needed for small and rural practices.

Response. We have shared all the comments received with the appropriate agencies and offices within the Department for consideration in subsequent rulemaking to implement section 3022(b)(2)(B) and (d) of the PHSA.

IX. Registries Request for Information

In the Proposed Rule, we included a Request for Information (RFI) on how health IT solutions and the proposals in the Proposed Rule could aid bidirectional exchange with registries for a wide range of public health, quality reporting, and clinical quality improvement initiatives (84 FR 7553). We received 75 comments in response to this RFI. We thank commenters for their input and we may consider including this information in a future rulemaking.

X. Patient Matching Request for Information

Patient matching is a critical component to interoperability and the nation's health IT infrastructure. In the Proposed Rule, we included a Request for Information (RFI) on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching (84 FR 7554). We received 128 comments in response to this RFI. We appreciate the input provided by commenters and may use this information to inform future rulemaking.

XI. Incorporation by Reference

The Office of the Federal Register has established requirements for materials (*e.g.,* standards and implementation specifications) that agencies incorporate by reference in the Code of Federal Regulations (79 FR 66267; 1 CFR 51.5). Specifically, § 51.5(b) requires agencies to discuss, in the preamble of a final rule, the ways that the materials they incorporate by reference are reasonably available to interested parties and how interested parties can obtain the materials, and to summarize, in the preamble of the final rule, the material they incorporate by reference.

To make the materials we intend to incorporate by reference reasonably available, we provide a uniform resource locator (URL) for the standards and implementation specifications. In many cases, these standards and implementation specifications are directly accessible through the URLs provided. In instances where they are not directly available, we note the steps and requirements necessary to gain access to the standard or implementation specification. In most of these instances, access to the standard or implementation specification can be gained through no-cost (non-monetary) participation, subscription, or membership with the adopted standards developing organization (SDO) or custodial organization. In certain instances, where noted, access requires a fee or paid membership. As an alternative, a copy of the standards may be viewed for free at the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, 330 C Street SW, Washington, DC 20201. Please call (202) 690–7171 in advance to arrange inspection.

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. As discussed in section IV of this preamble, we have followed the

NTTAA and OMB Circular A–119 in adopting standards and implementation specifications for adoption, including describing any exceptions in the adoption of standards and implementation specifications. Over the years of adopting standards and implementation specifications for certification, we have worked with SDOs, such as HL7, to make the standards we adopt and incorporate by reference in the **Federal Register** available to interested stakeholders. As described above, this includes making the standards and implementation specifications available through no-cost memberships and no-cost subscriptions.

As required by 1 CFR 51.5(b), we provide summaries of the standards we have adopted and incorporate by reference in the Code of Federal Regulations (CFR). We also provide relevant information about these standards and implementation specifications throughout the preamble.

We have organized the standards and implementation specifications that we have adopted through this rulemaking according to the sections of the Code of Federal Regulation (CFR) in which they will be codified and cross-referenced for associated certification criteria and requirements that we have adopted.

Content Exchange Standards and Implementation Specifications for Exchanging Electronic Health Information—45 CFR 170.205

• CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting Implementation Guide for 2019, May 4, 2018

URL: https://ecqi.healthit.gov/system/files/QRDA_HQR_2019_CMS_IG_final_508.pdf.

This is a direct access link.

Summary: This guide is a CMS Quality Reporting Document Architecture Category I (QRDA I) implementation guide to the *HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture Category I, Release 1, STU Release 5 (published December 2017),* and referred to as the HL7 QRDA IG STU R5 in this guide. This guide describes additional conformance statements and constraints for electronic health record (EHR) data submissions that are required for reporting information to the Centers for Medicare & Medicaid Services (CMS) for the Hospital Inpatient Quality Reporting Program 2019 Reporting Period. The purpose of this guide is to serve as a companion to the base HL7 QRDA I STU R5 for entities such as Eligible Hospitals (EH), Critical Access Hospitals (CAH), and developers to submit QRDA I data for consumption by CMS systems including for Hospital Quality Reporting (HQR).

• CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2019, October 8, 2018

URL: https://ecqi.healthit.gov/system/files/2019_CMS_QRDA_III_Eligible_Clinicians_and_EP_IG-508.pdf.

This is a direct access link.

Summary: The Health Level Seven International (HL7) Quality Reporting Document Architecture (QRDA) defines constraints on the HL7 Clinical Document Architecture Release 2 (CDA R2). QRDA is a standard document format for the exchange of electronic clinical quality measure (eCQM) data. QRDA reports contain data extracted from EHRs and other information technology systems. The reports are used for the exchange of eCQM data between systems for quality measurement and reporting programs. This QRDA guide contains the CMS supplemental implementation guide to the *HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture, Category III, STU Release 2.1 (June, 2017)* for the 2019 performance period. This HL7 base standard is referred to as the HL7 QRDA–III STU R2.1.

• Health Level 7 (HL7®) CDA R2 Implementation Guide: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2–US Realm, October 2019

URL: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=447.

Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Companion Guide to Consolidated Clinical Document Architecture (C–CDA) R2, provides essential implementer guidance to continuously expand interoperability for clinical information shared via structured clinical notes. The guidance supplements specifications established in the Health Level Seven (HL7) CDA® R2.1 IG: C–CDA Templates for Clinical Notes. This additional guidance is intended to make implementers aware of emerging expectations and best practices for C–CDA document exchange. The objective is to increase consistency and expand interoperability across the community of data sharing partners who utilize C–CDA for information exchange.

• National Council for Prescription Drug Programs (NCPDP), SCRIPT Standard Implementation Guide, Version 2017071 (Approval Date for ANSI: July 28, 2017)

URL: http://www.ncpdp.org/Standards/Standards-Info.

Access requires registration, a membership fee, a user account, and a license agreement to obtain a copy of the standard.

Summary: NCPDP SCRIPT standards are developed for transmitting prescription information electronically between prescribers, pharmacies, payers, and other entities for new prescriptions, changes of prescriptions, prescription refill requests, prescription fill status notifications, cancellation notifications, relaying of medication history, transactions for long-term care, electronic prior authorization and other transactions. New transactions in this update include Prescription drug administration message, New prescription requests, New prescription response denials, Prescription transfer message, Prescription fill indicator change, Prescription recertification, Risk Evaluation and Mitigation Strategy (REMS) initiation request, REMS initiation response, REMS request, and REMS response.

Standards for Health Information Technology To Protect Electronic Health Information Created, Maintained, and Exchanged—45 CFR 170.210

• ASTM E2147–18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1, 2018

URL: https://www.astm.org/Standards/E2147.htm.

This is a direct access link. However, a fee is required to obtain a copy of the standard.

Summary: This specification describes the security requirements involved in the development and implementation of audit and disclosure logs used in health information systems. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems, and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of confidential health care information to external users for use in manual and computer systems. This specification has two main purposes, namely: To define the nature, role, and function of system access audit logs and

their use in health information systems as a technical and procedural tool to help provide security oversight; and to identify principles for establishing a permanent record of disclosure of health information to external users and the data to be recorded in maintaining such record of disclosure.

United States Core Data for Interoperability—45 CFR 170.213

• United States Core Data for Interoperability (USCDI), February 2020, Version 1 (v1)

URL: https://www.healthit.gov/USCDI.

This is a direct access link.

Summary: The United States Core Data for Interoperability (USCDI) establishes a minimum set of data classes that are required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time. Data classes listed in the USCDI are represented in a technically agnostic manner.

Application Programming Interface Standards—45 CFR 170.215

• HL7 FHIR® US Core Implementation Guide STU 3.1.0, November 6, 2019

URL: http://hl7.org/fhir/us/core/STU3.1/.

This is a direct access link.

Summary: The US Core Implementation Guide STU 3.1.0 is based on FHIR Version R4 and defines the minimum conformance requirements for accessing patient data. The Argonaut pilot implementations, ONC 2015 Edition Common Clinical Data Set (CCDS), and the latest ONC United States Core Data for Interoperability (USCDI) provided the requirements for this guide. The prior Argonaut search and vocabulary requirements, based on FHIR DSTU2, are updated in this guide to support FHIR Version R4.

• Health Level 7 (HL7) Version 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR) Release 4, October 30, 2019

URL: http://hl7.org/fhir/R4/.

This is a direct access link.

Summary: The HL7 Version 4.0.1 Fast Healthcare Interoperability Resources (FHIR) Release 4, which also includes technical corrections to R4, provides the first set of normative FHIR resources. This normative designation means that the future changes will be backward compatible for the first time. These resources define the content and structure of core health data which can be used by developers to build standardized applications. Release 4 provides new standard operation on how to obtain data from multiple patients via FHIR. API services that focus on multiple patients would enable health care providers to manage various internal patient populations as well as external services a health care provider may contract for to support quality improvement, population health management, and cost accountability vis-à-vis the provider's partners (*e.g.,* health plans).

• HL7 FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1), August 22, 2019

URL: http://hl7.org/fhir/uv/bulkdata/.

This is a direct access link.

Summary: This implementation specification defines a standardized, HL7 FHIR-based approach for exporting health information for multiple patients from a server compliant with the HL7 FHIR standard. This implementation specification is intended to be used by apps to request information on multiple patients. The implementation specification includes OperationDefinitions, which define how the multiple patient export operations are invoked by clients, and the SMART Backend Services: Authorization Guide, which describes how a client can register with and obtain an access token from a server compliant with the implementation specification.

• HL7 FHIR SMART Application Launch Framework Implementation Guide Release 1.0.0, November 13, 2018

URL: http://hl7.org/fhir/smart-app-launch/.

This is a direct access link.

Summary: SMART on FHIR provides reliable, secure authorization for a variety of app architectures through the use of the OAuth 2.0 standard. This Authorization Guide supports the four use cases defined for Phase 1 of the Argonaut Project. This profile is intended to be used by developers of apps that need to access FHIR resources by requesting access tokens from OAuth 2.0 compliant authorization servers. The profile defines a method through which an app requests authorization to access a FHIR resource, and then uses that authorization to retrieve the resource. Other security mechanisms required by the HIPAA Security Rule, such as end-user authentication, session time-out, security auditing, and accounting of disclosures, are outside the scope of this profile.

• OpenID Connect Core 1.0 Incorporating Errata Set 1, November 8, 2014

URL: http://openid.net/specs/openid-connect-core-1_0.html.

This is a direct access link.

Summary: OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables clients to verify the identity of the end user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user in an interoperable and REST-like manner. This specification defines the core OpenID Connect functionality: Authentication built on top of OAuth 2.0 and the use of claims to communicate information about the end user. It also describes the security and privacy considerations for using OpenID Connect.

Incorporation by Reference—45 CFR 170.599

• ISO/IEC 17025:2017(E)—General Requirements for the Competence of Testing and Calibration Laboratories, (Third Edition), November 2017

URL: https://www.iso.org/standard/66912.html.

This is a direct access link. However, a fee is required to obtain a copy of the standard.

Summary: This document has been developed with the objective of promoting confidence in the operation of laboratories. This document contains requirements for laboratories to enable them to demonstrate they operate competently and are able to generate valid results. Laboratories that conform to this document will also operate generally in accordance with the principles of ISO 9001. This document requires the laboratory to plan and implement actions to address risks and opportunities. Addressing both risks and opportunities establishes a basis for increasing the effectiveness of the management system, achieving improved results, and preventing negative effects. The laboratory is responsible for deciding which risks and opportunities need to be addressed. This third edition cancels and replaces the second edition (ISO/IEC 17025:2005), which has been technically revised.

• ISO/IEC 17065:2012 (E)—Conformity Assessment—Requirements for Bodies Certifying Products, Processes and Services (First Edition), September 2012

URL: https://www.iso.org/standard/46568.html.

This is a direct access link. However, a fee is required to obtain a copy of the standard.

Summary: This International Standard specifies requirements, the observance of which is intended to ensure that certification bodies operate certification schemes in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of certified products, processes, and services on a national and international basis and so furthering international trade.

XII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), codified as amended at 44 U.S.C. 3501 *et seq.,* agencies are required to provide a 60-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to the Office of Management and Budget for review and approval. In order to fairly evaluate whether an information collection should be approved by the OMB, the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;
2. The accuracy of the agency's estimate of the information collection burden;
3. The quality, utility, and clarity of the information to be collected; and
4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We solicited comment on these issues in the Proposed Rule (84 FR 7558 and 7559) for the matters discussed in detail below.

A. ONC–ACBs

In the Proposed Rule, we proposed to add new ONC—Authorized Certification Bodies (ONC–ACB) collection and reporting requirements for the certification of health IT to the updated 2015 Edition (and any subsequent edition certification) in § 170.523(p), (q), (t), and § 170.550(1).

As stated in the Proposed Rule per § 170.550(l), ONC–ACBs would not be able to certify health IT until they review and verify health IT developers' attestations confirming that the developers are compliant with Conditions and Maintenance of Certification requirements. ONC–ACBs would also submit the health IT developer attestations to ONC per § 170.523(q).

As stated in the Proposed Rule for § 170.523(p)(3), ONC–ACBs would be required to collect and report certain information to ONC related to real world testing plans and results. ONC–ACBs would be required to verify that the health IT developer submits an annual, publicly available real world testing plan and perform a completeness check for both real world testing plans and results.

In the Proposed Rule, we stated for § 170.523(t), ONC–ACBs would ensure health IT developers opting to take advantage of the Standard Version Advancement Process flexibility per § 170.405(b) provide timely advance written notice to the ONC–ACB and all affected customers. ONC–ACBs would maintain a record of the date of issuance and the content of developers' notices, and timely post content of each notice received publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies.

In the 2015 Edition proposed rule (80 FR 16894), we estimated fewer than ten annual respondents for all of the regulatory ''collection of information'' requirements that applied to the ONC–ACBs, including those previously approved by OMB. In the 2015 Edition final rule (80 FR 62733), we concluded that the regulatory ''collection of information'' requirements for the ONC–ACBs were not subject to the PRA under 5 CFR 1320.3(c).

Comments. We did not receive any comments specific to the new ONC–ACB collection and reporting requirements for the certification of health IT to the 2015 Edition (and any subsequent edition certification) in § 170.523(p), (q), (t), and § 170.550(1).

Response. We continue to maintain our past determinations in that we estimate less than ten annual respondents for all of the regulatory ''collection of information'' requirements for ONC–ACBs under part 170 of title 45, including those previously approved by OMB and in this final rule, and that the regulatory ''collection of information'' requirements under the Program described in this section are not subject to the PRA under 5 CFR 1320.3(c). For the cost estimates of these new regulatory requirements, we refer readers to section XIII (Regulatory Impact Analysis) of this final rule.

B. Health IT Developers

We proposed two separate collections from health IT developers in the Proposed Rule. First, we proposed in 45 CFR 170.580(a)(2)(iii) that ONC may take action against a health IT developer for failure to comply with Conditions and Maintenance of Certification requirements. As stated in the Proposed Rule, we proposed to generally use the same processes previously codified in regulation (§§ 170.580 and 170.581) to take administrative enforcement action. These processes would require health IT developers to submit information to ONC to facilitate and conclude ONC's review. The PRA, however, exempts these information collections. We explained in the Proposed Rule that, specifically, 44 U.S.C. 3518(c)(1)(B)(ii) excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities.

Secondly, we proposed in 45 CFR 170.402(b)(1) that a health IT developer must, for a period of 10 years beginning from the date each of a developer's health IT is first certified under the Program, retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the Program for each health IT product. We stated in the Proposed Rule that it would take approximately two hours per week, on average, to comply with our proposed record retention requirement. We welcomed comments on whether more or less time should be included in our estimate.

TABLE 4—ESTIMATED ANNUALIZED TOTAL BURDEN HOURS FOR HEALTH IT DEVELOPERS TO COMPLY WITH RECORDS AND INFORMATION RETENTION REQUIREMENTS

Code of Federal Regulations section	Number of health IT developers	Average burden hours	Total
45 CFR 170.402(b)(1)	458	104	47,632
Total Burden Hours			47,632

Comments. We did not receive any comments specific to either collection of information from health IT developers or our corresponding PRA determinations.

Response. For the first information collection, we continue to maintain that information collected pursuant to an administrative enforcement action is not subject to the PRA under 44 U.S.C. 3518(c)(1)(B)(ii), which excludes collection activities during the conduct of administrative actions or investigations involving the agency against specific individuals or entities. For the second information collection, we continue to believe it will take approximately two hours per week on average to comply with our records and information retention requirements as reflected in Table 4. We refer readers to section XIII (Regulatory Impact Analysis) of this final rule for the cost estimates of the second information collection.

XIII. Regulatory Impact Analysis

A. Statement of Need

This final rule is necessary to meet our statutory responsibilities under the 21st Century Cures Act (Cures Act) and to advance HHS policy goals to promote interoperability and mitigate burden for stakeholders. The provisions finalized in this rule that could result in monetary costs for stakeholders include the: (1) Updates to the 2015 Edition health IT certification criteria; (2) Conditions and Maintenance of Certification requirements for a health IT developer; (3) oversight for the Conditions and Maintenance of Certification requirements; and (4) information blocking.

While much of the costs of this final rule will fall on health IT developers that seek to certify health IT under the ONC Health IT Certification Program (Program), we believe the implementation and use of health IT certified to the 2015 Edition (including the new and updated criteria in this final rule), compliance with the Conditions and Maintenance of Certification requirements, and the limited exceptions to information blocking would ultimately result in significant benefits for health care providers and patients. We outline some of these benefits below. We emphasize in this regulatory impact analysis (RIA) that we believe this final rule will create opportunities for health IT innovation through new market entrants and remove barriers to interoperability and electronic health information exchange. These efforts would greatly benefit health care providers and patients by increasing access to important health information and new technologies resulting in improvements in health care delivery and patient outcomes.

The provisions in this final rule seek to advance an interoperable health system that empowers individuals to use their electronic health information (EHI) to the fullest extent and enable health care providers and communities to deliver smarter, safer, and more efficient care. Given this goal, there will be instances where the benefits and costs are multifaceted and unquantifiable. We note in this RIA when we had difficulty quantifying benefits and costs due to lack of applicable research or data. Additionally, there are ongoing regulatory and policy activities outside of this final rule that might influence the rule's impact in an unquantifiable manner. When possible, we acknowledge these complexities as well. Unquantifiable costs and benefits identified in this rule are summarized in Table 31.

B. Alternatives Considered

In the Proposed Rule, we noted that we were unable to identify alternatives to our proposals that would appropriately implement our responsibilities under the Cures Act and support interoperability. At the time, we assessed whether there were alternatives to our proposals, specifically our proposals concerning EHI export, application programming interfaces (APIs), and real world testing. We concluded that our proposals took the necessary steps to fulfill the mandates specified in the Public Health Service Act (PHSA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Cures Act, in the least burdensome way. We welcomed comments on our assessment and any alternatives that we should consider.

Comments. We received comments suggesting alternatives to our proposals. Specifically, some commenters stated that we should consider an alternative approach to the EHI export (§ 170.315(b)(10)) certification criterion's scope to align with other regulations and data standards, such as the USCDI. Other commenters requested we reconsider the adoption of the consent management for APIs (§ 170.315(g)(11)) certification criterion or use a different platform because the consent2share (C2S) platform was not mature enough. We also received comments requesting we consider alternative definitions for various information blocking terms and reconsider our approach to certain information blocking exceptions. Commenters recommended that we consider these alternatives in order to provide clarity to and reduce potential burden for the regulated community.

Response. Based on comments received, we considered and adopted revisions to our proposals that will substantially reduce real and perceived burden. For the certification criteria, we revised and narrowed the scope of the EHI export certification criterion so that it is more manageable and less administratively burdensome for health IT developers. The criterion will link the data exported to the focused definition of EHI as finalized (see section IV.B.6.c). We also reevaluated and determined, consistent with commenter input, that there is continued work to be done to ballot and field test the C2S platform and the Consent Implementation Guide and, therefore, did not adopt the consent management for APIs (§ 170.315(g)(11)) certification criterion in this final rule (see section IV.B.9.b).

Within the information blocking section, we have focused the scope of many terms to address commenter concerns and reduce potential burden on actors. We have focused the definition of EHI (§ 171.102) (see VIII.C.3). We have also focused the

Health Information Network (HIN) definition in consideration of comments in four ways. First, we combined the definitions of HIN and Health Information Exchange (HIE) to create one functional definition that applies to both statutory terms in order to clarify the types of individuals and entities that would be covered. Second, we limited the types of actions that would be necessary for an actor to meet the definition of HIN or HIE. Third, we have revised the definition to specify that to be a HIN or HIE there must be exchange among more than two unaffiliated individuals or entities besides the HIN/HIE that are enabled to exchange with each other. Fourth, we focused the definition on treatment, payment, and health care operations, as each are defined in the HIPAA Rules (45 CFR 164.501) (see VIII.C.2.c). We have also clarified the scope of the ''access,'' ''exchange,'' and ''use'' definitions and refer readers to the discussion of those changes in section VIII.C.5.a.

We have also considered and finalized alternatives relating to the information blocking exceptions. Of note, we have finalized the new Content and Manner Exception (*see* § 171.301 and the preamble discussion in section VIII.D.2.a), which will significantly reduce burden on actors. First, the *content condition* (§ 171.301(a)) establishes that, in order to satisfy the exception, for up to May 2, 2022, an actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the USCDI standard adopted in § 170.213. Second, the *manner condition* (§ 171.301(b)) explains acceptable alternative manners for fulfilling a request to access, exchange, or use EHI when an actor is technically unable to fulfill a request in any manner requested or cannot reach agreeable terms with the requestor to fulfill the request in any manner requested. This exception creates a transparent and flexible framework for actors to fulfill requests for access, exchange, or use of EHI. We refer readers to the discussion of the Content and Manner Exception in section VIII.D.2.a, as well as the broader discussion within the information blocking section where we discuss various other changes we have made in response to comments that will reduce burden (see section VIII.D).

C. Overall Impact

We have examined the impact of this final rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (January 18, 2011), Executive Order 13771 on Reducing Regulation and Controlling Regulatory Costs (January 30, 2017), the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), and Executive Order 13132 on Federalism (August 4, 1999).

1. Executive Order 13771—Reducing Regulation and Controlling Regulatory Costs

Executive Order 13771 on Reducing Regulation and Controlling Regulatory Costs was issued on January 30, 2017 and directs agencies to repeal two existing regulations for each new regulation issued in fiscal year (FY) 2017 and thereafter. It further directs agencies, via guidance issued by the Office of Management and Budget (OMB), that the total incremental costs of all regulations should be no greater than zero in FY 2018. The analysis required by Executive Order 13771, as supplemented by Executive Order 13777, adds additional requirements for analysis of regulatory actions. The new requirements under Executive Orders 13771 and 13777 do not change or reduce existing requirements under Executive Orders 12866 or 13563. This final rule is an E.O. 13771 regulatory action. We estimate this rule generates $0.84 billion in annualized costs in 2016 dollars, discounted at 7 percent relative to year 2016 over a perpetual time horizon.

2. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis

Executive Orders 12866 on Regulatory Planning and Review and 13563 on Improving Regulation and Regulatory Review direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). Pursuant to the Congressional Review Act (5 U.S.C. 801 *et seq.*), the Office of Information and Regulatory Affairs designated this rule as a 'major rule' as defined by 5 U.S.C. 804(2). OIRA has also determined that this final rule is an economically significant rule as we have estimated the costs to implement this final rule may be greater than $100 million per year. Accordingly, we have prepared an RIA that to the best of our ability presents the costs and benefits of this final rule.

a. Costs and Benefits

We have estimated the monetary costs and benefits of this final rule for health IT developers, health care providers, patients, ONC—Authorized Certification Bodies (ONC–ACBs), ONC—Authorized Testing Laboratories (ONC–ATLs), and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out into the following categories: (1) Deregulatory actions (no associated costs); (2) updates to the 2015 Edition health IT certification criteria; (3) Conditions and Maintenance of Certification requirements for a health IT developer; (4) oversight for the Conditions and Maintenance of Certification requirements; and (5) information blocking.

In accordance with Executive Order 12866, we have included the RIA summary table as Table 30. In addition, we have included a summary to meet the regulatory reform analysis requirements under Executive Order 13771.

Cost and benefit calculations were performed in 2017 dollars, as this year was the most recent data available to address all cost and benefit estimates consistently. For summary tables 29 through 31, all estimates are rounded to the nearest dollar and expressed in 2016 dollars to meet regulatory reform analysis requirements under Executive Order 13771.

We note that estimates presented in the following ''Employee Assumptions and Hourly Wage,'' ''Quantifying the Estimated Number of Health IT Developers and Products,'' and ''Number of End Users that Might Be Impacted by ONC's Final Rule'' sections are used throughout this RIA.

In this final rule, we used a number of methods to quantify direct and indirect benefits of our provisions. For provisions where no such research was available, we developed estimates based on a reasonable proxy. Interoperability, for example, can positively impact patient safety, care coordination, and improve health care processes and health outcomes.[192] However, achieving interoperability is a function of several factors, not just the capability of the technology used by health care providers. Therefore, to assess some of the benefits of this final rule, we used regression analysis to assess their

[192] *https://www.qualityforum.org/Publications/2017/09/Interoperability_2016-2017_Final_Report.aspx.*

respective effects on interoperability holding other factors constant.

One example of this approach is the methodology used to quantify the benefits of our real world testing and API provisions on interoperability. We used regression analysis to calculate the impact of our real world testing and API provisions on interoperability. We assumed that the real world testing and API provisions would collectively have the same impact on interoperability as upgrading health IT certified to the 2014 Edition. Therefore, we estimated linear probability models that identified the impact of 2014 Edition certified health IT on hospitals' interoperability.[193] We used data from the 2014 and 2015 American Hospital Association (AHA) Annual Survey Information Technology Supplement (IT Supplement), which consists of an analytic sample of 4,866 observations of non-Federal acute care hospitals that responded to the IT Supplement.[194] We controlled for additional factors such as participation in a health information exchange organization, hospital characteristics, and urban/rural status. More specifically, we used the following explanatory variables:

Edition = 1 if a hospital adopted 2014 Edition EHR, 0 otherwise
RHIO = 1 if a hospital participates in health information exchange organization, 0 otherwise
Government = 1 if a hospital is publicly owned, 0 otherwise
Alt_teaching = 1 if a hospital is teaching, 0 otherwise
Nonprofit = 1 if a hospital is not for profit, 0 otherwise
Largebed = 1 if a hospital has more than 399 beds, 0 otherwise
Medbed = 1 if a hospital's number of beds is between 100 and 399, 0 otherwise
Urban_rural = 1 if a hospital is urban, 0 otherwise
CAH = 1 if a hospital is critical access, 0 otherwise
Year = year of the data (2014 and 2015)
S = state fixed effects

We found a statistically significant marginal effect of using 2014 Edition certified health IT associated with a five percentage point increase in interoperability.[195]

While we acknowledge that there might be shared benefits across provisions, we have taken steps to ensure that the benefits attributed to each provision is unique to the provision referenced. For example, in the case of assessing the impact of our real world testing and API provisions on interoperability, we assumed that the marginal effect is true and distributed the five percentage point benefit across our provisions at (0.1–1) to (1–4) percentage points respectively. Given data limitations, we believe this approach allowed us to estimate the benefits of our final provisions without double counting the impact each provision might have on interoperability.

Employee Assumptions and Hourly Wage

We have made employee assumptions about the level of expertise needed to complete the requirements in this section of the final rule. For wage calculations for Federal employees and ONC–ACBs, we have correlated the employee's expertise with the corresponding grade and step of an employee classified under the General Schedule (GS) Federal Salary Classification, relying on the associated employee hourly rates for the Washington, DC locality pay area as published by the Office of Personnel Management for 2017.[196] We have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages. Therefore, we have doubled the employee's hourly wage to account for overhead costs. We have concluded that a 100 percent expenditure on overhead costs which includes benefits is an appropriate estimate based on research conducted by HHS.[197]

We have used Bureau of Labor Statistics (BLS) data to calculate private sector employee wage estimates (*e.g.,* health IT developers, health care providers, health information networks (HINs), attorneys, etc.), as we believe BLS provides the most accurate and comprehensive wage data for private sector positions. Just as with the General Schedule Federal Salary Classification calculations, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages.

We estimated using 2016 dollars in the Proposed Rule. However, we stated in the Proposed Rule that we would consider using 2017 and even 2018 dollars, if available, for our cost and benefit estimates in the final rule. Therefore, in this final rule, we updated our estimates using 2017 dollars for the GS Federal Salary Classification and the BLS data.

Quantifying the Estimated Number of Health IT Developers and Products

We derived our estimates for the potential impact of the new 2015 criteria on the number of certified products in the health IT market. This analysis is based on the number of certified health IT products (*i.e.,* Health IT Modules), product capability, and the number of health IT developers that left, merged, and/or entered the ONC Health IT Certification Program between the 2011 Edition health IT certification criteria (2011 Edition) and the implementation of the 2014 Edition health IT certification criteria (2014 Edition).[198]

In Table 5, we quantify the extent to which the certified health IT market consolidated between the 2011 Edition and 2014 Edition. We found that the number of health IT developers certifying products between the 2011 Edition and 2014 Edition decreased by 22.1 percent and the number of products available decreased by 23.2 percent.

[193] The interoperability dependent variable is a binary indicator for whether a hospital routinely sends, receives, and integrates summary of care records electronically outside of its system and finds any health information electronically outside of its system.

[194] American Hospital Association Health IT Supplement Survey, *http://www.ahadata.com/aha-healthcare-database/.*

[195] Results were similar when we used logit or Probit specifications. Note, the percentage point refers to the arithmetic difference between two percentages.

[196] *https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2017/DCB_h.pdf.*

[197] *See* U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation (ASPE), *Guidelines for Regulatory Impact Analysis,* at 28–30 (2016), *available at https://aspe.hhs.gov/system/files/pdf/242926/HHS_RIAGuidance.pdf.*

[198] Availability of 2014 CEHRT for Meaningful Users Providers, Health IT Policy Committee Data Update (Sept. 9, 2015), *available at http://www.healthit.gov/FACAS/sites/faca/files/HITPC_Data_Update_Presentation_Final_2015-09-09.pdf.*

TABLE 5—CERTIFIED HEALTH IT MARKET CONSOLIDATION FROM THE 2011 EDITION TO THE 2014 EDITION

	2011 Edition	2014 Edition	Market consolidation (%)
Health IT Developers	1,017	792	−22.1
Products Available	1,408	1,081	−23.2

[A] For the purposes of these market consolidation calculations, we included the total number of active or suspended health IT products and their developers. Withdrawn products and their developers were excluded from this total.

Using the rates identified in Table 5, we then applied our estimate for market consolidation to estimate the number 2015 Edition certified health IT products and health IT developers that would be impacted by our policies in this final rule. Specifically, to estimate the number of 2015 Edition products and health IT developers in the market, we assumed:

- *Products capable of recording EHI will include new certification criteria.* We assume that products capable of recording patient health data will be the types of products most likely to be impacted by and include the new certification criteria.
- *Products capable of recording EHI data available in 2015 equal the number of products available in 2014.* In 2014, there were 710 products by 588 developers capable of recording EHI. Since the new criteria involve the access to and movement and exchange of EHI, we used only products that record EHI as a basis for our estimates. We believe the 2014 totals reflect a realistic estimate of the currently available products and their developers that could include the new 2015 certification criteria.
- *Market consolidation rates denoted in Table 5 hold constant.* We assume that the rate of market consolidation for products (–23.2 percent) and health IT developers (–22.1 percent) from the 2011 Edition to the 2014 Edition holds constant for the 2015 Edition. Although we are using this number to estimate product availability, we are unable to assess how market consolidation might impact other production costs such as the supply and demand for personnel over time.

As shown in Table 6, based on the assumptions, we have estimated the total number of 2015 products (545) and their developers (458).

TABLE 6—TOTAL NUMBER OF HEALTH IT DEVELOPERS AND PRODUCTS BY SCENARIO

Scenario	Estimated number of health IT developers	Estimated number of products
2015 Edition Projection—All Products	617	830
2015 Edition Projection—Products Capable of Recording EHI	458	545

Number of End Users That Might Be Impacted by ONC's Final Rule

For the purpose of this analysis, the population of end users differs according to the regulatory action finalized. In many cases, the end-user population impacted is the number of hospitals and health care providers that possess certified health IT. Due to data limitations, our analysis regarding the number of hospitals and health care providers impacted by the regulatory action is based on the number of hospitals and health care providers that have historically participated in the Centers for Medicare & Medicaid Services (CMS) EHR Incentive Programs (now Promoting Interoperability (PI) Programs).

One limitation of this approach is that we are unable to account for the impact of our provisions on users of health IT that were ineligible or did not participate in the CMS EHR Incentive Programs. For example, in 2017, 78 percent of home health agencies and 66 percent of skilled nursing facilities reported adopting an EHR.[199] Nearly half of these facilities reported engaging aspects of health information exchange. However, we are unable to quantify, specifically the use of certified health IT products, among these provider types.

Despite these limitations, participants in the CMS EHR Incentive Programs represent an adequate sample on which to base our estimates.[200] There were 439,187 health care providers [201] in 95,470 clinical practices [202] and 4,519 hospitals [203] that participated in the CMS EHR Incentive Program. We estimate that these entities will be impacted by our rule.

General Comments on the RIA

Comments. Several commenters expressed concern that the estimated costs and developer hours in the proposed rule were significantly underestimated. One commenter stated that the cost estimates did not accurately reflect provider implementations costs, including those related to ensuring compliance with the HIPAA Rules, 42 CFR part 2 and other Federal and State privacy laws. Some commenters were concerned about the impact of the requirements, as proposed in the Proposed Rule, on existing small health IT developers and their ability to

[199] Henry, J., Pylypchuck, Y., & Patel, V. (November 2018) Electronic Health Record Adoption and Interoperability among U.S. Skilled Nursing Facilities in 2017. ONC Data Brief, no. 41. Office of the National Coordinator for Health Information Technology: Washington, DC.

[200] *See* Office of the National Coordinator for Health Information Technology, *Office-based Health Care Professionals Participating in the CMS EHR Incentive Programs* (Aug. 2017), *dashboard.healthit.gov/quickstats/pages/FIG-Health-Care-Professionals-EHR-Incentive-Programs.php*; Office of the National Coordinator for Health Information Technology, *Hospitals Participating in the CMS EHR Incentive Programs* (Aug. 2017), *dashboard.healthit.gov/quickstats/pages/FIG-Hospitals-EHR-Incentive-Programs.php*.

[201] This estimate is the total number of eligible providers that ever participated in the CMS Medicare and Medicaid Electronic Health Record Incentive Program.

[202] This number was estimated based on the de-duplicated number of practices that had at least one clinician participate in the CMS Medicare Electronic Health Record Incentive Program.

[203] This estimate is the total number of eligible hospitals that ever participated in the CMS Medicare Electronic Health Record Incentive Program.

compete with large developers, as well as the impact on potential new market entrants. One commenter stated that this environment will result in only a small number of health IT developers surviving while also limiting market entry. One commenter expressed concern that the Proposed Rule will provide unfettered access to the intellectual property of health IT developers while increasing their compliance costs, which will limit their potential investment returns and create barriers to market entry. A few commenters expressed concern that the costs incurred by health IT developers to improve interoperability and comply with other aspects of the rule as proposed will be passed on to providers and patients.

Response. We thank commenters for their input regarding our estimated costs and developer hours in the Proposed Rule. We considered and adopted revisions to our proposals based on comments that would substantially reduce any real or perceived burden. We reanalyzed our approach and made adjustments for this final rule. For instance, we have included additional developer hours for the additional data elements we finalized in this final rule. We have also included additional costs for the bulk data standard support and API support. Lastly, with regards to the comment that the cost estimates did not accurately reflect implementation costs to providers, when possible ONC has quantified provider costs associated with the deployment of new certified health IT functionalities and the optional acquisition of emerging API technologies. Costs that are not quantifiable are noted in Table 31. However, costs related to ensuring compliance with the HIPAA Rules, 42 CFR part 2 and other Federal and State privacy laws, are beyond the scope of the certification criteria and are not included in the final rule.

We understand commenters' concerns about the impact of the provisions as proposed on small health IT developers and the potential impact on new market entrants. However, we continue to believe that while much of the costs of the final rule will fall on health IT developers seeking to certify health IT under the Program, the implementation and use of health IT certified to the 2015 Edition (including the updated and new criteria in this final rule), compliance with the Conditions and Maintenance of Certification requirements, and the limited exceptions to information blocking would ultimately result in significant benefits for health care providers and patients. We also emphasize that we believe the final rule will create opportunities for new market entrants and will remove barriers to interoperability and electronic health information exchange, which will greatly benefit health care providers and patients as well.

(1) Deregulatory Actions

Costs

We do not expect incurred costs to be associated with the deregulatory actions in this final rule, but rather cost savings as detailed further in this Regulatory Impact Analysis.

Benefits

We expect the deregulatory actions of the rulemaking to result in benefits for health IT developers, providers, ONC–ACBs, ONC–ATLs, and ONC.

(i) Removal of the Randomized Surveillance Minimum Threshold Requirements

In this final rule, we have revised § 170.556(c) to specify that ONC–ACBs *may* conduct in-the-field, randomized surveillance. We have removed § 170.556(c)(2), which specifies that ONC–ACBs must conduct randomized surveillance for a minimum of two percent of certified health IT products per year. Additionally, we have removed the requirement that ONC–ACBs make a good faith effort to complete randomized surveillance and the circumstances permitted for exclusion from the requirement found in § 170.556(c)(5).

In the 2015 Edition final rule, we did not independently estimate the costs for randomized surveillance. Rather, we relied on prior regulatory cost estimates for all surveillance actions. One of our four ONC–ACBs charges a $3,000 annual fee per product for surveillance due to the new randomized surveillance requirements and to help normalize their revenue stream during down cycles between certification editions. Using this fee as a cost basis and assuming it would apply to all certified health IT (as opposed to the market-adjusted universe of health IT that is used in other calculations in this RIA), we estimated that the removal of the randomized surveillance ''two percent minimum threshold'' requirements will result in cost savings between $6.8 and $13.7 million for all stakeholders. To arrive at this estimate, we multiplied the $3000 annual fee per product for surveillance by the total number of products certified to the 2014 Edition which was 4,559 products at the time ($3,000*4,559 = $13.7 million). We anticipate the number of products certified for 2014 to decrease to a little as half of the original count over time. Therefore, we estimated the low end to be half of the $13.7 million (0.5*$13.7 million = $6.8 million). This estimate is based on feedback we received from our ONC–ATLs and ONC–ACBs. ONC–ACBs performed randomized surveillance an average of 22 times the first year the requirement was in effect. The following year surveillance was performed an average of two times. We cannot predict how many randomized surveillance events the ONC–ACBs will perform now that we are not enforcing the requirement. It will be completely at the discretion of the ONC–ACBs.

In the Proposed Rule, we noted that we considered other potential benefits that we were unable to quantify. For instance, we considered that health care provider burden may decrease from the elimination of the two percent minimum threshold requirements because a provider would previously aid the ONC–ACB in software demonstrations.

We welcomed comments on potential means, methods, and relevant comparative studies and data that we could use to better quantify these benefits.

Comments. We did not receive any comments specific to the calculation of benefits of the elimination of the two percent minimum threshold requirements.

Response. We have maintained our approach in calculating the benefits of this provision in this final rule. We believe the removal of the randomized surveillance minimum threshold requirements will reduce the burden on health care providers by reducing their exposure to randomized in-the-field surveillance of their health IT products. Health care providers previously expressed concern about the time commitment to support ONC–ACB randomized surveillance of health IT products, particularly if no non-conformities with certified health IT were found. Providers have generally stated that reactive surveillance (*e.g.,* complaint-based surveillance) is a more logical and economical approach to surveillance of health IT products implemented in a health care setting. We also believe the removal of these requirements will provide health IT developers more time to focus on interoperability, and will provide ONC–ACBs more time to respond to reactive surveillance, including health care provider complaints about certified health IT.

(ii) Removal of the 2014 Edition From the Code of Federal Regulations

We estimate that health IT developers would realize monetary savings from no

longer supporting the 2014 Edition certification criteria due to a reduction in activities related to maintaining certification and surveillance. We are aware that one of our ONC–ACBs charges an inherited certified status (ICS) fee of $1,000. This fee has been applied over the last calendar year. Over that time period, the number of new, unique 2014 Edition products has been declining (24 products, and no new products in the last four months) compared to the number of ICS certifications (569). Just assuming the cost of continued ICS certification, health IT developers would be paying approximately $569,000 each year to keep their 2014 Edition products up to date. Based on recent analysis of the number of unique 2014 Edition products, our assumptions hold true.

We are not aware of comparable fees charged by ONC–ATLs; however, based on our experience with the Program, we expect health IT developers would realize similar cost savings associated with ONC–ATL maintenance of the testing component associated with ICS. Thus, we estimate an additional $569,000 cost savings for health IT developers due to the reduced testing requirements.

We also attempted to identify a potential reduction in maintenance and administrative costs as a result of removing 2014 Edition certification criteria. We could not obtain data to conduct a full quantitative analysis specific to the reduction of health IT developer and health care provider costs related to supporting and maintaining the 2014 Edition. However, we invited comments on methods to quantify potential costs for maintaining and supporting products to previous editions.

We did conduct a review of academic literature and qualitative analysis regarding potential savings from no longer supporting the 2014 Edition. We looked at data in IT industry systems as whole, which showed that upgrading outdated legacy systems saves resources otherwise spent on maintaining compatibilities to multiple systems and also increases quality and efficiency.[204] Furthermore, as technology evolves, newer software and products allow for smoother updates compared to their predecessors. Newer products provide better security features that can address both new and existing issues. In addition, older software has an increased risk of failure, which, in the health IT industry, increases risk to patient safety.

From the implementer's perspective, the research indicated that retaining legacy systems tends to inhibit scalability and growth for businesses. The perpetuity of outdated legacy systems increases connection and system integration costs and limits the ability to realize increased efficiency through IT implementation. Newer products are developed to current specifications and updated standards, which decreases barriers and marginal cost of ancillary product implementation and increases the accessibility of data in ancillary systems—including via mobile devices and the latest applications. Finally, office staff in a health care setting would no longer need to be trained to accommodate differing data access needs or workarounds required to integrate to the legacy product.[205]

The research also indicates that retaining legacy software would not be beneficial or profitable to the health IT market. Prolonging backwards compatibility of newer products to legacy systems encourages market fragmentation.[206] We intend to encourage the health IT market to keep progressing with a baseline expectation of functionalities that evolve over time. This requires limiting fragmentation by no longer supporting outdated or obsolete legacy software.[207]

We also estimate that additional savings could be realized by reducing regulatory complexity and burden caused by having two certification editions. We observed that the task of managing two different editions within different rules increases complexity and burden for ONC staff, contractors, ONC–ACBs, CMS programs referencing the certification criteria, and other stakeholders, as compared to removing the 2014 Edition certification criteria. However, we were unable to estimate these benefits because we have no means for quantifying the benefits gained from only using the 2015 Edition.

We also expect that health care providers would benefit from removing the 2014 Edition certification criteria because such action would likely motivate health IT developers to certify health IT products to the 2015 Edition, thus enabling providers to use the most up-to-date and supported systems to care for patients.

Comments. We did not receive comments specific to our methods for quantifying the potential costs for maintaining and supporting products to previous editions.

Response. We have maintained our approach for quantifying costs for health IT developers maintaining and supporting products to the previous 2014 Edition. We have also emphasized again that the research indicates that retaining legacy software would not be beneficial or profitable to the health IT market.

(iii) Removal of the ONC-Approved Accreditor From the ONC Health IT Certification Program

We expect ONC to realize monetary cost savings from removing the ONC-Approved Accreditor (ONC–AA) from the Program. We expect ONC to realize costs savings from no longer: (1) Developing and publishing a **Federal Register** Notice and listserv; (2) monitoring the open application period and reviewing and making decisions regarding applications; and (3) oversight and enforcement of the ONC–AA. We have calculated the estimated annual cost savings for removing the ONC–AA from the Program, taking into consideration that the ONC–AA renewed its status every three years.

For our calculations, we used the estimated hours for collaborating with and informing an ONC–AA in 2017 (using 2017 wage estimates). We estimated that ONC spent approximately 110 hours collaborating with the ONC–AA in 2017, which includes (all at the GS–13, Step 1 level): Annual assessments; providing appropriate guidance; implementing new requirements and initiatives; and consultations as necessary. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Therefore, we estimated the annual cost savings to be $3,337.

We estimate that ONC would commit approximately eight hours of staff time to develop the **Federal Register** Notice, which would include approximately: Four hours for drafting and review by an analyst at the GS–13, Step 1 level; two hours for review and analysis by senior certification staff at the GS–14, Step 1 level; and two hours for review and submittal for publication by Immediate Office staff at the GS–15, Step 1 level. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. The hourly wage with benefits for a GS–14, Step 1 employee located in

[204] James Crotty and Ivan Horrocks, *Managing legacy system costs: A case study of a meta-assessment model to identify solutions in a large financial services company,* Applied Computing and Informatics (2017), at 1–9.

[205] *Id.*

[206] Il-Horn Hann, Byungwan Koh, and Marius F. Niculescu, *The Double-Edged Sword of Backward Compatibility: The Adoption of Multigenerational Platforms in the Presence of Intergenerational Services,* Inform. Systems Res. (2016), at 112–30.

[207] *Id.*

Washington, DC is approximately $107. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $126. Therefore, we estimate the annual cost savings to be $277. Additionally, we estimate a cost of $477 to publish each page in the **Federal Register**, which includes operational costs. The **Federal Register** Notice for ONC–AAs requires, on average, one page in the **Federal Register** (every three years), so we estimated an additional annual cost savings of $159.

We estimated that ONC will commit approximately two hours of staff time by an analyst at the GS–13, Step 1 level to draft, review, and publish the listserv to announce the **Federal Register** Notice. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Therefore, we estimate the annual cost savings to be $61.

We estimated that ONC would commit approximately 25 hours of staff time to manage the open application process, review applications and reach application decisions, which would include approximately: 20 hours by an analyst at the GS–13, Step 1 level; three hours by senior certification staff at the GS–14, Step 1 level; and two hours for review and approval by Immediate Office staff at the GS–15, Step 1 level. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. The hourly wage with benefits for a GS–14, Step 1 employee located in Washington, DC is approximately $107. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $126. Therefore, we estimated the annual cost savings to be $798.

Taking all of these potential costs savings into consideration, we estimated the overall annual costs savings for removing the ONC–AA from the Program to be $4,632.

(iv) Removal of Certain 2015 Edition Certification Criteria

In section III.B.4 of this final rule, we removed the following certification criteria from the 2015 Edition: § 170.315(b)(4) ''Common Clinical Data Set summary—create;'' (b)(5) ''Common Clinical Data Set summary—receive'' and § 170.315(a)(11) ''Smoking status.'' We did not finalize the proposal to remove of § 170.315(a)(10) ''Drug formulary and preferred drug list checks,'' § 170.315(a)(13) ''Patient-specific education resources'' and § 170.315(e)(2) ''Secure messaging'' but rather will only permit ONC–ACBs to issue certificates for these criteria until January 1, 2022 to align with requirements of the CMS Medicaid PI Program.

For determining calculations for the majority of the 2015 Edition certification criteria we removed, we used the following assumptions. (For the removal of § 170.315(b)(4) Common Clinical Data Set summary—create and (b)(5) Common Clinical Data Set summary—receive, we outlined the slightly different approach used).

In the 2015 Edition final rule, we estimated the costs for developing and preparing health IT to meet the 2015 Edition certification criteria. The development and preparation costs we estimated were derived through a health IT developer per criterion cost. We estimated the development and preparation costs over a four-year period, and we projected the costs would be unevenly distributed. In figuring out the cost savings for the deregulatory actions, we initially used the distribution from the 2015 Edition, but then adjusted the percentages of development and preparation costs due to current empirical and anecdotal evidence. The distribution was reevaluated to account for 2019 and we estimated the actual development and preparation distribution for 2018 to be 35 percent and for 2019 to be 15 percent. We took the average development and preparation cost estimates (low and high) per criterion from Table 14 of the 2015 Edition final rule (80 FR 62737). We then used our new distribution to identify the cost per year for years 2018 and 2019. We took the total estimated costs for 2018 and 2019 and divided that by 12 to determine the cost savings per month and took a range of 6 to 12 months. Based on analysis of recent data, our assumptions continue to hold true.

To determine the testing costs of the deregulatory actions, we took the number of health IT developers who develop products for certification for the identified criteria from the 2015 Edition final rule and then figured out the average cost per criterion. Based on the costs that one of the ONC–ATLs charges for testing, we estimated the average cost for testing per criterion and determined subsequent cost savings. In 2017, only about five to ten percent of products have been tested and certified compared to the number of certified 2014 Edition products. Therefore, up to 90 to 95 percent of products remain to be tested and certified to the 2015 Edition. Based on analysis of recent data, our assumptions continue to hold true.

We estimated the total cost savings by multiplying the number of health IT developers who developed products for certification to a certain criterion by the estimated cost per criterion, $475. We then took five percent of that number to identify the high end for the cost savings. We then took 10 percent to identify the low end. The five percent was derived from looking at the number of unique developers who have at least one active 2014 Edition product and the number of unique developers who have at least one active 2015 Edition. The denominator is the number of unique developers who have at least one active 2014 Edition product, which is 793. The numerator is the number of unique developers who have at least one active 2015 Edition product and one active 2014 edition product, which is 41. (41/793 = 0.0517024 or 5 percent).

(A) Common Clinical Data Set Summary Record Criteria

In this final rule, we removed the Common Clinical Data Set summary—create (§ 170.315(b)(4)) and Common Clinical Data Set summary—receive (§ 170.315 (b)(5)) criteria.

Our expectation was for ONC to realize cost savings associated with internal infrastructure support and maintenance, which would include actions such as: (1) Developing and maintaining information regarding these criteria on the ONC website; (2) creating documents related to these criteria and making those documents 508 compliant; (3) updating, revising, and supporting Certification Companion Guides, test procedures, and test tools; and (4) responding to inquiries concerning these criteria. Based on ONC data on the number of inquiries received since early 2016, we estimated approximately 12 annual inquiries about § 170.315(b)(4) and (5) respectively, (24 total inquiries for two criteria). We estimate it will take an analyst at the GS–13, Step 1 level an average of two hours to conduct all tasks associated with each inquiry. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Based on analysis of recent data, our assumptions continue to hold true.

Therefore, we estimated the annual cost savings to be $4,360.

We do not expect cost savings associated with software maintenance because both criteria incorporate the Common Clinical Data Set and essentially the same data input and validation requirements as the transitions of care criterion (§ 170.315(b)(1)). The removal of these two criteria would not affect the test data and software maintenance costs, as the same test data and software validation elements remain in

§ 170.315(b)(1) and the Common Clinical Data Set used in other criteria.

ONC–ACBs could realize minimal savings, as they would need to conduct slightly less surveillance based on the two products that are currently certified to these criteria. We estimated the overall annual costs savings for removing the Common Clinical Data Set summary record certification criteria from the 2015 Edition to be $4,368.

Comments. We did not receive comments specific to the removal of the Common Clinical Data Set summary—create (§ 170.315(b)(4)) and Common Clinical Data Set summary—receive (§ 170.315 (b)(5)) criteria.

Response. We maintained our approach and estimates for removing the Common Clinical Data Set summary record certification criteria from the 2015 Edition. However, we did update estimates to 2017 dollars.

(B) Smoking Status

In this final rule, we removed the 2015 Edition ''smoking status'' criterion (§ 170.315(a)(11)), which would include removing it from the 2015 Edition Base EHR definition. To calculate the cost savings for removing this criterion, we used the 2015 Edition estimated costs of developing and preparing the criterion to the 2015 Edition, between $15,750 and $31,500 and estimated that 35 percent of developers would be newly certified in 2018 and 15 percent in 2019. We estimated the cost of development and preparation costs to be between $5,512.50 and $11,025 for 2018 and $2,362.50 and $4,725 for 2019. We calculated the cost per month for years 2018 and 2019 and using the high point estimates, estimated the development and preparation costs over a 6 to 12 month period between August 2018 and August 2019. We estimated the costs to be between $4,068.75 at six months and $6,825 at 12 months. Based on analysis of recent data, our assumptions continue to hold true.

To calculate the cost for testing for this criterion, five developers were estimated in the 2015 Edition to develop products to this criterion. We multiplied the five developers by our estimated cost to test per criterion of $475. This estimated cost per criterion was based on what one ONC–ATL charged for testing and averaged per criterion. To be conservative, we reduced the number by ten percent and five percent respectively resulting in $2,137.50 and $2,256.25.

Taking these estimated costs into account we expect the cost savings for removing the 2015 Edition ''smoking status'' criterion to be between $8,962.50 and $9,081.25.

Comments. We did not receive comments specific to the removal of the 2015 Edition ''smoking status'' criterion (§ 170.315(a)(11)).

Response. We maintain our approach and estimates for removing the 2015 Edition ''smoking status'' criterion (§ 170.315(a)(11)) from the 2015 Edition. However, we did update estimates to 2017 dollars.

(v) Removal of Certain Certification Requirements

In this final rule, we removed § 170.523(k)(1)(iii)(B), which requires ONC–ACBs to ensure that certified health IT includes a detailed description of all known material information concerning limitations that a user may encounter in the course of implementing and using the certified health IT, whether to meet ''meaningful use'' objectives and measures or to achieve any other use within the scope of the health IT's certification. We also removed § 170.523(k)(1)(iv)(B) and (C), which state that the types of information required to be disclosed include, but are not limited to: (B) Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified; (C) limitations, including, but not limited to, technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

To calculate the savings related to removing these two disclosure requirements, we estimated 830 products certified to the 2015 Edition. We did so by applying the market consolidation rate of −23.2 percent which was the rate observed between 2011 and 2014 Editions. If an ONC–ACB spends 1 hour on average reviewing costs, limitations and mandatory disclosures, we estimated the time saved by no longer having to review the limitations to be two-thirds of an hour. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91 and we assume this to be the hourly rate for an ONC–ACB reviewer. We multiplied 830, the projected number of certified products, by two-thirds of an hour and the assumed hourly rate and calculated the cost savings to be $50,353.

(2) Updates to the 2015 Edition Certification Criteria

The following section details the costs and benefits for updates to the 2015 Edition health IT certification criteria, which includes costs and benefits to update certain 2015 Edition criteria to due to the adoption of the United States Core Data for Interoperability (USCDI) as a standard, and costs for new or revised 2015 Edition criteria for: EHI export, API, privacy and security transparency attestations, and security tags.

(i) United States Core Data for Interoperability

In order to advance interoperability by ensuring compliance with new structured data and code sets that support the data, we have replaced the ''Common Clinical Data Set'' (CCDS) definition and its references with the ''United States Core Data for Interoperability'' (USCDI) standard, naming Version 1 (v1) in § 170.213 and incorporated it by reference in § 170.299. The USCDI will replace the CCDS 24 months after the publication date of this final rule. The USCDI v1 establishes a minimum set of data classes (including structured data) that are required for health IT to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time.

The USCDI v1 adds three new data classes, ''Allergies and Intolerances,'' ''Clinical Notes,'' and ''Provenance;'' and adds to ''Patient Demographics'' the data elements ''Previous Address,'' ''Phone Number,'' ''Phone Number Type,'' and ''Email Address'' that were not defined in the CCDS. This requires updates to the Consolidated Clinical Document Architecture (C–CDA) standard and updates to the following certification criteria: § 170.315(b)(1) (transitions of care); (e)(1) (view, download, and transmit to 3rd party); (g)(6) (Consolidated CDA creation performance); (f)(5) (transmission to public health agencies—electronic case reporting); and (g)(9) (application access—all data request). From our analysis of the C–CDA standard, we concluded that the requirements of the ''Provenance'' data class are already met by the existing C–CDA standard and will not require any new development. Therefore, we have estimated the cost to health IT developers to add support for ''Allergies and Intolerances'' and ''Clinical Notes'' data classes and ''Previous Address,'' ''Phone Number,''

''Phone Number Type,'' and ''Email Address'' data elements in C–CDA, and the necessary updates to the affected certification criteria. These estimates are detailed in Table 7 and are based on the following assumptions:

• *Health IT developers will use the same labor costs and data models.* Table 7 shows the estimated labor costs per product for a health IT developer to develop support for the additional USCDI data element in the C–CDA standard and affected certification criteria. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 7.

• *A proxy is needed to project the number of 2015 Edition certified health IT products.* As the 2015 Edition certification is ongoing, using the current count of developers and products would underestimate the overall costs and benefits, so we therefore use a proxy. We estimate that 545 products from 458 developers will be affected. Our proxy is based on the number of 2014 Edition certified health IT products that are capable of recording patient data.[208] There were 710 products by 588 developers with at least one 2014 Edition product capable of recording patient data. We then multiplied these numbers by our certified health IT market consolidation estimates of −22.1 percent and −23.2 percent to project the number of 2015 developers and products, respectively.

• *According to the May 2017 BLS occupational employment statistics,* the mean hourly wage for a ''Software Developer'' is $53.74.[209]

TABLE 7—COSTS TO HEALTH IT DEVELOPERS TO DEVELOP SUPPORT FOR THE ADDITIONAL USCDI DATA ELEMENT IN C–CDA STANDARD AND AFFECTED CERTIFICATION CRITERIA

[2017 Dollars]

Tasks	Details	Lower bound hours	Upper bound hours	Remarks
Update C–CDA creation	New development to support ''Allergies and Intolerances,'' ''Clinical Notes,'' ''Previous Address,'' ''Phone Number,'' ''Phone Number Type,'' and ''Email Address'' for C–CDA and C–CDA 2.1 Companion Guide.	1,200	2,400	(1) Lower bound assumes health IT already has developed C–CDA R2.1 into their system and only needs to be updated for new data elements. (2) Upper bound estimates effort for organizations that are on older versions of C–CDA standard, for example C–CDA R1.1.
§ 170.315(b)(1) (transitions of care)	New development to support ''Allergies and Intolerances,'' ''Clinical Notes,'' ''Previous Address,'' ''Phone Number,'' ''Phone Number Type,'' and ''Email Address'' for C–CDA and C–CDA 2.1 Companion Guide.	200	600	Necessary updates to health IT to support the new data class to meet the criteria requirements.
§ 170.315(e)(1) (view, download, and transmit to 3rd party).	New development to support ''Allergies and Intolerances,'' ''Clinical Notes,'' ''Previous Address,'' ''Phone Number,'' ''Phone Number Type,'' and ''Email Address'' for C–CDA and C–CDA 2.1 Companion Guide.	400	1,000	Necessary updates to health IT to support the new data class to meet the criteria requirements.
§ 170.315(g)(6) (Consolidated CDA creation performance).	New development to support ''Allergies and Intolerances,'' ''Clinical Notes,'' ''Previous Address,'' ''Phone Number,'' ''Phone Number Type,'' and ''Email Address'' for C–CDA and C–CDA 2.1 Companion Guide.	200	600	§ 170.315(b)(1) and § 170.315(g)(6) are related and may be developed together.
Total Hours		2,000	4,600	
Hourly Rate		$107		
Cost per Product		$214,000	$492,200	
Total Cost (545 products)		$116.6 million	$268.2 million	

We estimated that the cost to a health IT developer to develop support for the additional USCDI data elements would range $214,000 to $492,200. Therefore, assuming 545 products, we estimate that the total annual cost to all health IT developers would, on average, range from $116.6 million to $268.2 million. This would be a one-time cost to developers per product that is certified to the specified certification criteria and would not be perpetual.

We believe this would benefit health care providers, patients, and the industry as a whole. Clinical notes and provenance were included in the draft USCDI v1 based on significant feedback from the industry, which highly

[208] We defined ''products capable of recording patient data'' as any 2014 Edition health IT product that was certified for at least one of the following criteria: Demographics ((a)(5)), Medication List ((a)(7)), Medication Allergy List ((a)(8)), Problem List ((a)(6)), and Family Health History ((a)(12)).

[209] See ''software developer, systems software''—*https://www.bls.gov/oes/2017/may/oes151133.htm.*

regarded their desirability as part of interoperable exchanges. The free text portion of the clinical notes was most often relayed by clinicians as the data they sought, but were often missing during electronic health information exchange. Similarly, the provenance of data was also referenced by stakeholders as a fundamental need to improve the trustworthiness and reliability of the data being exchanged.

We expect improvements to interoperable exchange of information and data provenance to significantly benefit providers and patients. For example, in 2018, among individuals who had viewed their online medical record within the past year (representing 30 percent nationally), about half indicated that clinical notes were included in their online medical record.[210] Additionally, seven percent of individuals who viewed their online medical record requested a correction of inaccurate information. Thus, enabling patients to have access to their clinical notes might assist in reducing medical coding errors.

Patient matching is a barrier to interoperability. In 2017, 36 percent of non-Federal acute care hospitals reported difficulty matching or identifying the correct patient between systems.[211] The data elements ''Previous Address,'' ''Phone Number,'' ''Phone Number Type,'' and ''Email Address'' were included in the USCDI v1 based on feedback from industry, for their usage in accurate patient matching.

However, we are not aware of an approach for quantifying these benefits and we welcomed comments on potential approaches to quantifying these benefits in the Proposed Rule.

Comments. We did not receive comments regarding an approach to quantify benefits. However, we did receive comment regarding estimation of the time and effort on behalf of health IT developers to update to the USCDI. Commenters stated that we have underestimated the number of hours necessary for health IT developers, suggesting that it is triple our estimates.

Response. We thank commenters for their input. We maintain the approach we proposed in the Proposed Rule in regard to our estimates for updating the USCDI. This final rule constrains ''provenance'' to only the scope of data for which the health IT developer is the owner/steward. Hence, the scope is fairly limited and therefore, we believe our estimates to be accurate. We note the removal of ''data export'' (§ 170.315(b)(6)) from the cost estimate in Table 6, in alignment with our final policy decisions and no longer updating the criterion to USCDI. We did, however, increase the hour per developer based on additional data elements included in this final rule.

(ii) Electronic Health Information Export

In this final rule, we adopted a modified version of the ''EHI export'' criterion in § 170.315(b)(10). Notably, we have defined and further constrained the criterion's scope of data for export as EHI, as defined in § 171.102, that can be stored at the time of certification by the product, of which the Health IT Module is a part. The final criterion provides a focused set of data from a scope perspective and clarifies what a product with a certified Health IT Module must be capable of exporting. The intent of this criterion aims to provide Health IT Module users the functionality to efficiently export or direct the export of EHI for a single patient or a patient population in a computable, electronic format.

(A) Costs To Develop and Maintain EHI Export Criterion

This section describes the estimated costs of the ''EHI export'' criterion. The cost estimates are based on the following assumptions:

- *Health IT developers will use the same labor costs and data models.* Table 8 shows the estimated labor costs per product for a health IT developer to develop and maintain the EHI export functionality. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs noted in Table 8.

- *A proxy is needed to project the number of 2015 Edition certified health IT products containing the ''EHI export'' criterion.* We estimated that 545 products from 458 developers will contain the ''EHI export'' criterion. To develop these estimates, we first identified a proxy for the number of health IT developers that may create a 2015 Edition certified health IT product containing the ''EHI export'' criterion. Our proxy is based on the number of 2014 Edition certified health IT products that are capable of recording patient data.[212] We based our estimates on these products because data must be captured to be exported under the adopted criterion. There were 710 products by 588 developers with at least one 2014 Edition product capable of recording patient data. We then multiplied these numbers by our certified health IT market consolidation estimates of −22.1 percent and −23.2 percent to project the number of 2015 developers and products, respectively.

- *Wages are determined using BLS estimates.* According to the May 2017 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $53.74.[213] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $107.

[210] Patel V & Johnson C. (May 2019). Trends in Individuals' Access and Use of Online Medical Records and Technology for Health Needs: 2017–2018. ONC Data Brief, no.48 Office of the National Coordinator for Health Information Technology: Washington DC.

[211] Pylypchuk Y., Johnson C., Henry J. & Ciricean D. (November 2018). Variation in Interoperability among U.S. Non-Federal Acute Care Hospitals in 2017. ONC Data Brief, no.42. Office of the National Coordinator for Health Information Technology: Washington DC.

[212] We defined ''products capable of recording patient data'' as any 2014 Edition product that was certified for at least one of the following criteria: Demographics ((a)(5)), Medication List ((a)(7)), Medication Allergy List ((a)(8)), Problem List ((a)(6)), and Family Health History ((a)(12)).

[213] *https://www.bls.gov/oes/2017/may/oes151133.htm.*

TABLE 8—ESTIMATED LABOR COSTS TO DEVELOP AND MAINTAIN THE EHI EXPORT CRITERION PER PRODUCT

Activity	Lower bound hours	Upper bound hours	Remarks
Task 1: Developing the Data Dictionary software capability to export EHI in a developer format (per product).	160	1,600	This is the effort to document all the data exported by the product for a single patient and for all patients. The lower bound assumes that the health IT developer already has a standard format in which they are exporting the data for either case (*e.g.,* C–CDA for single patient, CSV file or database dump for all data) and the effort is merely to publish it to the users. On the other hand, the upper bound reflects the case where the health IT has to develop the export capability de novo into their product and document the data output. This still assumes that the developer will be able to use the format of their choice.
Task 2: Updating the Data Dictionary and publishing the updated format (per product).	80	500	This is the maintenance cost to update the data dictionary published by the product to ensure that the data dictionary is compatible with newer releases of the product. The lower bound estimate assumes the effort when there are only minor changes to the formats of the data stored by the product. The upper bound estimate assumes the effort when the product makes substantial changes to the formats of the data.
Task 3: Updating the software that performs EHI Export (per product).	80	500	This is the maintenance cost to upgrade the software that would generate the EHI export files. The lower bound estimates the cost to maintain the software when there are only minor changes to the product, including updates to underlying software (*e.g.,* database versions, operating systems, etc.). The upper bound estimate accounts for substantial reworking of the export software program to export in new formats or based on substantial changes made to the underlying storage system.
Total Labor Hours	320	2,600	

TABLE 9—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO HEALTH IT DEVELOPERS TO PERFORM TASK 1 FOR THE EHI EXPORT CRITERION

[2016 Dollars]

Activity	Estimated labor hours lower bound	Developer salary	Projected products
Task 1	160 hours	$107 per hour	545 products
Example Calculation			
160 hours * $107 * 545 products = $9,330,400			

TABLE 10—TOTAL COST TO DEVELOP AND MAINTAIN THE EHI EXPORT CRITERION

[2017 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (545 products)	$9,330,400	$93,304,000
Task 2 (545 products)	4,665,200	29,157,500
Task 3 (545 products)	4,665,200	29,157,500
Total (545 products)	18,660,800	151,619,000

(B) Costs To Implement and Support the EHI Export Criterion

The cost estimates are based on the following assumptions:

• *Health care providers will use the same costs and data models.* Table 11 shows the estimated costs to implement and support the EHI Export criterion. The cost estimates used in this calculation were published by the Agency for Healthcare Research and Quality and were based on the average cost to implement an EHR for a clinical practice.[214] This publication was based on the implementation of an entire EHR system. We assume that all stakeholders impacted by this rule will already have a base EHR system implemented, therefore we discounted these estimates by a factor of 10 to better reflect the cost to implement an EHI Export module only. We did not have cost estimates for hospitals. Therefore, to estimate the cost for a hospital to implement an EHR system, we multiplied the estimate to

[214] Fleming, N., Impact of Health Information Technology on Primary Care Workflow and Financial Measures AHRQ Publication No. 11–0081–4–EF, October 2011 *https://digital.ahrq.gov/sites/default/files/docs/page/Fleming_SS_508_20111021_d.pdf.*

implement an EHR for a clinical practice by a factor of 10. We believe this will better reflect the increased magnitude and complexity of implementing and supporting a new health IT module in a hospital compared to a clinical practice. We recognize that costs health care providers incur will vary; our estimates in this section assume health care providers incur the costs noted in Table 11.

• *Hospitals and clinical practices that have participated in the CMS EHR Incentive Program will be impacted.* We estimate that 95,470 clinical practices [215] and 4,519 hospitals [216] will be impacted by our rule.

TABLE 11—ESTIMATED COST TO HOSPITALS AND CLINICAL PRACTICES TO IMPLEMENT AND SUPPORT THE EHI EXPORT CRITERION

[2017 Dollars]

Task	Entity type	Number of entities	Cost per entity		Remarks
			Lower bound	Upper bound	
Task 1: Implementation and Support.	Clinical Practices	95,470	$2,000	$4,000	This task would involve costs associated with staff support during implementation, workflow mapping and redesign, content development and customization, project management, and other technical deployment including networking.
	Hospitals	4,519	20,000	40,000	
Task 2: Staff Training	Clinical Practices	95,470	500	1,000	This task would involve staff training for implementation teams and staff end users.
	Hospitals	4,519	5,000	10,000	

TABLE 12—TOTAL COST TO IMPLEMENT AND SUPPORT THE EHI EXPORT CRITERION

[2017 Dollars]

Task		Lower bound	Upper bound
Task 1: Implementation and Support	Clinical Practices	$190,940,000	$381,880,000
	Hospitals	90,380,000	180,760,000
Task 2: Staff Training	Clinical Practices	47,735,000	95,470,000
	Hospitals	22,595,000	45,190,000
Total Cost		351,650,000	703,300,000

Based on the stated assumptions and costs outlined in Tables 8 and 10, the total estimated cost for health IT developers to develop products to the ''EHI export'' criterion will range from $18.7 million to $151.6 million. Assuming 458 health IT developers, there would be an average cost per health IT developer ranging from $40,744 to $331,045. We note that the development costs, which equal half of the total, would be a one-time cost and would not be perpetual. The total estimated cost for hospitals and clinical practices to implement and support the EHI Export will range from $351.7 million to $703.3 million. The midpoint of ranges stated is used as the primary estimate of costs.

(C) Benefits

Health care providers may choose to change their EHRs for a number of reasons. However, the steps and costs associated with switching one's EHR are complex. Market forces, such as health IT developers' business incentives, make it difficult and costly for EHR users to transfer system data from one developer to another. Data transfer costs vary depending on how contracts are structured.[217] Specifically, contracts might include high data-transfer fees or do not include conditions for data transfer. Providers may also pay fees for consultants or technical staff to help with the data-transfer process given differences in how data may be mapped from one developer to another. Hence, health care providers will experience benefits associated with the standardization proposed in the EHI export functionality.

Because of the EHI export functionality, providers will no longer incur the costs associated with mapping data from their health IT database into standard terms or exporting said data using a standardized format when switching EHRs. In our analysis, we calculated the benefits in terms of the reduced costs to providers as a result of our rule eliminating these two tasks. The benefit calculations below are based on the following assumptions:

• *On average, five percent of providers and hospitals switch their health IT annually.* Using CMS Medicare EHR Incentive Program data from years 2013–2016, we estimate the rate of providers (hospitals and eligible professionals) that changed their health IT developer. We believe that the EHI export functionality would help alleviate the burden of switching between health IT systems by increasing portability of EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part. Thus, the benefit calculations are based on assumptions regarding the number of clinical practices (n = 4,774) and hospitals (n = 226) that are projected to switch products in a year.

[215] This number was estimated based on the de-duplicated number of practices that had at least one clinician participate in the CMS Medicare Electronic Health Record Incentive Program.

[216] This estimate is the total number of eligible hospitals that ever participated in the CMS Medicare Electronic Health Record Incentive Program.

[217] Pratt, Mary, The True Cost of Switching EHRs, Medical Economics, May 30, 2018, Volume: 96 Issue: 10.

• *Health IT consultants*[218] *will use the same labor costs and data models.* Table 13 shows the estimated labor costs per product for a hospital or health care provider to hire a health IT consultant to perform data export of EHI, as defined in 45 CFR 171.102, without the EHI export functionality. We recognize that these costs will vary based on the size of the hospital or clinical practice.

• *Wages are determined using BLS estimates.* According to the May 2017 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $53.74.[219] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $107.

TABLE 13—COST PER PROVIDER TO PERFORM DATA EXPORT WITHOUT EHI EXPORT FUNCTIONALITY WHEN SWITCHING HEALTH IT PRODUCTS

[2017 Dollars]

Activity	Estimated cost per health IT switch (lower bound) (hours)	Estimated cost per health IT switch (upper bound) (hours)	Remarks
Task 1: Understanding and mapping the data in health IT database into standard terms.	320	3,200	The lower bound is an estimate for a small provider practice using the standard instance of a certified health IT product with no customization and use of nationally recognized content standards. The upper bound estimates a medium to large practice with substantial local customization of content.
Task 2: Exporting the data from the health IT into a format that can be subsequently used to import.	160	1,600	The lower bound assumes that the certified health IT product is capable of exporting most of the data into standard output format such as C–CDA. The upper bound estimates the case where a large amount of data is not easily exported by the certified health IT product and therefore substantial one-off software needs to be written to export the data into a custom (de novo) format developed for the transition.
Total Labor Hours	480	4,800	

Table 14 provides an example calculation for how we calculated our total costs presented in Table 15.

TABLE 14—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO PROVIDERS TO HIRE A HEALTH IT CONSULTANT TO PERFORM TASK 1 WITHOUT THE EHI EXPORT CRITERION

[2017 Dollars]

Activity	Estimated labor hours lower bound	Developer salary	Estimated annual number of health IT switches
Task 1	320 hours	$107 per hour	5,000 switches
Example Calculation: 320 hours * $107 * 5000 switches = $171,200,000.			

TABLE 15—TOTAL COST TO PROVIDERS TO PERFORM DATA EXPORT WITHOUT THE EHI EXPORT CRITERION WHEN SWITCHING HEALTH IT PRODUCTS

[2017 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1	$171,200,000	$1,712,000,000
Task 2	85,600,000	856,000,000
Total Cost Savings (5,000 switches)	256,800,000	2,568,000,000

[218] ''Health IT consultant'' refers to a technical expert that a hospital or provider will hire to migrate their data from a legacy system to a new EHR.

[219] *https://www.bls.gov/oes/2017/may/oes151133.htm.*

We multiplied the costs to switch health IT by the estimated number of hospitals and clinical practices affected. Thus the estimated annual benefit, in terms of cost savings to hospitals and clinical practices, would range from $256.8 million to $2.6 billion.

(iii) Application Programming Interfaces

The API requirements in this final rule reflect the full depth and scope of what we believe is necessary to implement the API Condition of Certification requirement described in section 4002 of the Cures Act. We have adopted new standards, new implementation specifications, a new certification criterion, and detailed Conditions and Maintenance of Certification requirements in §§ 170.213 and 170.215, 170.315, and 170.404, respectively. We also modified the Base EHR definition in § 170.201.

(A) Costs To Develop and Maintain Certified API Technology

This section describes the potential costs of the API certification criterion. The cost estimates below are based on the following assumptions:

- *Health IT developers will use labor costs and data models based on whether they have adopted aspects of the API certification criterion.* Tables 16 A and 16 B show the estimated labor costs per product for a health IT developer to develop and maintain an API. We recognize that health IT developer costs will vary based on whether they have already implemented aspects of the API certification criterion; including adopting the Fast Healthcare Interoperability Resources (FHIR®) API. To account for this variation, we have estimated two cost tables. Table 16 A reflects the range of costs incurred for new products or those developers that have not previously certified to the API certification criteria. Table 16 B shows the cost for developers that have already implemented the API criteria. We have assumed in our calculations that all health IT developers will incur costs noted in either Table 16 A or Table 16 B.
- *A proxy is needed to project the number of 2015 Edition certified health IT products containing the API certification criterion.* We estimated that 459 products from 394 developers will contain the API criterion. We used a proxy to determine the number of health IT developers that may develop an API for the certification to the 2015 Edition. There were 598 products and 506 developers with at least one 2014 Edition certified health IT product that could perform transitions of care. We then multiplied this number by our certified health IT market consolidation estimates of −22.1 percent and −23.2 percent to project the number of 2015 developers and products, respectively. Some developers and products are already leveraging aspects of the API certification criterion. This could reduce their cost to implement the criterion. To determine the number of developers and products applicable to cost Table 16 A or 16 B, we calculated the proportion of products and developers that have already certified to API certification criterion. We then applied this estimate to the projected number of 2015 Edition certified health IT products. Specifically, we estimate that 50 percent of products (230) and 55 percent of developers (217) will incur costs reflected in Table 16 A because they have no prior experience with certifying to the API criteria. We believe this estimate serves as a reasonable proxy for products' capability to send patient data and the cost of implementation. The API functionality required by the 2015 Edition achieves a similar end by allowing providers to retrieve patient data from secure data servers hosted by other developers, as well as providing patients access to their medical records through third-party applications connected to these same secure servers.
- *Wages are determined using BLS estimates.* According to the May 2017 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $53.74.[220]

TABLE 16 A—ESTIMATED LABOR HOURS TO DEVELOP AND MAINTAIN API—NEW PRODUCTS

Activity	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 1: Implementing security via SMART App Launch Framework IG (per product).	(1) New development to support OpenID Connect. (2) Implementation of the Smart Guide with support for refresh tokens and the core capabilities specified in the rule. (3) New development to respond to request for access token verification.	1000	1500	(1) Lower bound assumes health IT has already implemented security via SMART App Launch Framework IG and need to be updated to account for additional requirements in the rule including Support for additional ''core'' capabilities required by rule and Token Introspection. (2) Upper bound assumes new development for implementation of SMART App Launch Framework IG, and additional requirements in the rule including Token Introspection.
Task 2: Develop support for Fast Healthcare Interoperability Resources (FHIR®) API and associated IGs (per product).	(1) New development to support FHIR R4 (2) Implementation to the FHIR US Core IG.	2000	6000	(1) Lower bound assumes health IT already has developed FHIR DSTU2 2015 Edition for data classes that were specified in prior rule and only needs to be updated to R4 and new data classes specified in the rule (2) Upper bound assumes new development of FHIR API for all resources

[220] *https://www.bls.gov/oes/2017/may/oes151133.htm.*

TABLE 16 A—ESTIMATED LABOR HOURS TO DEVELOP AND MAINTAIN API—NEW PRODUCTS—Continued

Activity	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 3: Develop API for Population Level Services (per product). *Note: One-time cost* ..	(1) New development to support FHIR Bulk Data Access IG.	2000	4500	(1) Lower bound assumes health IT already has an existing API for population level services; and need to migrate to the standardized API specified in the rule. (2) Upper bound assumes new development of FHIR Bulk Data Access IG.
Task 4: Development of App registration Server and Portal (per developer).	(1) New registration server development (or updates to existing server) to support registration timeliness and publication of FHIR endpoints. (2) Development of portal and managing the application registration system.	1000	2500	(1) Lower bound assumes that the developer already has existing application registration infrastructure in place, and only needs to update it to support the API Maintenance of Certification requirements. (2) Upper bound is new development of an application registration service and portal.
Task 5: Update Application Registration Server and Portal (per developer).	(1) Yearly updates and maintenance to keep the portal running. We do not anticipate any major changes to the standard and will be primarily driven by usage and developer interest.	400	1300	(1) Lower bound estimates hours to keep it running with junior staff. (2) Upper bound estimates small updates.
Task 6: Develop support for patients to revoke access to authorized app (per product).. *Note: One-time cost* ..	(1) Develop capability to identify apps authorized by registered users. (2) Provide capability to remove access at patient direction.	250	1500	(1) Lower bound assumes that the developer already has a portal used by patients for managing their preferences and new development will be needed to provide patients with ability to view and revoke access to their authorized apps. (2) Upper bound assumes that developer's current capability of managing registered patients need to be significantly enhanced to support enabling patients to revoke access to the authorized apps.
Other costs (50% per product, 50% per developer) (2017 Dollars). *Note: One-time cost* ..	(1) Server costs for application registration, sandbox, bulk data storage, and costs associated with making documentation publicly available. (2) Software costs (*e.g.,* databases, application servers, portal technology).	$7,500	$30,000	(1) Estimated as monetized costs and not as hours; most of the costs would be one-time procurement costs plus yearly maintenance.

TABLE 16 B—ESTIMATED LABOR HOURS TO DEVELOP AND MAINTAIN API—CURRENTLY CERTIFIED PRODUCTS

Activity	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 1: Implementing security via SMART App Launch Framework IG (per product).	(1) Development to support OpenID Connect. (2) Implementation of the Smart Guide with support for refresh tokens and the core capabilities specified in the rule. (3) Development to respond to request for access token verification.	800	1000	(1) Lower bound assumes health IT has already implemented security via SMART App Launch Framework IG and need to be updated to account for additional requirements in the rule. (2) Upper bound assumes additional development for implementation of SMART App Launch Framework IG, and additional requirements in the rule.
Task 2: Develop support for Fast Healthcare Interoperability Resources (FHIR®) API and associated IGs (per product).	(1) Development to support FHIR R4 ..... (2) Implementation to the FHIR US Core IG.	1600	2000	(1) Lower bound assumes health IT already has developed FHIR R4 for data classes that were specified in prior rule and only needs to be updated to new data classes specified in the rule. (2) Upper bound assumes health IT was originally developed for FHIR DSTU2 and needs additional development of FHIR API to support upgrading to FHIR R4 and new data classes.

TABLE 16 B—ESTIMATED LABOR HOURS TO DEVELOP AND MAINTAIN API—CURRENTLY CERTIFIED PRODUCTS—Continued

Activity	Details	Estimated labor hours		Remarks
		Lower bound	Upper bound	
Task 3: Develop API for Population Level Services (per product). *Note: One-time cost* ..	(1) New development to support FHIR Bulk Data Access IG.	2000	4500	(1) Lower bound assumes health IT already has an existing API for population level services; and need to migrate to the standardized API specified in the rule. (2) Upper bound assumes new development of FHIR Bulk Data Access IG.
Task 4: Development of App registration Server and Portal (per developer).	(1) New registration server development (or updates to existing server) to support registration timeliness and publication of FHIR endpoints. (2) Development of portal and managing the application registration system.	800	1000	(1) Lower bound assumes that the developer already has existing application registration infrastructure in place, and only needs to update it to support the API Maintenance of Certification requirements. (2) Upper bound assumes additional development to support requirements in rule.
Task 5: Update Application Registration Server and Portal (per developer).	(1) Yearly updates and maintenance to keep the portal running. We do not anticipate any major changes to the standard and will be primarily driven by usage and developer interest.	320	400	(1) Lower bound estimates hours to keep it running with junior staff. (2) Upper bound estimates small updates.
Task 6: Develop support for patients to revoke access to authorized app (per product). *Note: One-time cost* ..	(1) Develop capability to identify apps authorized by registered users. (2) Provide capability to remove access at patient direction.	150	250	(1) Lower bound assumes the developer provides this functionality based on 2015 ONC Edition and needs to perform minimum verification. (2) Upper bound assumes that the developer already has a portal used by patients for managing their preferences and new development will be needed to provide patients with ability to view and revoke access to their authorized apps.
Other costs (50% per product, 50% per developer) (2017 Dollars). *Note: One-time cost* ..	(1) Server costs for application registration, sandbox, bulk data storage, and costs associated with making documentation publicly available. (2) Software costs (*e.g.,* databases, application servers, portal technology).	$6000	$7,500	(1) Estimated as monetized costs and not as hours; most of the costs would be one-time procurement costs plus yearly maintenance.

Table 17 provides an example calculation for how we calculated our total costs presented in Tables 18 A and 18 B.

TABLE 17—EXAMPLE CALCULATION FOR THE LOWER BOUND ESTIMATED COST TO NEW PRODUCTS TO PERFORM TASK 1 IN TABLE 13 A TO DEVELOP API

[2017 Dollars]

Activity	Estimated labor hours	Developer salary	Projected products
	Lower bound		
Task 1	1,000 hours	$107 per hour	230 products.
Example Calculation: 1,000 hours * $107 * 230 products = $24,610,000.			

TABLE 18 A—TOTAL COST TO DEVELOP AND MAINTAIN API—NEW PRODUCTS

[2017 Dollars]

Activity	Estimated lost	
	Lower bound	Upper bound
Task 1 (230 products)	$24,556,500	$36,834,750
Task 2 (230 products)	49,113,000	147,339,000
Task 3 (230 products)	49,113,000	110,504,250

TABLE 18 A—TOTAL COST TO DEVELOP AND MAINTAIN API—NEW PRODUCTS—Continued

[2017 Dollars]

Activity	Estimated lost	
	Lower bound	Upper bound
Task 4 (217 developers)	23,186,900	57,967,250
Task 5 (217 developers)	9,274,760	30,142,970
Task 6 (230 products)	6,152,500	36,915,000
Other Costs (230 products)	860,625	3,442,500
Other Costs (217 developers)	812,625	3,250,500
Total (230 products and 217 developers)	163,069,910	426,396,220

TABLE 18 B—TOTAL COST TO DEVELOP AND MAINTAIN API—CURRENTLY CERTIFIED PRODUCTS

[2017 Dollars]

Activity	Estimated cost	
	Lower bound	Upper bound
Task 1 (229 products)	$19,645,200	$24,556,500
Task 2 (229 products)	39,290,400	49,113,000
Task 3 (229 products)	49,113,000	110,504,250
Task 4 (177 developers)	15,176,880	18,971,100
Task 5 (177 developers)	6,070,752	7,588,440
Task 6 (229 products)	3,675,450	6,125,750
Other Costs (229 developers)	688,500	860,625
Other Costs (177 products)	531,900	664,875
Total (229 products and 177 developers)	134,192,082	218,384,540

We note that we have adopted in § 170.404(b)(3) a specific requirement that an API Technology Supplier must support the publication of Service Base URLs for all of its customers that are centrally managed by the Certified API Developer, and make such information publicly available (in a computable format) at no charge. Thus, we are placing the responsibility of publishing the URLs on health IT developers and those costs are captured in the registration portal cost estimation in this RIA.

Based on the stated assumptions and costs outlined in Tables 16 A and 16 B, the total estimated costs for health IT developers to develop and maintain a product to the API criterion would range from $297.3 million to $644.8 million with an average cost per developer ranging from $0.75 million to $1.64 million. We note that the ''other costs'' and costs associated with tasks 3 and 6, which account for $110.9 million to $272.3 million of this total, are one-time costs and are not perpetual.

(B) Optional Cost To Acquire and Use Applications That Interact With Certified API Technology

We believe the API certification criterion and associated Condition and Maintenance of Certification requirements finalized in this rule will create an environment that promotes innovation for software developers to connect new tools and services that create efficiencies for health care providers throughout their course of care delivery. Software applications that connect to APIs is an emerging market that we believe will be further enhanced by the standards, transparency, and pro-competitive requirements finalized in this rule. As of October 25, 2018, researchers identified nearly 300 software applications being marketed on EHR vendors' app stores. The majority of these applications are designed for health care providers to help support use cases for population health analytics, clinical decision support, patient education, as well as to conduct administrative and financial tasks.[221]

Although not required under this rule, this section describes the potential costs of health care providers to acquire and use new software applications that interact with certified API technology. The cost estimates are based on the following assumptions:

- *Health care providers will use the same costs and data models.* Table 19 shows the estimated costs to acquire and use software applications that interact with certified API technology. We recognize that costs health care providers incur will vary based on several factors including, but not limited to, size of the health care entity, application usage, and complexity of deployment and maintenance. However, our estimates in this section assume health care providers incur the costs noted in Table 19.
- *Hospitals and clinical practices that have participated in the CMS EHR Incentive Program will be impacted.* We estimate that 95,470 clinical practices[222] and 4,519 hospitals[223] will be impacted by our rule.

[221] Dullabh P, Hovey L, Heaney-Huls K, Rajendron N, Wright A, Sittig D. Application Programming Interfaces in Health Care: Findings from a Current-State Sociotechnical Assessment. Applied Clinical Informatics. 2020; 11(01): 059–069.

[222] This number was estimated based on the de-duplicated number of practices that had at least one clinician participate in the CMS Medicare Electronic Health Record Incentive Program.

[223] This estimate is the total number of eligible hospitals that ever participated in the CMS Medicare Electronic Health Record Incentive Program.

TABLE 19—ESTIMATED COST TO HOSPITALS AND CLINICAL PRACTICES TO ACQUIRE AND USE SOFTWARE APPLICATIONS THAT ENGAGE WITH CERTIFIED API TECHNOLOGY

[2017 Dollars]

Entity type	Number of entities	Cost per entity		Total cost	
		Lower bound	Upper bound	Lower bound	Upper bound
Clinical Practices	95,470	$1,000	$5,000	$95,470,000	$477,350,000
Hospitals	4,519	10,000	100,000	45,190,000	451,900,000
Total	.....	.....	.....	140,660,000	929,250,000

The total cost to health care providers to acquire and use software applications that engage with certified API technology would range from $140.6 million to $929.3 million. The midpoint of ranges stated is used as the primary estimate of costs.

(C) Benefits

The Medicare Access and CHIP Reauthorization Act (MACRA), (Pub. L. 114–10), tasks ONC with measuring interoperability in the health IT industry.[224] The measurement concepts developed include a multi-part approach analyzing not only adoption of health IT functionalities supporting information exchange but the downstream impact of these technologies on data completeness, data integration, and supports for core functions of patient care. The benefits of our API proposal are similarly multifaceted.

Our API proposal will increase interoperability by ensuring that more data is available and shared between EHR users. The proposal will also make data more widely available to software developers outside of those specializing in EHR development. As a result, this data will lead to greater innovation in the app market resulting in new technologies for health care providers and patients alike. In the analysis, we quantify benefits in the following three areas: First, provider time saved as a result of new efficiencies in care delivery due to new technologies, such as provider facing apps. Second, the effects of interoperability on cost-savings associated with reductions in duplicate lab tests, readmissions, emergency room (ER) visits, and adverse drug events. We focused on these outcomes for two reasons: Evidence in literature indicates that health information exchange impacts the chosen measures; and cost of care associated with these measures is high and the impact of health information exchange is likely to result in significant benefits in the form of a cost reduction.[225] Finally, we quantify an increase in the number of individuals with access to their health information through a mechanism of their choice such as apps.

The benefit calculations are based on the following assumptions:

- *Benefits noted in academic literature are assumed accurate.* Estimates of the benefits are based on estimates obtained from peer reviewed academic literature. ONC reviewed academic articles for validity; however, models were not replicated.
- *Hospitals and eligible professionals that have participated in the CMS EHR Incentive Programs will be impacted:* Estimates assume that 439,187 health care providers and/or 4,519 hospitals would be affected by this regulatory action.

(D) Benefits: Provider Time Saved as a Result of New Efficiencies in Care Delivery Due to the Optional Purchase of New Technologies, Such as Provider Facing Apps

Improvements in technology result in benefits for consumers and producers through increased production efficiencies (Stoneman 2018).[226] The introduction of EHRs into the health care industry is an example of this. Sinsky (2016) found physicians spend 27 percent of their total time on direct clinical face time with patients, and 49.2 percent of their time on EHR and desk work.[227] Outside of office hours, physicians spend another one to two hours of personal time each night doing additional computer and other clerical work. Despite the number of hours providers spend in their EHR, there is evidence that the introduction of EHRs is associated with time saved. Adler-Milstein (2013) found that EHR use compared to non-EHR use resulted in a 5.3 percent increase in work relative value units per clinician work day.[228]

Improved efficiencies are not limited to the installation of an EHR. Providers also benefit from the use of emerging technologies. Amusan (2008) found that EHR and computerized provider order entry (CPOE) implementation was associated with 3.69 minutes of time saved five months post implementation.[229] Similarly, Helmons (2015) found that the impact of suppressing clinically irrelevant alerts and adding clinical-decision support to EHRs saved providers about two percent of their time.

To measure the benefits of the API provision on providers' time as a result of new technologies, we examined the literature on the impact of IT on productivity across various industries. As explained in Bartel (2007), improvements in IT could affect productivity through multiple mechanisms that are not necessarily associated with the underlying intention of that technology.[230] When examining the effect of IT in manufacturing, researchers found that adoption of IT affected production plants' composition of products, reduced time of production processes, and increased hiring of skilled workers. We adopt the same logic here. Specifically, we assume that the impact of the data made available under our API provisions will not be

[224] Health IT Buzz Blog, *Measuring Interoperability: Listening and Learning, https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/interoperability-electronic-health-and-medical-records/measuring-interoperability-listening-learning/.*

[225] Analyzing the Public Benefit Attributable to Interoperable Health Information Exchange *https://aspe.hhs.gov/pdf-report/analyzing-public-benefit-attributable-interoperable-health-information-exchange.*

[226] Stoneman P, Bartoloni E., Baussola M. The Microeconomics of Product Innovation. Oxford, United Kingdom: Oxford University Press, 2018.

[227] Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialtie*s, Ann Intern Med. (Dec. 6, 2016), at 753–60.

[228] Julia Adler-Milstein and Robert S. Huckman, The Impact of Electronic Health Record Use on Physician Productivity, Am J Manag Care (Nov. 19, 2013).

[229] Amusan, Tongen, Speedie, and Mellin, A time-motion study to evaluate the impact of EMR and CPOE implementation on physician efficiency, J. Healthcare Inf. Manag. (Fall 2008), at 31–7.

[230] Bartel, Ann & Ichniowski, Casey & Shaw, Kathryn. (2007). How Does Information Technology Affect Productivity? Plant-Level Comparisons of Product Innovation, Process Improvement, and Worker Skills. The Quarterly Journal of Economics. 122. 1721–1758. 10.1162/qjec.2007.122.4.1721.

through a single mechanism, such as an EHR, but will have multiple spillover effects. For example, data made available through an API could be used by a software developer to create tools to improve patient scheduling and billing processes. Use of this tool could result in improvements in the providers' workflow. Thus, is important to quantify the impacts of data made available through APIs on the future health IT market.

Table 20 provides a summary of the results of the literature review used to quantify this benefit.

TABLE 20—FINDINGS FROM LITERATURE ON THE IMPACT OF INFORMATION TECHNOLOGY ON PRODUCTIVITY

Study	Description	Findings: (%)
Bartel et al (2007)	Identify impact in improvements in information technology on production time of valve manufacturing. IT is defined as adoption of separated information system that enable various automations.	4–8
Lee et al (2013)	Identified impact of IT capital on hospital productivity where IT capital is defined as hospital expenditure on IT.	3–6
Shao and Lin (2002)	Identifies impact of IT expense on productivity of fortune 500 firms	2–7
Adler-Milstein et al (2013)	Identifies the impact of the introduction of the EHR on providers' time compared to non-EHR users.	5
Helmons et al (2015)	Identifies impact of suppressing clinically irrelevant alerts and adding clinical-decision support to EHRs on time saved.	2
Wagholikar KB, et al (2015)	Identifies impact of clinical-decision support on time saved among primary care providers	1

Sources:

[a] Jinhyung Lee Jeffrey S. McCullough Robert J. Town. The impact of health information technology on hospital productivity. The RAND Journal of Economics 44(3):545.

[b] Shao, W. Lin, Technical efficiency analysis of information technology investments: a two-stage empirical investigation, Information and Management 39, 2002, pp. 391–401.

[c] Adler-Milstein, J. and Huckman, R, The Impact of Electronic Health Record Use on Physician Productivity, AM J Manage Care, Nov. 19, 2013.

[d] Helmons PJ1, Suijkerbuijk BO2, Nannan Panday PV3, Kosterink JG4. Drug-drug interaction checking assisted by clinical decision support: a return on investment analysis. J Am Med Inform Assoc. 2015 Jul; 22(4):764–72. doi: 10.1093/jamia/ocu010. Epub 2015 Feb 10.

[e] Wagholikar KB1, Hankey RA2, Decker LK2, Cha SS2, Greenes RA3, Liu H2, Chaudhry R2. Evaluation of the effect of decision support on the efficiency of primary care providers in the outpatient practice. J Prim Care Community Health. 2015 Jan;6(1):54–60. doi: 10.1177/2150131914546325. Epub 2014 Aug 25.

As illustrated in the Table 20, the incremental effects of improvements in IT on productivity range from one percent to eight percent. Based on these findings, we assume the impact of the API provision on providers' time ranges between one percent and five percent. The lower bound estimate of one percent assumes that, at a minimum, providers will use one new app created as a result of the data made available under the API provision. We assume that this app will save providers time equivalent to the introduction of clinical decision support tools found in Wagholikar (2015). The upper bound estimate of five percent assume that, at a maximum, providers will use multiple apps created such that the combination will result in an increase in productivity. Furthermore, we assume that the API provision will affect only providers with certified EHRs and those that participated in the CMS EHR Incentive Program (439,187). Given that an average provider spends six hours with an EHR per day,[231] earns $97.85 per hour, and works 260 days per year, physicians' time saved attributed to API technology range from $670 million to $3.4 billion per year.

(E) Benefits: Reduced Costs Associated With the Impact of Interoperability on Health Outcomes

To identify the impact of the API proposal on interoperability and therefore identified health outcomes, we used regression analysis. Specifically, we estimated linear probability models that identified the impact of 2014 Edition certified EHR on hospitals' interoperability (whether a hospital sends, receives, finds, and integrates summary of care records). Using data from the American Hospital Association (AHA)[232] from years 2014 to 2015 in the model, we controlled for hospital size, profit status, participation in a health information organization, and state and year fixed effects. The marginal effect of using a 2014 Edition certified health IT equated to a five percent increase in interoperability. This is an upper bound estimate. For the purpose of this analysis, we assume that one to four percentage points would be a reasonable range for API's marginal impact on interoperability.

As noted previously, there might be shared benefits across certain provisions, and we have taken steps to ensure that the benefits attributed to each provision are unique to the specific provision. We assumed that the collective impact of real world testing and API proposals on interoperability would not exceed the impact of 2014 Edition certified health IT (estimated at five percent). We distributed the five percent benefit across our real world testing and API proposals at (0.1–1 percent) to (1–4 percent) respectively. Moreover, the number of providers impacted is specific to each provision. Thus, to finalize our calculations of the reduced costs related to reductions in duplicate lab tests, readmissions, emergency room (ER) visits, and adverse drug events due to increased interoperability, we leveraged evidence from the literature that found an association between providers' rates of interoperability and applied the estimated marginal effect of each proposal on interoperability. Given data limitations, we believe this approach allows us to estimate the benefits of our final rule without double counting the impact each provision might have on interoperability.

[231] Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties*, Ann Intern Med. (Dec. 6, 2016), at 753–60.

[232] American Hospital Association Health IT Supplement Survey, *http://www.ahadata.com/aha-healthcare-database/*.

TABLE 21—BENEFIT OF API ON HEALTH CARE OUTCOMES
[2017 dollars]

Benefit type	Number affected	Overall interop impact (marginal effect)	Impact of API		Total cost	Percentage of total cost impacted	Total benefit[a]	
			Min	Max			Min	Max
Duplicate testing	439,187 providers.	0.09[b]	0.01	0.04	$200 billion[c]	100	$185 million per year.	$742 million per year.
Avoidable hospitalizations and readmissions	4,519 hospitals	0.09[b]	0.01	0.04	$41 billion[d]	100	$38 million per year.	$152 million per year.
ER visits	131 million visits[e].	0.03[b]	0.01	0.04	$1,233 per ER visit.	100	$50 million per year.	$200 million per year.
Adverse drug events	20 of events affected.	22[f]	0.01	0.04	$30 billion[g]	20	$14 million per year.	$54 million per year.

[a] Total benefit is a product of *total cost, percent of total cost impacted, overall impact of interoperability, and impact of API, adjusted for inflation (1.03).*
[b] Stephen E. Ross, Tiffany A. Radcliff, William G. Leblanc, L. Miriam Dickinson, Anne M. Libby, and Donald E. Nease Jr., Effects of health information exchange adoption on ambulatory testing rates, J. Am. Med. Inform. Assoc. (2013), at 1137–1142; Bridget A. Stewart, Susan Fernandes, Elizabeth Rodriguez-Huertas, and Michael Landzberg, A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients, J. of the Am. Med. Informatics Assoc. (2010), at 341–344; Sezgin Ayabakan, Indranil R. Bardhan, Zhiqiang (Eric) Zheng, and Kirk Kirksey Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals, MIS Quarterly (Jan. 1, 2017); Eric J. Lammers, Julia Adler-Milstein, and Keith E. Kocher, Does health information exchange reduce redundant imaging? Evidence from emergency departments, Med Care (Mar. 2014), at 227–34.
[c] National Academy of Medicine. (2016), *http://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html.*
[d] Agency for Healthcare Research and Quality (AHRQ) Statistical Brief #199 (Dec. 2015), https://www.hcup-us.ahrq.gov/reports/statbriefs/sb199-Readmissions-Payer-Age.pdf; AHRQ Statistical Brief #72, Nationwide Frequency and Costs of Potentially Preventable Hospitalizations (Apr. 2009), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb72.pdf.*
[e] National Center for Health Statistics (NCHS) Data Brief No. 252 (June 2016), *https://www.cdc.gov/nchs/data/databriefs/db252.pdf*; Nolan Caldwell, Tanja Srebotnjak, Tiffany Wang, and Renee Hsia, ''How Much Will I Get Charged for This?'' Patient Charges for Top Ten Diagnoses in the Emergency Department (2013), *https://doi.org/10.1371/journal.pone.0055491.*
[f] M.F. Furukawa, W.D. Spector, M.R. Limcangco, and W.E. Encinosa, Meaningful use of health information technology and declines in in-hospital adverse drug events, J. of the Am. Med. Informatics Assoc. (2017).
[g] Janet Sultana, Paola Cutroneo, and Gianluca Trifirò, *Clinical and economic burden of adverse drug reactions.*

Based on this analysis, the benefits of the API provision on reduced costs on health outcomes range from $287 million to $1.1 billion.

(F) Benefits: Increase in Percent of Individuals With Access to Their Health Information

This provision will also provide individuals with better access to their data. APIs make it easier for patients to transmit data to smartphone health applications. According to the Health Information National Trends Survey,[233] nearly 20 percent of Americans were offered access and viewed their online medical record using smartphone health applications in 2019. The proportion of individuals accessing their online medical records using smartphone health applications is expected to grow as APIs become more widespread. This will result in cost savings to patients. Specifically, patients who use new applications to access copies of their medical record instead of contacting their provider will have cost savings.

Under the HIPAA Privacy Rule, individuals have the right to access their Protected Health Information (PHI) (45 CFR 164.524), and 45 CFR 164.524(c)(4) sets forth implementation specifications for fees that covered entities may charge individuals for access to their PHI. Under 45 CFR 164.524(c)(4), a covered entity may impose a reasonable, cost-based fee (consistent with the conditions in § 164.524(c)(4)(i) through (iv)). For purposes of this analysis, we assume covered entities can charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and any applicable postage). The API Condition and Maintenance of Certification requirements finalized in § 170.404 do not allow for a ''Certified API Developer'' (as defined in § 170.404(c)) to charge patients for connecting to an API to access, exchange, or use their EHI. A Certified API Developer is permitted to charge fees to an API Information Source related to the use of certified API technology. The fees must be limited to the recovery of incremental costs reasonably incurred by the Certified API Developer when it hosts certified API technology on behalf of the API Information Source (§ 170.404). Thus, patients would ultimately see cost savings by accessing their online medical record using a smartphone health application instead of contacting their provider for an electronic copy.

To identify the potential cost savings this rule will have for patients, we used data from the Health Information National Trends Survey to estimate the proportion of individuals who reported having to bring a test result to a doctor's appointment at least once in the past year. In 2018, approximately 81 percent of Americans reported that they saw a doctor in the past year and about 19 percent of these individuals reporting having to bring a test result to an appointment. Therefore, using Census data from December 31, 2017, we conducted the following calculation (total U.S. population 325.9M) * (81 percent of individuals saw a doctor in the past year) * (19 percent of individuals who had to bring a test result to an appointment). This resulted in an estimate of 50.2 million Americans who bring test results to a doctor's appointment each year. We recognize that not all of these individuals will have the capability to access an online medical record using a smartphone health application. Therefore, we discounted this estimate based on the proportion of individuals who currently access their online medical records using a smartphone health applications (14 percent), as our lower bound. Our upper bound is the proportion of individuals who reported being offered access to an online medical record by a health care provider or insurer (58 percent). These calculations are in Table 22.

[233] These estimates were derived from Health Information National Trends Survey 5, Cycle 1 (2017).

TABLE 22—BENEFIT OF API ON PATIENTS HAVING ACCESS TO THEIR HEALTH INFORMATION

[2017 Dollars]

Benefit type	Number affected	Proportion of individuals impacted		Total cost savings	Total benefit	
		Min	Max		Min	Max
Cost savings to patients for requesting an electronic copy of their medical record.	50,156,010[a] patients.	14%[b]	58%[b]	$6.50[c] per patient	$45.8 million per year.	$189.8 million per year.

[a] This represents the number of individuals who had to bring a medical test result to an appointment with a health care provider in the past year. Calculation: US Population on December 31, 2017 (325.9M)*81 percent who saw a doctor in the past year*19 percent who had to bring a test result to an appointment. Sources: (1) *https://www.census.gov/popclock/;* (2) *https://dashboard.healthit.gov/quickstats/pages/consumers-gaps-in-information-exchange.php.*

[b] Lower bound represents the proportion of individuals nationwide who were offered access to their online medical record by a health care provider or insurer. Upper bound represents the proportion of individuals nationwide who were offered access and subsequently viewed their online medical record using a smartphone health app. Source: Johnson C. & Patel V. The Current State of Patients' Access and Using their Electronic Health Information. Presented at the ONC Annual Meeting on January 27, 2020.

[c] We assume that providers charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage.

Based on the above calculations, we estimated the annual benefit to health care providers for the use of these API capabilities would, on average, range from $6.7 million to $140 million. We estimated the annual benefit due to improved health outcomes would, on average, range from $287 million to $1.1 billion. We estimated the annual benefit to patients having access to their online medical record would, on average, range from $45.8 million and $189.8 million. Therefore, we estimated the total annual benefit of APIs, on average, to range from $0.34 billion to $1.43 billion.

Comments. We did not receive comments specific to our approach to estimating the benefits of API support.

Response. We have maintained our overall approach for the costs and benefits associated with the API provisions of this rule. As discussed in section IV.B.7 of this final rule preamble, we have added a new requirement in the finalized § 170.315(g)(10) that gives patients the capability to revoke access to an authorized application. Cost estimates for this new requirement were added to cost tables 16 A and 16 B as task six. The task of meeting this additional finalized requirement increased the overall cost estimate for the API provisions by $9.8 million to $43 million. Due to this increase in cost, we re-evaluated our benefits estimates associated with increasing patients' access to their health information. In the Proposed Rule, we qualitatively discussed benefits of patients having increased access to their health information. However, upon further consideration, and additional data sources, we were able to estimate cost savings to patients for requesting electronic copies of their medical record. These estimates are reflected in Table 22. We provided additional rationale to substantiate our approach and we updated estimates to 2017 dollars.

(iv) New Privacy and Security Certification Criteria

As specified in section IV.C.3 of this final rule, we have adopted two new privacy and security transparency attestation certification criteria in § 170.315(d)(12) and (13) that are part of the 2015 Edition privacy and security certification framework. The criteria will serve to identify whether certified health IT supports encrypting authentication credentials and/or multi-factor authentication (MFA). They do not require new development or implementation to take place in order to be met. However, certification to these criteria will provide increased transparency and, perhaps, motivate the small percentage of health IT developers that do neither to encrypt authentication credentials and/or support multi-factor authentication, which will help prevent exposure to unauthorized persons/entities.

(A) Costs

Comments. We did not receive any comment specific to any method we could use to quantify the costs of the new privacy and security certification criteria, encrypt authentication credentials (§ 170.315(d)(12)) and multi-factor authentication (MFA) (§ 170.315 (d)(13)), and requiring health IT developers to assess their Health IT Modules' capabilities and attest ''yes'' or ''no'' to the certification criteria.

Response. We have maintained our estimates of the costs of this provision in the final rule.

(B) Benefits

As stated previously, we have not required health IT developers to encrypt authentication credentials or support multi-factor authentication (MFA). Instead, we have required that they attest to whether or not they support the certification criteria. By requiring an attestation, we are promoting transparency, which might motivate some health IT developers that do not currently encrypt authentication credentials or support MFA to do so. If health IT developers are motivated by these criteria and ultimately do encrypt authentication credentials and/or support MFA, we acknowledge that there would be costs to do so; however, we assume that the benefits will substantially exceed the costs. Such encryption and adopting MFA would reduce the likelihood that authentication credentials would be compromised and would eliminate an unnecessary use of IT resources. Encrypting authentication credentials and adopting MFA could directly reduce providers' operating and support costs, which will reduce their administrative and financial burden. Encrypting authentication credentials will also help decrease costs and burdens by reducing the number of password resets due to possible phishing or other vulnerabilities.

According to Verizon's 2017 Data Breach Investigations Report, 81 percent of hacking-related breaches leveraged either stolen and/or weak passwords.[234] The Verizon report encourages customers to vary their passwords and use two-factor authentication. Also, National Institute of Standards and Technology (NIST) Special Publication 800–63B: Digital Identity Guidelines, *Authentication and Lifecycle*

[234] *https://enterprise.verizon.com/resources/reports/2017_dbir.pdf.*

Management,[235] recommends the use of, and provides the requirements for multi-factor authenticators.

Based on these reports and other anecdotal evidence, we believe encrypting authentication credentials and supporting MFA are established best practices among industry developers, including health IT developers. As described above, in this final rule, we required health IT developers to attest to whether they encrypt authentication credentials. We do not have access to published literature that details how health IT developers are already encrypting authentication credentials and supporting MFA industry-wide, but we believe most health IT developers, or around 80 percent, are taking such actions. We assume that building this functionality is in the future project plans for the remaining 20 percent because, as noted previously, adopting these capabilities is an industry best practice. Health IT developers that have not yet adopted these capabilities are likely already making financial investments to get up to speed with industry standards. We believe the adoption of these criteria will motivate these health IT developers to speed their implementation process, but we have not attributed a monetary estimate to this potential benefit because our rule is not a direct cause of health IT developers adopting these capabilities. We anticipate that when we release this final rule, many more, or perhaps all, health IT developers will likely already be encrypting authentication credentials and supporting MFA. We welcomed comments on this expectation and any means or methods we could use to quantify these benefits.

Comments. We did not receive any comment specific to any means or methods we could use to quantify the costs and benefits of having the new privacy and security transparency attestation certification criteria, encrypt authentication credentials (§ 170.315(d)(12)) and multi-factor authentication (MFA) (§ 170.315(d)(13)), and requiring health IT developers to assess their Health IT Modules' capabilities and attest ''yes'' or ''no'' to the certification criteria.

Response. We maintain our estimates of the costs and benefits of this provision in the final rule. We also continue to believe that the adoption of these criteria will motivate these health IT developers to speed their implementation process.

(v) Security Tags—Summary of Care—Send and Security Tags—Summary of Care—Receive

In this final rule, we updated the 2015 Edition Data Segmentation for Privacy (DS4P) certification criteria in § 170.315(b)(7) and (8) to support a more granular approach to privacy tagging data for health information exchange. We also renamed the criteria to reduce confusion and better align with the criteria, ''Security tags—Summary of Care—send'' and ''Security tags—Summary of Care—receive.'' The criteria will remain based on the C–CDA and the HL7 DS4P standard. These criteria will include capabilities for applying the DS4P standard at the document, section, and entry level. In the Proposed Rule, we proposed to adopt a third 2015 Edition DS4P certification criterion, ''consent management for APIs'' (§ 170.315(g)(11)), that requires health IT to be capable of responding to requests for data through an API in accordance with the Consent Implementation Guide, which we did not finalize.

(A) Costs

We anticipate these updated criteria will result in up-front costs to health IT developers as health IT would be required to support all three levels—document, section, and entry—as specified in the current DS4P standard. However, we note that these criteria are not being required in any program at this time. As of the beginning of the fourth quarter of the 2019 calendar year, only about 30 products (products with multiple certified versions were counted once) were certified to the current 2015 Edition DS4P certification criteria. We estimated that 10 to 15 products will implement the new DS4P criteria. Developers may need to perform fairly extensive health IT upgrades to support the more complex and granular data tagging requirements under these criteria. We anticipate developers will need approximately 1,500 to 2,500 hours to upgrade databases and/or other backend infrastructure to appropriately apply security tags to data and/or develop access control capabilities. Moreover, developers will likely incur costs to upgrade health IT to generate a security-labeled C–CDA conforming to the DS4P standard. We estimated developers will need 400 to 600 hours per criterion to make these upgrades on systems that had previously certified to the document-level DS4P criteria, or 720 to 1220 hours per criterion for systems that are implementing these criteria for the first time. We believe this work would be performed by a ''Software Developer.'' According to the May 2017 BLS occupational employment statistics, the mean hourly wage for software developer is $53.74. As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $107. Therefore, we estimated the total cost to developers could range from $2,910,400 to $6,933,600. We note that this would be a one-time cost. The midpoint of ranges stated is used as the primary estimate of costs.

Additionally, we proposed that the health IT support the capability to respond to requests for patient consent information through an API compatible with FHIR Release 3. However, we did not finalize that proposal. Therefore, we did not include an estimate in this final rule.

We have estimated costs using the following assumptions:

- For the two Security tags—Summary of Care criteria, we anticipate developers will need approximately 1,500 to 2,500 hours to upgrade databases and/or other backend infrastructure to appropriately apply security tags to data and/or develop access control capabilities. We expect that this would be a one-time cost.
- According to the May 2017 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $53.74.

Our cost estimates are explained in the Table 23.

[234] *https://enterprise.verizon.com/resources/reports/2017_dbir.pdf.*

TABLE 23—COSTS RELATED TO SECURITY TAGS—SUMMARY OF CARE CRITERIA

[2017 Dollars]

Tasks	Lower bound	Upper bound	Remarks
Task 1: Enhancements to health IT to upgrade databases and/or other backend infrastructure to appropriately apply security tags to data and/or develop access control capabilities.	1,500 hours	2,500 hours	This is a *one-time cost* for health IT systems to support data segmentation for discrete data.
Total Labor Hours	1,500 hours	2,500 hours.	
Hourly Rate	$107 per hour		
Cost per Product	$160,500	$267,500.	
Total Cost (23 products)	$3,691,500	$6,152,500.	

We believe the voluntary nature of these criteria would significantly mitigate health IT developer costs. We also expect developers to see a return on their investment in developing and preparing their health IT for these certification criteria given the benefits to interoperable exchange.

We anticipate potential costs for ONC related to the updated DS4P criteria (Security tags—Summary of Care—send and Security tags—Summary of Care—receive) associated with: (1) Developing and maintaining information regarding these updated criteria on the ONC website; (2) creating documents related to these updated criteria and making those documents 508 compliant; (3) updating, revising, and supporting Certification Companion Guides, test procedures, and test tools; and (4) responding to inquiries concerning these criteria. We estimate an ONC analyst at the GS–13, Step 1 level staff would devote, on average, 200 hours to the above tasks annually. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Therefore, we estimate the annual costs to be $18,200.

(B) Benefits

We believe leveraging the DS4P standard's ability to allow for both document level and more granular tagging would offer functionality that is more valuable to providers and patients, especially given the complexities of the privacy landscape for multiple care and specialty settings. The updated DS4P criteria (Security tags—Summary of Care—send and Security tags—Summary of Care—receive) would benefit providers, patients, and ONC because it would support more complete records, contribute to patient safety, and enhance care coordination. We believe this will also reduce burden for providers by enabling an automated option, rather relying on case-by-case manual redaction and subsequent workarounds to transmit redacted documents. Implementing security tags enables providers to more effectively share patient records with sensitive information, thereby protecting patient privacy while still delivering actionable clinical content. We emphasize that health care providers already have processes and workflows to address their existing compliance obligations, which could be made more efficient and cost effective through the use of health IT. We expect these benefits for providers, patients, and ONC to be significant; however, we are unable to quantify these benefits at this time because we do not have adequate information to support quantitative estimates. We welcomed comments regarding potential approaches for quantifying these benefits.

Comments. Several commenters indicated there would be cost burden associated with our proposal of adopting two new DS4P certification criteria and a consent management for API criterion. Commenters stated that ONC needs to quantify and include the cost of this burden in our impact analysis section. Another commenter conducted their own analysis and indicated a cost of $5–6 billion with a multi-year implementation timeframe. Commenters stated there could be significant upfront costs and ongoing costs for maintenance of the systems necessary to comply with these criteria and one commenter further explained that segmenting data at the document, section, and entry level as opposed to the document level only, would significantly increase costs and could potentially impact system performance. One commenter was specifically concerned that the proposal would broadly impact HIEs both in terms of administration and implementation but did not state specifics.

Response. We thank commenters for their input. We did not finalize the consent management for API criterion. For the DS4P-related criteria (Security tags—Summary of Care—send and Security tags—Summary of Care—receive), the developer costs were estimated for supporting DS4P IG enhancements to include tagging the data at the section and entry level when exchanged using the C–CDA. The lower bound estimates include developers who are already supporting the DS4P IG for tagging data at ''document'' level and estimates additional effort to support tagging at ''section'' and ''entry'' level. The criteria do not require the capability to segment the data, only to tag the data.

The certification criteria does not make any additional expectations around compliance beyond what the providers are currently expected to do, nor does it add any additional requirements for developers around how they handle the data received with the tags. Therefore, we disagree with the commenters about underestimating the cost. Rather, the commenters may be suggesting implementation costs which are beyond the costs associated with the certification criteria itself. These costs are unquantifiable and are noted in Table 31.

(3) Conditions and Maintenance of Certification Requirements

(i) Information Blocking

For a discussion of the costs and benefits of the exceptions to information blocking, please see section (5) of this RIA.

(ii) Assurances

In this final rule, we included a provision that requires health IT developers to make certain assurances as Conditions and Maintenance of Certification requirements: (1) Assurances regarding the ''EHI export'' certification criterion in § 170.315(b)(10) and (2) assurances regarding retaining records and information in 170.402(b)(1)(i)–(ii).

(A) Electronic Health Information Export

Alongside the criterion revisions in § 170.315(b)(10), we have finalized in § 170.402(a)(4), that a health IT developer of a certified health IT Modules that is part of a health IT product which electronically stores EHI must certify to the certification criterion in § 170.315(b)(10). We have finalized in § 170.402(b)(2) that within 36 months from the final rule's publication date, a health IT developer that must comply with the requirements of paragraph § 170.402(a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10). We also finalized that on and after 36 months from the publication of this final rule, health IT developers that must comply with the requirements of § 170.402(a)(4) must provide all of their customers of certified health IT with health IT certified to § 170.315(b)(10). In addition, a health IT developer must attest accurately in accordance with § 170.402(a)(4) and (b)(2) if the Health IT Module presented for certification is part of a heath IT product which can electronically store EHI. If the product stores such information, the health IT developer must ensure all EHI is available for export in accordance with § 170.315(b)(10).

For a detailed discussion of the costs and benefits of the assurances regarding the criterion in § 170.315(b)(10), please see section (2)(ii) (EHI export) of this RIA above.

(B) Records and Information Retention

As a Maintenance of Certification requirement in § 170.402(b)(1), a health IT developer must, for a period of 10 years beginning from the date of certification, retain all records and information necessary that demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program. In an effort to reduce administrative burden, we also finalized that in situations where applicable certification criteria are removed from the Code of Federal Regulations before the 10 years have expired, records must only be kept for three years from the date of removal for those certification criteria and related Program provisions unless that timeframe would exceed the overall 10-year retention period. This ''three-year from the date of removal'' records retention period also aligns with the records retention requirements for ONC–ACBs and ONC–ATLs under the Program.

As stated in the Proposed Rule, currently, there are no existing regulatory requirements regarding record and information retention by health IT developers. We expect there are costs to developers to retain the records and information described above but they may be mitigated due to other factors. For example, we expect that health IT developers are already keeping most of their records and information in an electronic format. We also expect that some developers may already be retaining records and information for extended periods of time due to existing requirements of other programs, including for those programs their customers participate in. For instance, Medicaid managed care companies are required to keep records for 10 years from the effective date of a contract.

We estimated that each health IT developer will, on average, spend two hours each week to comply with our proposed record retention requirement. We expect that a health IT developer's office clerk could complete the record retention responsibilities. According to the May 2017 BLS occupational employment statistics, the mean hourly wage for an office clerk is $16.30.[236] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $32.

Therefore, we estimated the annual cost per developer on average, would be $3,328 and the total annual cost for all health IT developers (458 health IT developers have products certified to the 2015 Edition that are capable of recording patient health data) on average, would be $1.5 million. We note that this is a perpetual cost.

(iii) Prohibition or Restriction of Communications

(A) Costs

Health IT developers need to notify their customers about the unenforceability of communications and contract provisions that violate the Communications Condition of Certification requirements in § 170.403(a). Generally, health IT developers already have mechanisms in place, whether via online postings, email, mail, or phone, for alerting customers to changes in their policies and procedures. Such alerts should be standard practice. However, we have estimated the potential costs for health IT developers to draft the notice and mail the notice as appropriate. We estimated that a health IT developer's office clerk will commit (overall) approximately 40 hours to drafting and mailing notices when necessary. According to the May 2017 BLS occupational employment statistics, the mean hourly wage for an office clerk is $16.30.[237] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $32. Therefore, we estimated the annual cost per developer to be $1,280 and the total cost for all health IT developers (792 health IT developers certified to the 2014 Edition) to be $1 million. We note that a developer must notify all customers annually until any contracts contravening the Condition are amended.

We also note that mailing is one option for delivery, along with other means such as email. We do not have information concerning how health IT developers will deliver their notices. We have estimated a total cost for all developers to mail the initial notices (including postage) to be $80,000. As noted above, this notice may have to be provided annually, depending on when contracts contravening this provision are amended.

In order to meet the Cures Act requirement that health IT developers do not prohibit or restrict communication regarding health IT, some health IT developers will eventually need to amend their contracts to reflect such a change. Many standard form health IT contracts limit the ability of users to voluntarily discuss problems or report usability and safety concerns that they experience when using their health IT. This type of discussion or reporting is typically prohibited through broad confidentiality, nondisclosure, and intellectual property provisions in the developer's standard form health IT contract. Some standard form health IT contracts may also include non-disparagement clauses that prohibit customers from making statements that could reflect negatively on the health IT developer. These practices are often referred to colloquially in the industry as ''gag clauses.'' We expect amendments to these clauses to be accomplished in the normal course of business, such as when renegotiating contracts or updating them for HIPAA Rules or other compliance requirements outside of the ONC Health IT Certification Program. As such, we do not estimate any direct or indirect costs

[235] *https://pages.nist.gov/800-63-3/sp800-63b.html.*

[237] *See https://www.bls.gov/oes/2017/may/oes439061.htm.*

for health IT developers to amend their contracts to comply with this Condition of Certification requirement.

(B) Benefits

We expect health care providers to benefit from this provision. There is growing recognition that these practices of prohibiting or restricting communication do not promote health IT safety or good security hygiene and that health IT contracts should support and facilitate the transparent exchange of information relating to patient care. We were unable to estimate these benefits because we do not have adequate information to determine the prevalence of gag clauses and other restrictive practices, nor do we have a means to quantify the value to providers of being able to freely communicate and share information. We welcomed comments on approaches to quantify these benefits.

Comments. We did not receive comments specific to our approach of quantifying the benefits of our provision to inform customers regarding the prohibition or restriction of communications. We did receive several comments stating that our notification and contract revision estimates underestimate the volume of agreements for large developers and the cost of compliance. We also received several comments that the burden for revising contracts could be significant and costly, particularly in the timeframe originally proposed, with one comment adding that the cost for revising contracts should be included in the impact analysis.

Response. We maintain that we were unable to estimate the benefits of the provision due to inadequate information however, we believe that prohibiting or restricting communication does not promote health IT safety or good security hygiene and that health IT contracts should support and facilitate the transparent exchange of information relating to patient care. We maintain our notification estimates as we believe that large developers would have efficient means of sending notifications *i.e.* by email. We reiterate that we expect revision of contracts to be accomplished in the normal course of business and do not estimate any direct or indirect costs for health IT developers to amend their contracts to comply.

(iv) Application Programming Interfaces

For a discussion of the costs and benefits of the new API criterion in § 170.315(g)(10), please see section (2)(iii) of this RIA.

(A) Transparency Requirements for Application Programming Interfaces

In this final rule, as part of the Conditions and Maintenance of Certification requirements in § 170.404, we have required that API Technology Suppliers make specific business and technical documentation necessary to interact with the APIs in production freely and publicly accessible. We expect that the API Technology Suppliers will perform the following tasks related to transparency of business and technical documentation and would devote the following number of hours annually to such tasks: (1) Health Level 7's (HL7®) Fast Healthcare Interoperability Resources (FHIR®) API documentation (the developer would most likely point to the HL7 FHIR standard for API documentation) (estimated eight hours); (2) patient application registration documentation, which will include a development effort to create a website that manages the application registration activity (estimated 40 hours); (3) publication of the FHIR Endpoint—Base URLs for all centrally managed providers (estimated 40 hours); (4) publication of FHIR Endpoints for provider-managed APIs (estimated 160 hours); and (5) API cost information documentation, which will typically be documented as a tiered rate based on usage or some form of monthly rate (estimated 40 hours).

We believe each of the above tasks would be performed by a ''Software Developer.'' According to the May 2017 BLS occupational employment statistics, the mean hourly wage for software developer is $53.74.[238] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs is $107. Therefore, we estimated the cost per developer to be $30,816. As noted in section (2)(iii) of this RIA, we estimated that 459 products from 394 developers will contain the API criterion. Therefore, we estimated the total developer cost would be $12.1 million. We note that this is a one-time cost and would not be perpetual. We did not receive comments on this discussion and have therefore finalized our figures.

(v) Real World Testing

The objective of real world testing in § 170.405 is to verify the extent to which deployed health IT products in operational production settings are demonstrating compliance to certification criteria and functioning with the intended use cases for continued maintenance of certification requirements. Real world testing should ensure certified health IT products have the ability to share electronic health information between systems. Real world testing should assess that the certified health IT is meeting the intended use case(s) of the certification criteria to which it is certified within the workflow, health IT architecture, and care/practice setting in which the health IT is implemented. We note that we expect real world testing would take about three months of the year to perform.

(A) Costs

This section describes the potential costs of the real world testing requirements in this final rule. The costs estimates are based on the following assumptions:

- *Health IT developers will use the same labor costs.* Table 24 shows the estimated labor costs for a health IT developer to perform real world testing. We recognize that health IT developer costs will vary; however, our estimates in this section assume all developers will incur the costs noted in Table 24.

- *Proxy needed to project the number of 2015 Edition products impacted by real world testing.* We estimated that 523 products from 429 developers will be impacted by real world testing. We used a proxy to determine developers that would be subject to real world testing. There were 681 products and 551 developers with at least one of its 2014 Edition certified products that could perform transitions of care and/or send any type of public health data. We then multiplied these numbers by our estimates for certified health IT market consolidation by −22.1 percent and −23.2 percent to project the number of 2015 developers and products, respectively. We believe this estimate serves as a reasonable proxy for products impacted by real world testing, as these products primarily focus on interoperability.

The tables below describe the various costs to health IT developers to perform real world testing by task.

[238] *See https://www.bls.gov/oes/2017/may/oes439061.htm.*

TABLE 24—ESTIMATED COST TO HEALTH IT DEVELOPERS TO PERFORM REAL WORLD TESTING

[2017 Dollars]

Tasks and labor category	Hours	Rate	Total
Task 1: Design Real world Testing Approach and Submit Plan (per developer)			$34,560
15–1133 Software Developers, Systems Software	80	107	8,560
15–1143 Computer Network Architects	120	104	12,480
15–1121 Computer Systems Analysts	80	89	7,120
15–1199 Computer Occupations, All Other	40	88	3,520
27–3042 Technical Writers	40	72	2,880
Task 2: Prepare Staff and Environments (per developer)			14,920
15–1121 Computer Systems Analysts	40	89	3,560
15–1142 Network and Computer Systems Administrators	40	83	3,320
15–1152 Computer Network Support Specialists	40	65	2,600
15–1199 Computer Occupations, All Other	40	88	3,520
15–1122 Information Security Analysts	20	96	1,920
Task 3: Perform Testing (per product)			32,240
15–1121 Computer Systems Analysts	80	89	7,120
15–1133 Software Developers, Systems Software	40	107	4,280
15–1199 Computer Occupations, All Other	160	88	14,080
15–1142 Network and Computer Systems Administrators	40	83	3,320
15–1141 Database Administrators	40	86	3,440
Task 4: Collect Results and Prepare-Submit Report (per developer)			20,560
15–1199 Computer Occupations, All Other	120	88	10,560
15–1121 Computer Systems Analysts	80	89	7,120
27–3042 Technical Writers	40	72	2,880
Total Labor Hours	1,140		
Other Direct Costs—printing, publishing (per product)			150.00

TABLE 25—REAL WORLD TESTING TOTAL ANNUAL COST

[2017 Dollars]

Task	Calculation	Total cost
Task 1	$34,560 * 429 developers	$14,826,240
Task 2	$14,920 * 429 developers	6,400,680
Task 3	$32,240 * 523 products	16,861,520
Task 4	$20,560 * 429 developers	8,820,240
Other Direct Costs	$150 * 523 products	78,450
Total Cost		46,987,130

Based on the stated assumptions and costs outlined in the above tables, we estimated the total annual cost for real world testing would, on average, be $47 million with an average cost per developer of $109,557.

(B) Benefits

There are several benefits that can be attributed to real world testing. Real world testing may impact the effective integration of varied health IT systems, including integration of certified health IT with non-certified and ancillary technologies such as picture archiving and communications systems (PACS) or specialty-specific interfaces. This could result in greater interoperability among health IT systems. For providers that are currently dissatisfied with how their health IT is performing, real world testing might also influence the effective implementation of workflows in a clinical setting. In this analysis, we calculated the benefits in the following categories: For providers that have complained about their EHR system, time saved documenting in their EHR due to improved usability; for providers that are dissatisfied with their EHR, increased provider satisfaction resulting in fewer providers incurring the costs of switching products; and benefits related to reductions in duplicate lab tests, readmissions, ER visits, and adverse drug events due to increased interoperability. We focused on these outcomes for two reasons: (i) Evidence in literature indicates that health information exchange impacts the chosen measures; and (ii) cost of care associated with these measures is high and the impact of health information exchange is likely to result in significant benefits in the form of reduced costs.

The benefit calculations were based on the following assumptions:

- *Benefits noted in academic literature are assumed accurate and results were not externally validated.*
- *Hospitals and eligible professionals that participate in the CMS Promoting Interoperability Programs will be impacted.* Estimates were based on the assumption that 439,187 health care providers and/or 4,519 hospitals will be affected by this regulatory action.
- *Estimates of the impact of real world testing on rates of interoperability (0.1 to 1 percent) are based on ONC analysis.* To identify the impact of real world testing on interoperability, we used regression analysis. Specifically, we estimated linear probability models that identified impact of 2014 Edition certified EHR on hospitals' interoperability (whether a hospital sends, receives, finds, and integrates summary of care records). Using data from the AHA from years 2014 and 2015 in the model, we controlled for hospital size, profit status, participation in a health information organization, and state and year fixed effects. The marginal effect of using a 2014 Edition was a five percentage point increase in interoperability. This is an upper bound estimate. For the purpose of this

analysis, we assume 0.1 percent to 1 percent would be a reasonable range for real world testing to impact interoperability.

- *Impact of real world testing is also based on the estimated number of providers that switch health IT developers (rate = five percent) and are dissatisfied with their current EHR (44 percent).* To calculate the number of providers that are likely to switch their EHR due to dissatisfaction with their system, we estimate the rate of switching using CMS Medicare EHR Incentive Program data from years 2013 to 2016. This results in 4,774 clinical practices and 226 hospitals that are projected to switch products in a year. We then leverage results from Stanford Medicine's research conducted by The Harris Poll which reports that nearly 44 percent of providers are not satisfied with their EHR.[239] Based on this research, we assume that approximately 2,195 providers are less likely to switch their EHR with real world testing.
- *Estimates of the rate of eligible professionals (10 percent) and hospitals (five percent) that will be impacted by real world testing are based on ONC complaint data.* We recognize that the benefits of real world testing are limited to those providers that have systems that might be underperforming. Therefore, we estimated that the providers impacted by this rule are limited to the proportion of providers that have issued complaints about their system to ONC.

As noted previously in this analysis, we acknowledge that there might be shared benefits across certain provisions and have taken steps to ensure that the benefits attributed to each provision are unique to the provision referenced. Specifically, we used regression analysis to calculate the impact of our real world testing and API provisions on interoperability. We assumed that the real world testing and API provisions would collectively have the same impact on interoperability as use of 2014 Edition certified health IT. Therefore, we estimated linear probability models that identified the impact of 2014 Edition certified health IT on hospitals' interoperability.[240] We controlled for additional factors such as participation in a health information exchange organization, hospital characteristics, and urban/rural status. We found the marginal effect of using 2014 Edition certified health IT was a five percentage point increase in interoperability.

We assumed that this marginal effect is true for our provisions and distributed the five percent benefit across our real world testing and API provisions at (0.1 to 1 percent) to (1 to 4 percent) respectively. Moreover, the number of providers impacted is provision specific. Given data limitations, we believe this approach allows us to estimate the benefits of our provisions without double counting the impact each provision might have on interoperability.

Table 26 shows the benefits of real world testing for providers. We quantified the monetary benefits of real world testing based on a reduction in the amount of time a provider spends on their EHR by improving its usability or the cost-savings associated with switching from an underperforming EHR system. Note, these benefits are limited to providers who have expressed dissatisfaction with their EHR and only represent a fraction of all health care providers. Table 27 quantifies the benefits associated with improved interoperability for these providers. This is primarily because provider behavior is more directly affected by improvements in interoperability.

TABLE 26—BENEFIT OF REAL WORLD TESTING FOR PROVIDERS

[2017 Dollars]

Benefit type	Number affected	Hourly wage	Hours saved (percent) [A] [B]		Hours per day with EHR	Number of working days in a year	Total benefit [C]	
			Min	Max			Min	Max
Reduction in provider time spent in health IT by improving usability and interoperability.	43,919 providers or 10% [D] (based on complaint data).	$97.85	1	5	6 [E]	260	$65 million per year.	$335 million per year.
Number of providers switching health IT [F].	2,195; Cost of Switching. Min = $15,000 Max = $70,000	.....	.....	.....	.....	.....	$34M per year.	$158M per year.
Total Benefit	.....	.....	.....	.....	.....	.....	$99M per year.	$493M per year.

[A] Julia Adler-Milstein and Robert S. Huckman, *The Impact of Electronic Health Record Use on Physician Productivity,* Am J Manag Care (Nov. 19, 2013).

[B] Amusan, Tongen, Speedie, and Mellin, *A time-motion study to evaluate the impact of EMR and CPOE implementation on physician efficiency,* J. Healthcare Inf. Manag. (Fall 2008), at 31–7.

[C] Total benefits for the provider and administrative time spent in health IT by improving usability and interoperability. Total benefits from switching EHR developer is a product of the number providers switching and cost of EHR.

[D] The estimate is based on the number of providers that currently possess products with complaints. This is identified by flagging health IT developers and products about whom/which complaints are logged on ONC's database. These health IT developers are then matched to physicians using the Meaningful Use database.

[E] Christine Sinsky et al., *Allocation of Physician Time in Ambulatory Practice: A Time and Motion Study in 4 Specialties,* Ann Intern Med. (Dec. 6, 2016), at 753–60. Physician Practice, *Calculating the Right Number of Staff for Your Medical Practice, available at http://www.physicianspractice.com/blog/calculating-right-number-staff-your-medical-practice.*

[F] This estimate was obtained from Meaningful Use data from years 2013–2016. ''Switching'' is defined as an annual change in all health IT developers by providers/hospitals.

[239] How Doctors Feel About Electronic Health Records National Physician Poll by The Harris Poll *http://med.stanford.edu/content/dam/sm/ehr/documents/EHR-Poll-Presentation.pdf.*

[240] American Hospital Association Health IT Supplement Survey, *http://www.ahadata.com/aha-healthcare-database.*

TABLE 27—BENEFIT OF REAL WORLD TESTING FOR PATIENTS AND PAYERS
[2017 Dollars]

Benefit type	Population affected	Overall interop impact (marginal effect)	Impact of real world testing		Total cost	Percentage of total cost impacted	Total benefit [A]	
			Min	Max			Min	Max
Duplicate testing	35,607 providers	[B] 0.09	0.001	0.01	$200 billion [C]	10	$1.9 million per year.	$18.5 million per year.
Avoidable hospitalizations and readmissions.	5% of hospitals (n = 226).	[B] 0.09	0.001	0.01	$41 billion [D]	5	$0.2 million per year.	$1.9 million per year.
ER visits	5% of visits affected (n = 131 million).	[B] 0.03	0.001	0.01	$1,233, Per ER visit [E].	5	$0.2 million per year.	$2.54 million per year.
Adverse drug events.	5% of events affected.	[F] 0.22	0.001	0.01	$30 billion [G]	5	$0.3 million per year.	$3.4 million per year.
Total Benefit	.....	.....	.....	.....	.....	.....	$2.6 million	$26.3 million.

[A] Total benefit is a product of *total cost, percent of total cost impacted, overall impact of interoperability, and impact of real world testing.*

[B] Stephen E. Ross, Tiffany A. Radcliff, William G. Leblanc, L. Miriam Dickinson, Anne M. Libby, and Donald E. Nease Jr., Effects of health information exchange adoption on ambulatory testing rates, J. Am. Med. Inform. Assoc. (2013), at 1137–1142; Bridget A. Stewart, Susan Fernandes, Elizabeth Rodriguez-Huertas, and Michael Landzberg, A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients, J. of the Am. Med. Informatics Assoc. (2010), at 341–344; Sezgin Ayabakan, Indranil R. Bardhan, Zhiqiang (Eric) Zheng, and Kirk Kirksey Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals, MIS Quarterly (Jan. 1, 2017); Eric J. Lammers, Julia Adler-Milstein, and Keith E. Kocher, Does health information exchange reduce redundant imaging? Evidence from emergency departments, Med Care (Mar. 2014), at 227–34.

[C] National Academy of Medicine. (2016), *http://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html.*

[D] Agency for Healthcare Research and Quality (AHRQ) Statistical Brief #199 (Dec. 2015), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb199-Readmissions-Payer-Age.pdf*; AHRQ Statistical Brief #72, Nationwide Frequency and Costs of Potentially Preventable Hospitalizations (Apr. 2009), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb72.pdf.*

[E] National Center for Health Statistics (NCHS) Data Brief No. 252 (June 2016), *https://www.cdc.gov/nchs/data/databriefs/db252.pdf*; Nolan Caldwell, Tanja Srebotnjak, Tiffany Wang, and Renee Hsia, ''How Much Will I Get Charged for This?'' Patient Charges for Top Ten Diagnoses in the Emergency Department (2013), *https://doi.org/10.1371/journal.pone.0055491.*

[F] M.F. Furukawa, W.D. Spector, M.R. Limcangco, and W.E. Encinosa, *Meaningful use of health information technology and declines in in-hospital adverse drug events,* J. of the Am. Med. Informatics Assoc. (2017).

[G] Janet Sultana, Paola Cutroneo, and Gianluca Trifirò, *Clinical and economic burden of adverse drug reactions* (Dec. 2013).

Based on the stated assumptions and benefits outlined in Table 26, we estimate the total annual benefit for real world testing to providers would range, on average, from $99 million to $493 million. Based on the stated assumptions and benefits outlined in Table 27, we estimate the total annual benefit for patients and payers would range, on average, from $2.6 million to $26.3 million. Therefore, we estimate the total benefit of real world testing would range, on average, from $101.6 million to $519.3 million.

We recognize that health IT developers may deploy their systems in a number of ways, including cloud-based deployments, and requested comment on whether our cost estimates of real world testing should factor in such methods of system deployment. For example, we requested feedback about whether health IT developers would incur reduced real world testing costs through cloud-based deployments as opposed to other deployment methods. We specifically solicited comment on the general ratio of cloud-based to non-cloud-based deployments within the health care ecosystem and specific cost variations in performing real world testing based on the type of deployment. We also requested comment on our assumptions about the burden to providers in time spent assisting health IT developers since we encourage health IT developers to come up with ways to perform real world testing that mitigate provider disruption.

Comments. We did not receive comment specific to whether health IT developers would incur reduced real world testing costs through cloud-based deployments as opposed to other deployment methods. We also did not receive comments regarding the ratio of cloud-based to non-cloud based deployments and cost variations regarding different types of deployments. We also did not receive comments regarding the burden to providers in time spent assisting health IT developers.

Response. We maintain our assumptions and estimates as proposed regarding real world testing.

(C) Real World Testing Maintenance Requirements

In this final rule, we revised the Principle of Proper Conduct in § 170.523(m) to require ONC–ACBs to collect, no less than quarterly, all updates successfully made to standards in certified health IT pursuant to the developers having opted to avail themselves of the Standards Version Advancement Process flexibility under the real world testing Condition of Certification requirement. Under § 170.523(p), ONC–ACBs will be responsible for: (1) Reviewing and confirming that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1); (2) reviewing and confirming that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2); and (3) submitting real world testing plans by December 15 and results by March 15 of each calendar year to ONC for public availability. In addition, under § 170.523(t), ONC–ACBs will be required to: (1) Maintain a record of the date of issuance and the content of developers' notices; and (2) timely post content of each notice on the CHPL.

Using the information from the ''Real World Testing Costs'' section of this RIA, we estimated that 429 developers will be impacted by real world testing. We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to collect all updates made to standards in Health IT Modules in accordance with § 170.523(m). The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Since the collection must occur no less than quarterly, we assume it occurs, on average, four times per year. Therefore, we estimate the annual cost to ONC–ACBs to comply with the collection requirements under § 170.523(m) to be $78,078.

We estimated that, on average, it will take an ONC–ACB employee at the GS–

13, Step 1 level approximately one hour to review and confirm that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1). We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to review and confirm that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2). We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to submit real world testing plans and results to ONC for public availability. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Therefore, we estimate the annual cost to ONC–ACBs to comply with the submission and reporting requirements under §§ 170.523(m) and 170.550(l) to be $156,156.

Throughout the RIA we have used 830 products as our 2015 Edition projection. We came up with this projection by multiplying a −23.2 percent market consolidation rate from the total number of products certified to 2014 Edition. This assumption was based on the market consolidation rate observed between the 2011 and 2014 Editions. We have estimated the number of 2015 Edition products that will certify each criterion included in the real world testing Condition of Certification requirement. We assume that there will be a cost associated with a notice for each certified criterion (even if an individual product were to update the same standard across multiple criteria that use that standard). This estimation was calculated by multiplying the current percent of 2015 Edition products that certify a criterion by the estimated number of total 2015 Edition products (830). For example, we calculated that 43 percent of 2015 Edition products certified 170.315(b)(1); we then multiplied this percentage by 830—the predicted number of 2015 Edition products. Thus, based on this calculation, for 2015 Edition, we predict that 359 products will certify the 170.315(b)(1) criterion. This method was used across all criteria included in the real world testing Condition of Certification requirement.

We assume that the amount of time for an ONC–ACB staff person to: (1) Maintain a record of the date of issuance and the content of developers' notices; and (2) to timely post content of each notice on the CHPL can be anywhere from 30 minutes to one hour.

The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. This was the hourly rate we used for this RIA, so it is consistent with prior calculations. This wage is used to determine the ONC–ACB time cost to complete this requirement under § 170.523(t). For this estimate, we take half the hourly rate and multiply it by the number of products predicted to certify each of the applicable criteria. For each criterion, we estimate a lower bound and upper bound prediction. The lower bound assumes that 25 percent of certified products update any of the applicable standards. The upper bound prediction assumes that all certified products update any of the applicable standards. These estimates are calculated for each criterion and then the cumulative sum of all the individual criterion calculations is made. We estimate, at 30 minutes per notice, it will cost $60,606 if 25 percent of certified products update any of the applicable standards across all criteria, and if all products update any of the applicable standards, we estimate it will cost $242,424. Our maximum estimate for time to comply is one hour per notice.

Using the same methodology explained above, we estimate, at 60 minutes per notice, it will cost $121,212 if 25 percent of certified products update any of the applicable standards across all criteria, and if all products update any of the applicable standards, we estimate it will cost $484,848. Our lower bound estimate for the cost of this requirement is $60,606. Our upper bound estimate for the cost of this requirement is $484,848.

Comments. We received a comment recommending that ONC add accountability to the real world testing process by having ONC–ACBs review a randomly selected percentage of submitted results for potential non-conformity with certification requirements.

Response. We thank commenters for their input. It is within ONC–ACBs' rights and interests to randomly select certified Health IT Modules that have been real world tested as part of their surveillance activities. ONC will be working closely with ONC–ACBs to provide direction on how ONC–ACBs can leverage existing Program and ISO/IEC 17065 requirements to provide oversight without increasing burden by setting a minimum expectation in regulation. Setting a regulatory quota could potentially create burden as workloads amongst the different ONC–ACBs vary. Additionally, it limits ONC–ACBs to what is adopted in the final rule and prevents future adjustments that may be needed to improve efficiency without additional rulemaking. We have finalized our estimates.

(vi) Attestations

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification requirement under the Program, provide to the Secretary an attestation to all the Conditions and Maintenance of Certification requirements specified in the Cures Act, except for the ''EHR Reporting Program'' Condition of Certification requirement. It also requires that a health IT developer attest that its health IT allows for health information to be exchanged, accessed, and used in the manner described by the API Condition of Certification requirement. We have finalized our proposal to implement the Cures Act ''attestations'' requirement in § 170.406 by requiring health IT developers to attest to the aforementioned Conditions. For the purposes of estimating the potential burden of these attestations on health IT developers, ONC–ACBs, and ONC, we estimate that all health IT developers under the Program will submit an attestation biannually. As noted previously in this RIA, there are 792 health IT developers certified to the 2014 Edition.

We estimated it would take a health IT developer employee approximately one hour on average to prepare and submit each attestation to the ONC–ACB. According to the May 2017 BLS occupational employment statistics, the mean hourly wage for a software developer is $53.74.[241] Therefore, we estimated the annual cost including overhead costs to be $84,744. We have finalized that attestations will be submitted to ONC–ACBs on behalf of ONC and the Secretary. We assume there will be four ONC–ACBs as this is the current number of ONC–ACBs, and we also assume an equal distribution in responsibilities among ONC–ACBs. ONC–ACBs would have two responsibilities related to attestations. One responsibility we finalized in § 170.523(q) is that an ONC–ACB must review attestations for completion and submit the health IT developers' attestations to ONC. We estimate it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes on average to review and submit each attestation to ONC. The other responsibility we are finalizing in § 170.550(l) is that an ONC–ACB would need to ensure that the health IT developer of the Health IT Module has

[241] *See https://www.bls.gov/oes/2017/may/oes439061.*

met its responsibilities related to the Conditions and Maintenance of Certification requirements as solely evidenced by its attestation. We estimate it will take an ONC–ACB employee at the GS–13, Step 1 level approximately one hour on average to complete this task. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Therefore, we estimate the annual cost to ONC–ACBs to be $108,108.

We have finalized that we would make the attestations publicly available on the CHPL once they are submitted by the ONC–ACBs. ONC posts information regularly to the CHPL and we estimate the added costs to post the attestation will be de minimis.

Comments. We did not receive comment specific to the methods related to the estimates for posting attestations.

Response. We maintain our assumptions and estimates as proposed regarding attestations.

(4) Oversight for the Conditions and Maintenance of Certification Requirements

Our processes for overseeing the Conditions and Maintenance of Certification requirements will, for the most part, mirror our processes for direct review of non-conformities in certified health IT as described in current § 170.580. We may directly review a health IT developer's actions to determine whether they conform to the Conditions and Maintenance of Certification requirements finalized in this final rule. The estimated costs and benefits for such oversight and review are detailed below.

(i) Costs

We estimated the potential monetary costs of allowing ONC to directly review a health IT developer's actions to determine whether the actions conform to the requirements of the Program as follows: (1) Costs for health IT developers to correct non-conforming actions identified by ONC; (2) costs for health IT developers and ONC costs related to ONC review and inquiry into non-conforming actions by the health IT developer; and (3) costs for ONC–ACBs related to the new reporting requirement in the Principles of Proper Conduct in § 170.523(s).

(A) Costs for Health IT Developers to Correct Non-Conforming Actions Identified by ONC

We do not believe health IT developers face additional direct costs for the ONC direct review of health IT developer actions (*see* cost estimates for the Conditions and Maintenance of Certification requirements). However, we acknowledge that this final rule may eventually require health IT developers to correct certain actions or non-conformities with their health IT that do not conform to the Conditions and Maintenance of Certification requirements.

If we identify a non-conforming action by a health IT developer, the costs incurred by the health IT developer to bring its actions into conformance will be determined on a case-by-case basis. Factors that will be considered include, but are not limited to: (1) The extent of customers and/or business affected; (2) how pervasive the action(s) is across the health IT developer's business; (3) the period of time that the health IT developer was taking the action(s) in question; and (4) the corrective action required to resolve the issue. We are unable to reliably estimate these costs as we do not have cost estimates for a comparable situation. We requested comment on existing relevant data and methods we could use to estimate these costs.

Comments. We did not receive any comments specific to the relevant data and methods used to estimate the costs to correct non-conforming actions identified by ONC.

Response. We maintain our approach used to estimate the costs to correcting identified non-conformities.

(B) Costs for Health IT Developers and ONC Costs Related to ONC Review and Inquiry Into Health IT Developer Actions

In order to calculate the potential costs to health IT developers and ONC related to ONC review and inquiry into health IT developer actions, we have created the following categories for potential costs: (1) ONC review and inquiry prior to the issuance of a notice of non-conformity; (2) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer does not contest ONC's findings (*i.e.,* no appeal); and (3) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer contests ONC's findings (*i.e.,* appeal).

(C) ONC Review and Inquiry Prior to the Issuance of a Notice of Nonconformity

We anticipate that ONC will receive, on average, between 100 and 200 complaints per year concerning the Conditions and Maintenance of Certification requirements that will warrant review and inquiry by ONC. We estimate that such initial review and inquiry by ONC will require, on average, two to three analysts at the GS–13 level working one to two hours each per complaint. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Therefore, we estimate each review and inquiry will cost ONC, on average, between $182 and $546. We estimate the total annual cost to ONC will, on average, range from $18,200 and $109,200. This range takes into account both the low end of reviews that are resolved quickly and the high end in which staff will need to discuss issues with ONC leadership or in some cases, HHS senior leadership including the Office of General Counsel. We have not estimated health IT developer costs associated with ONC review prior to the issuance of a notice of non-conformity because, in most cases, health IT developers are not required to take action prior to the notice of non-conformity.

(D) ONC Review and Inquiry Following the Issuance of a Notice of Non-Conformity and the Health IT Developer Does Not Contest ONC's Findings

This category captures cases that require review and inquiry following ONC's issuance of a notice of non-conformity, but that do not proceed to the appeals process. Examples of such situations would include, but not be limited to: (1) A health IT developer violates a Condition of Certification requirement and does not contest ONC's finding that it is in violation of the Condition of Certification requirement; or (2) a health IT developer fails to meet a deadline, such as for its corrective action plan (CAP). We estimate that ONC will, on average, conduct between 12 and 18 of these reviews annually.

We estimate that a health IT developer may commit, on average and depending on complexity, between 10 and 40 hours of staff time per case to provide ONC with all requested records and documentation that ONC would use to review and conduct an inquiry into health IT developer actions, and, when necessary, make a certification ban and/or termination determination. We assumed that the work will be performed by a ''Computer Systems Analyst.'' According to the May 2017 BLS occupational employment statistics, the mean hourly wage for computer systems analyst is $44.59.[242] As noted previously, we have assumed that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including overhead costs would be $89. Therefore,

[242] *https://www.bls.gov/oes/2017/May/oes151121.htm.*

we estimate the average annual cost for health IT developers would range from $10,680 to $64,080. We note that some health IT developers' costs are expected to be less and some health IT developers' costs are expected to be more than this estimated cost range. Further, we note that these costs would be perpetual.

We estimate that ONC may commit, on average and depending on complexity, between eight and 80 hours of staff time to complete a review and inquiry into health IT developer actions. We assume that the expertise of a GS–15, Step 1 Federal employee(s) will be necessary. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $126. Therefore, based on the estimate of between 12 and 18 cases each year, we estimate ONC's annual costs would range, on average, from $12,096 to $181,440. We note that some reviews and inquiries may cost less and some may cost more than this estimated cost range. Further, we note that these costs would be perpetual.

We welcomed comments on our estimated costs and any comparable processes and costs that we could use to improve our estimates.

Comments. We did not receive any comments specific to the relevant data and methods used to estimate the costs to: (1) ONC review and inquiry prior to the issuance of a notice of non-conformity; (2) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer does not contest ONC's findings (*i.e.,* no appeal); and (3) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer contests ONC's findings (*i.e.,* appeal).

Response. We maintain our approach used to estimate the costs to health IT developers and to ONC, related to ONC review and inquiry into health IT developer actions.

(E) ONC Review and Inquiry Following the Issuance of a Notice of Non-Conformity and the Health IT Developer Contests ONC's Findings

As discussed in section VII.C of this preamble, we permit a health IT developer to appeal an ONC determination to issue a certification ban and/or terminate a certification under § 170.580(a)(2)(iii). This category of cost calculations captures cases that require review and inquiry following ONC's issuance of a notice of non-conformity and where the health IT developer contests ONC's finding and files an appeal. We estimate that ONC will, on average, conduct between three and five of these reviews annually.

We estimated that a ''Computer Systems Analyst'' for the health IT developer may commit, on average and depending on complexity, between 20 and 80 hours to provide the required information to appeal a certification ban and/or termination under § 170.580(a)(2)(iii) and respond to any requests from the hearing officer. According to the May 2017 BLS occupational employment statistics, the mean hourly wage for a computer systems analyst is $44.59.[243] Assuming that overhead costs (including benefits) are equal to 100 percent of pre-tax wages, the hourly wage including overhead costs is $89. Therefore, we estimate the annual cost, including overhead costs, for a health IT developer to appeal a certification ban and/or termination under § 170.580(a)(2)(iii) would, on average, range from $5,340 to $35,600. We note that some health IT developers' costs are expected to be less and some health IT developers' costs are expected to be more than this estimated cost range. Further, we note that these costs would be perpetual.

We estimated that ONC would commit, on average and depending on complexity, between 40 and 160 hours of staff time to conduct each appeal. This will include the time to represent ONC in the appeal and support the costs for the hearing officer. We assume that the expertise of a GS–15, Step 1 Federal employee(s) would be necessary. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $126. Therefore, based on the estimate of between three and five cases each year, we estimate the cost for ONC to conduct an appeal would range, on average, from $15,120 to $100,800. We note that some appeals may cost less and some may cost more than this estimated cost range. Further, we note that these costs would be perpetual.

Based on the above estimates, we estimated the total annual costs for health IT developers related to ONC review and inquiry into health IT developer actions would range, on average, from $16,020 to $99,680. We estimated the total annual costs for ONC related to ONC review and inquiry into health IT developer actions would range, on average, from $44,603 to $383,345.

Comments. We did not receive any comments specific to the relevant data and methods used to estimate the costs of (1) ONC review and inquiry prior to the issuance of a notice of non-conformity; (2) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer does not contest ONC's findings (*i.e.,* no appeal); and (3) ONC review and inquiry following the issuance of a notice of non-conformity and the health IT developer contests ONC's findings (*i.e.,* appeal).

Response. We maintain our approach used to estimate the costs to health IT developers and to ONC, related to ONC review and inquiry into health IT developer actions.

(F) Costs for ONC–ACBs

We also note that ONC–ACBs could realize costs associated with the new reporting requirement in the Principles of Proper Conduct in § 170.523(s) that they report, at a minimum, no later than a week after becoming aware of, any information that could inform whether ONC should exercise direct review under § 170.580(a). We estimate that, on average, it will take an ONC–ACB employee at the GS–13, Step 1 level approximately 30 minutes to prepare the report. The hourly wage with benefits for a GS–13, Step 1 employee located in Washington, DC is approximately $91. Since the collection must occur no less than weekly, we will assume it occurs, on average, 52 times per year. Therefore, given that there are currently three ONC–ACBs, we estimate the annual cost to ONC–ACBs to comply with the reporting requirement under § 170.523(s) would, on average, be $7,098. We did not receive comments regarding our calculations. We have finalized these estimates.

(ii) Benefits

This final rule's provisions for ONC direct review of the Conditions and Maintenance of Certification requirements would promote health IT developers' accountability for their actions and ensure that health IT developers' actions conform with the requirements of the Cures Act and Conditions and Maintenance of Certification requirements in §§ 170.400–406. Specifically, ONC's direct review of health IT developer actions will facilitate ONC's ability to require comprehensive corrective action by health IT developers to address non-conforming actions determined by ONC. If ONC ultimately implements a certification ban and/or terminates a certification(s), such action will serve to protect the integrity of the Program and users of health IT. While we do not have available means to quantify the benefits of ONC direct review of health IT developer actions, we note that ONC

[243] *See https://www.bls.gov/oes/2017/May/oes151121.htm.*

direct review supports and enables the National Coordinator to fulfill his responsibilities under the HITECH Act and Cures Act, instills public confidence in the Program, and protects public health and safety. We did not receive comments regarding our calculations. We have finalized these estimates. (5) Information Blocking

(i) Costs

We expect ONC to incur an annual cost for issuing educational resources related to the information blocking ''reasonable and necessary'' exceptions. We estimate that ONC issues educational resources each quarter, therefore, four per year. We assume that the educational resources would be provided by ONC staff with the expertise of a GS–15, Step 1 Federal employee(s). The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately $126. We estimate it would take ONC staff between 200 and 400 hours to develop the guidance. Therefore, we estimate the annual cost to ONC would range, on average, from $100,800 to $201,600.

Comments. We did not receive any comments regarding the specific costs associated with information blocking.

Response. We have adopted our estimates as proposed. We note that we did receive comments regarding ''burden'' on various stakeholder groups related to our information blocking proposals, and those comments are addressed throughout the information blocking section (section VIII) of this final rule.

(ii) Benefits

Information blocking not only interferes with effective health information exchange, but also negatively impacts many important aspects of health and health care. For a detailed discussion of the negative impacts of information blocking, we refer readers to section XIV.C.2.a(2) of the Proposed Rule (84 FR 7584).

The exceptions to the information blocking definition adopted in this final rule create clear guidelines for industry regarding pro-competitive and other beneficial activities and will enable stakeholders to determine more easily and with greater certainty whether their activities are excepted from the information blocking definition. Overall, the finalized exceptions are accommodating to legitimate industry practices for health IT developers, hospitals, and health care providers and, we believe, will ease the burden and compliance costs for these parties.

To estimate the benefits of information blocking, we first examined existing data sources to identify a proxy that will indicate the extent to which information blocking is occurring. According to analysis of data from the American Hospital Association IT Supplement survey, 53 percent of non-Federal acute care hospitals reported that they had challenges with exchanging data across different vendor platforms.[244] Moreover, 31 percent reported that they must pay additional costs to exchange information with organizations outside of the system. Nearly one in four hospitals reported that they had to develop customized interfaces to electronically exchange information.

To quantify the magnitude of information blocking and the benefits of restricting information blocking, we estimated the following, which gives us the imposed cost of information blocking for each health outcome: [Percent of providers that engage in cross-vendor exchange] * [marginal effect (ME) of information blocking on interoperability] * [ME effect of interoperability on the health outcome] * [total cost of health outcome].

We extracted the ''ME effect of interoperability on the health outcome'' and ''cost of health outcomes'' from academic literature (*see* citations in Table 24). We then determined a proxy for the number of providers that engage in cross-vendor exchange. We did this by leveraging hospital referral data from 2015 to determine the proportion of hospitals that referred patients to a provider outside of their system where the receiving provider used a different EHR vendor. We determined that 82 percent of hospitals engaged in cross-vendor exchange. This estimate was used as the proxy for ''providers that engaged in cross-vendor exchange.''

We estimated the ''ME of information blocking on interoperability'' through the following research design:

$$Y = b1InforBlock + X'B + e$$

Where y = 1 if a hospital routinely engages in four domains of interoperability—sending, receiving, finding, and integrating data, 0 otherwise. The variable InforBlock is a binary indicator for whether a hospital reported experiencing challenges with exchanging data across different vendor platforms. We assume the impact of reporting this barrier is a proxy for the extent to which vendors hinder a hospital's interoperability. In the model, we control for the following: Hospital's primary vendor, participation in health exchange organization, participation in five different networks, system ownership, level of system centralization, bed size, profit status, public status, region, location in urban area. The marginal effect of b is 0.04. We assume that this effect may capture other reasons not related to information blocking, so we use half of this estimate for our benefit calculations—0.02.

TABLE 28—BENEFITS OF PROHIBITING AND/OR DETERRING INFORMATION BLOCKING

[2017 Dollars]

Benefit type	Total cost impacted	Total cost	Overall interop impact (marginal effect)	Percent of providers susceptible to information blocking	Marginal effect of information blocking (percentage points)	Benefit benefit [A]
Duplicate testing	100%	200 billion [B]	[C] 0.09	82	0.02	$295,200,000
Avoidable hospitalizations and readmissions.	100%	$41 billion [D]	0.09	82	0.02	60,516,000
ER visits	131 million visits [E].	Cost per ER visit $1,233.	0.03	82	0.02	79,469,316
Adverse drug events	20%	$30 billion [F]	0.22	82	0.02	21,648,000

[244] Pylypchuk Y., Johnson C., Henry J. & Ciricean D. (November 2018). Variation in Interoperability among U.S. Non-Federal Acute Care Hospitals in 2017. ONC Data Brief, no.42. Office of the National Coordinator for Health Information Technology: Washington DC.

TABLE 28—BENEFITS OF PROHIBITING AND/OR DETERRING INFORMATION BLOCKING—Continued

[2017 Dollars]

Benefit type	Total cost impacted	Total cost	Overall interop impact (marginal effect)	Percent of providers susceptible to information blocking	Marginal effect of information blocking (percentage points)	Benefit benefit [A]
Total benefit per year	.....	.....	.....	.....	.....	$456,833,316

[A] Total benefit would be a product of *% of total cost impacted, total cost, overall interop impact, percent of providers susceptible to information blocking, and marginal effect of information blocking;* however, no reasonable estimate of the marginal effect of information blocking is currently available.

[B] National Academy of Medicine (2016), *http://money.cnn.com/2017/05/20/news/economy/medical-tests/index.html.*

[C] Stephen E. Ross, Tiffany A. Radcliff, William G. Leblanc, L. Miriam Dickinson, Anne M. Libby, and Donald E. Nease Jr., *Effects of health information exchange adoption on ambulatory testing rates,* J. Am. Med. Inform. Assoc. (2013), at 1137–1142; Bridget A. Stewart, Susan Fernandes, Elizabeth Rodriguez-Huertas, and Michael Landzberg, *A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients,* J. of the Am. Med. Informatics Assoc. (2010), at 341–344; Sezgin Ayabakan, Indranil R. Bardhan, Zhiqiang (Eric) Zheng, and Kirk Kirksey *Value of health information sharing in reducing healthcare waste: An analysis of duplicate testing across hospitals,* MIS Quarterly (Jan. 1, 2017); Eric J. Lammers, Julia Adler-Milstein, and Keith E. Kocher, *Does health information exchange reduce redundant imaging? Evidence from emergency departments,* Med Care (Mar. 2014), at 227–34.

[D] Agency for Healthcare Research and Quality (AHRQ) Statistical Brief #199 (Dec. 2015), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb199-Readmissions-Payer-Age.pdf;* AHRQ Statistical Brief #72, Nationwide Frequency and Costs of Potentially Preventable Hospitalizations (Apr. 2009), *https://www.hcup-us.ahrq.gov/reports/statbriefs/sb72.pdf.*

[E] National Center for Health Statistics (NCHS) Data Brief No. 252 (June 2016), *https://www.cdc.gov/nchs/data/databriefs/db252.pdf;* Nolan Caldwell, Tanja Srebotnjak, Tiffany Wang, and Renee Hsia, "How Much Will I Get Charged for This?" Patient Charges for Top Ten Diagnoses in the Emergency Department (2013), *https://doi.org/10.1371/journal.pone.0055491.*

[F] Janet Sultana, Paola Cutroneo, and Gianluca Trifirò, *Clinical and economic burden of adverse drug reactions.*

As a result of this calculation, we estimate that the benefit of the information blocking provision is $456 million.

Comments. We did not receive any comments regarding our approach to estimating benefits or the specific benefit estimates associated with information blocking.

Response. ONC has revised its methodological approach to quantifying the benefits of our information blocking provision. This new methodology is described in the RIA.

(6) Total Annual Cost Estimate

The total annual cost estimate is expressed in 2016 dollars to meet regulatory reform analysis requirements under Executive Order 13771. We estimated that the total cost for this final rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would range, on average, from $953 million to $2.6 billion with an average annual cost of $1.8 billion. We estimated that the total perpetual cost for this final rule (starting in year two), based on the cost estimates outlined above, would range, on average, from $366 million to $1.3 billion with an average annual cost of $840 million. We also included estimates based on the stakeholder groups affected. We estimated the total costs to health IT developers to be between $483 million and $1.1 billion (including one-time and perpetual costs) with $633,000 in cost savings from deregulatory actions. Assuming that 458 health IT developers will be impacted, the cost per developer will range from $1.1 million to $2.4 million. Based on previous participation in the CMS EHR Incentive Program, we estimated that 439,187 health care providers in 95,470 clinical practices and 4,519 hospitals that participated in the CMS EHR Incentive Program will be impacted by this final rule. We estimated the total cost to health care providers to be between $478 million to $1.6 billion. We did not calculate per entity costs for health care providers. We acknowledged that costs may be passed from health IT developers to their customers (*i.e.* health care providers) during the licensing of their health IT modules. We estimated the total costs to ONC–ACBs to be between $391,000 and $792,000. We estimated the government costs (through labor hours of ONC staff) to be between $159,000 and $586,000 with $4,497 in cost savings from deregulatory actions. In addition to the above-mentioned cost savings that are attributable to specific stakeholder groups, we estimated an additional cost savings of $6.6 million to $13.3 million to all stakeholders affected by this provision. We are unable to attribute these amounts to specific stakeholder groups. We did not receive comment regarding these calculations. We have finalized our estimates.

(7) Total Annual Benefit Estimate

The total annual benefit estimate is expressed in 2016 dollars to meet regulatory reform analysis requirements under Executive Order 13771. We estimated the total annual benefit for this final rule, based on the benefit estimates outlined above, would range from $1.2 billion to $5.0 billion with primary estimated annual benefit of $3.1 billion. Our estimates include benefits attributed to the entire health care system, including hospitals, clinicians, payers and patients.(8) Total Annualized Net Benefit

The total annualized net benefit is expressed in 2016 dollars to meet regulatory reform analysis requirements under Executive Order 13771. We estimate the total annualized net benefit for this final rule, based on the estimates outlined above, would range from $191 million to $2.3 billion with a primary net benefit estimate of $1.3 billion.

b. Accounting Statement and Table

When a rule is considered an economically significant rule under Executive Order 12866, we are required to develop an accounting statement indicating the classification of the expenditures associated with the provisions of the proposed rule. Monetary annual benefits are presented as discounted flows using three percent and seven percent factors in Table 29. We are not able to explicitly define the universe of all costs, but have provided an average of likely costs of this final rule as well as a high and low range of likely costs. Unquantifiable costs and benefits are noted in Table 31. This final rule requires no Federal transfers, but it might bring about a reduction in fraudulent payments to providers by the

Federal Government and other payers.[245]

TABLE 29—EO 12866 SUMMARY TABLE

[In $ millions, 2016 Dollars]

	Primary (3%)	Lower bound (3%)	Upper bound (3%)	Primary (7%)	Lower bound (7%)	Upper bound (7%)
Present Value of Quantified Costs	6,454	2,966	9,943	4,574	2,120	7,028
Present Value of Quantified Benefits	23,411	8,831	37,991	16,552	6,244	26,859
Present Value of Net Benefits	16,957	5,865	28,049	16,552	4,124	19,832
Annualized Quantified Costs	852	391	1,312	854	396	1,312
Annualized Quantified Benefits	3,089	1,165	5,013	2,184	824	3,544
Annualized Net Quantified Benefits	2,237	774	3,701	1,330	428	2,232

TABLE 30—E.O. 12866 SUMMARY TABLE NON-DISCOUNTED FLOWS

[2016 Dollars]

	Year 1	Year 2	Year 3	Year 4	Year 5
Costs	942,795,801	839,887,346	839,887,346	839,887,346	839,887,346
Benefits	3,088,980,583	3,088,980,583	3,088,980,583	3,088,980,583	3,088,980,583
	Year 6	Year 7	Year 8	Year 9	Year 10
Costs	839,887,346	839,887,346	839,887,346	839,887,346	839,887,346
Benefits	3,088,980,583	3,088,980,583	3,088,980,583	3,088,980,583	3,088,980,583

TABLE 31—NON-QUANTIFIABLE BENEFITS

[2016 Dollars]

Benefits	Present value of 10 years by discount rate (in millions)		Annualized value over 10 years by discount rate (in millions)	
	3 Percent	7 Percent	3 Percent	7 Percent
Quantified Benefits	23,411	16,552	3,089	2,184

Non-quantified Benefits:

Impact on users of health IT that were ineligible or did not participate in the CMS EHR Incentive Programs; developer cost savings from no longer supporting the 2014 Edition; provider and patient benefit from implementation of USCDI and Security tags (DS4P) provisions due to improvements in interoperability; benefits associated with communication provision because we do not have adequate information to determine the prevalence of gag clauses and other such restrictive practices nor do we have a means to quantify the value to providers of being able to freely communicate and share information; benefit of ONC oversight on real world testing and non-conformance; external regulatory and policy activities.

Costs	3 Percent	7 Percent	3 Percent	7 Percent
Quantified Costs	6,454	4,574	852	396

Non-quantified Costs:

Impact of provisions on health IT production costs such as the supply and demand for personnel over time; costs developers to correct non-conformities; ONC cost to review non-conformities, real-world testing maintenance by ACBs; additional provider implementation activities related to USCDI and DS4P; external regulatory and policy activities.

3. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. The Small Business Administration (SBA) establishes the size of small businesses for Federal Government programs based on average annual receipts or the average employment of a firm.[246] The entities that are likely to be directly affected by the requirements in this final rule are health IT developers. We note that the reasonable and necessary activities that do not constitute information blocking provide flexibilities and relief for health IT developers of certified health IT, health information networks, health information exchanges, and health care providers in relation to the information blocking provision of the Cures Act. These reasonable and necessary activities also take into account the potential burden on small entities to

[245] Parente, Stephen T., Karen Mandelbaum, Susan P. Hanson, Bonnie S. Cassidy and Donald W. Simborg. ''Crime and Punishment: Can the NHIN Reduce the Cost of Healthcare Fraud?'' *Journal of Healthcare Information Management* 22(3): 42–51. June 2008.

[246] The SBA references that annual receipts means ''total income'' (or in the case of a sole proprietorship, ''gross income'') plus ''cost of goods sold'' as these terms are defined and reported on Internal Revenue Service tax return forms.

meet these ''exceptions'' to information blocking, such as with considering the size and resources of small entities when meeting security requirements to qualify for the ''promoting the security of electronic health information'' exception.

While health IT developers that pursue certification of their health IT under the Program represent a small segment of the overall information technology industry, we believe that many health IT developers impacted by the requirements in this final rule most likely fall under the North American Industry Classification System (NAICS) code 541511 ''Custom Computer Programming Services.'' [247] The SBA size standard associated with this NAICS code is set at $27.5 million annual receipts or less. There is enough data generally available to establish that between 75 percent and 90 percent of entities that are categorized under the NAICS code 541511 are under the SBA size standard. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification of their health IT under the Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it is difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not perfectly correlated to the size standard for NAICS code 541511, we do have information indicating that over 60 percent of health IT developers that have had Complete EHRs and/or Health IT Modules certified to the 2011 Edition had less than 51 employees (80 FR 62741).

We estimated that the requirements in this final rule will have effects on health IT developers, some of which may be small entities, that have certified health IT or are likely to pursue certification of their health IT under the Program. We believe, however, that we have finalized the minimum amount of requirements necessary to accomplish our primary policy goal of enhancing interoperability. Further, as discussed in section XIII.B of this RIA above, there are no appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this final rule because many of the provisions are derived directly from legislative mandates in the Cures Act. Additionally, we have attempted to offset some of the burden imposed on health IT developers in this final rule with cost saving provisions through deregulatory actions (*see* section III). Additionally, the Secretary certifies that this final rule will not have a significant impact on a substantial number of small entities.

[247] *https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2017.pdf.*

4. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a final rule that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has federalism implications. Nothing in this final rule imposes substantial direct compliance costs on State and local governments, preempts State law, or otherwise has federalism implications. We are not aware of any State laws or regulations that are contradicted or impeded by any of the provisions in this final rule.

5. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule that imposes unfunded mandates on State, local, and tribal governments or the private sector requiring spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory threshold is approximately $150 million. While the estimated potential cost effects of this final rule reach the statutory threshold, we do not believe this final rule imposes unfunded mandates on State, local, and tribal governments or the private sector.

OMB reviewed this final rule.

List of Subjects

45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and recordkeeping requirements, Public health, Security.

45 CFR Part 171

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health care provider, Health information exchange, Health information technology, Health information network, Health insurance, Health records, Hospitals, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter D, is amended as follows:

PART 170—HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

■ 1. The authority citation for part 170 continues to read as follows:

Authority: 42 U.S.C. 300jj–11; 42 U.S.C 300jj–14; 5 U.S.C. 553

■ 2. Revise § 170.101 to read as follows:

§ 170.101 Applicability.

The standards, implementation specifications, and certification criteria adopted in this part apply to Health IT Modules and the testing and certification of such Health IT Modules.

■ 3. Amend § 170.102 by:
■ a. Removing the definitions of ''2014 Edition Base EHR'' and ''2014 Edition EHR certification criteria'';
■ b. Revising paragraph (3) in the definition of ''2015 Edition Base EHR'';
■ c. Revising the definition of ''Common Clinical Data Set'';
■ d. Removing the definition of ''Complete EHR, 2014 Edition''; and
■ e. Adding in alphabetical order definitions for ''Electronic Health Information'', ''Fee'', ''Health information technology'', ''Interoperability'', and ''Interoperability element''.

The revisions and additions read as follows:

§ 170.102 Definitions.

* * * * *

2015 Edition Base EHR * * *

(3) Has been certified to the certification criteria adopted by the Secretary in—

(i) Section 170.315(a)(1), (2), or (3); (a)(5), (a)(9), (a)(14), (b)(1), (c)(1), (g)(7) and (9), and (h)(1) or (2);

(ii) Section 170.315(g)(8) or (10) until May 2, 2022; and

(iii) Section 170.315(g)(10) on and after May 2, 2022.

* * * * *

Common Clinical Data Set means the following data expressed, where indicated, according to the specified standard(s):

(1) Patient name.

(2) *Sex:* The standard specified in § 170.207(n)(1).

(3) Date of birth.

(4) *Race:*

(i) The standard specified in § 170.207(f)(2); and

(ii) The standard specified in § 170.207(f)(1) for each race identified in accordance § 170.207(f)(2).

(5) *Ethnicity:*

(i) The standard specified in § 170.207(f)(2); and

(ii) The standard specified in § 170.207(f)(1) for each ethnicity identified in accordance § 170.207(f)(2).

(6) *Preferred language:* The standard specified in § 170.207(g)(2).

(7) Smoking status.

(8) *Problems:* At a minimum, the standard specified in § 170.207(a)(4).

(9) *Medications:* At a minimum, the standard specified in § 170.207(d)(3).

(10) *Medication allergies:* At a minimum, the standard specified in § 170.207(d)(3).

(11) *Laboratory test(s):* At a minimum, the standard specified in § 170.207(c)(3).

(12) Laboratory value(s)/result(s).

(13) *Vital signs:*

(i) The patient's diastolic blood pressure, systolic blood pressure, body height, body weight, heart rate, respiratory rate, body temperature, pulse oximetry, and inhaled oxygen concentration must be exchanged in numerical values only; and

(ii) In accordance with the standard specified in § 170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in § 170.207(m)(1).

(iii) *Optional:* The patient's BMI percentile per age and sex for youth 2–20 years of age, weight for age per length and sex for children less than 3 years of age, and head occipital-frontal circumference for children less than 3 years of age must be recorded in numerical values only in accordance with the standard specified in § 170.207(c)(3) and with the associated applicable unit of measure for the vital sign measurement in the standard specified in § 170.207(m)(1). For BMI percentile per age and sex for youth 2–20 years of age and weight for age per length and sex for children less than 3 years of age, the reference range/scale or growth curve should be included as appropriate.

(14) *Procedures:*

(i) At a minimum, the version of the standard specified in § 170.207(a)(4) or § 170.207(b)(2); or

(ii) For technology primarily developed to record dental procedures, the standard specified in § 170.207(b)(3).

(iii) *Optional:* The standard specified in § 170.207(b)(4).

(15) Care team member(s).

(16) *Immunizations:* In accordance with, at a minimum, the standards specified in § 170.207(e)(3) and (4).

(17) Unique device identifier(s) for a patient's implantable device(s): In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4).

(18) *Assessment and plan of treatment:*

(i) In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or

(ii) In accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(19) *Goals:* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(20) *Health concerns:* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

* * * * *

Electronic health information (EHI) is defined as it is in § 171.102.

Fee is defined as it is in § 171.102 of this subchapter.

* * * * *

Health information technology means hardware, software, integrated technologies or related licenses, IP, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.

* * * * *

Interoperability is, with respect to health information technology, such health information technology that—

(1) Enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;

(2) Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and

(3) Does not constitute information blocking as defined in § 171.103 of this subchapter.

Interoperability element is defined as it is in § 171.102 of this subchapter.

* * * * *

§ 170.200 [Amended]

■ 4. Amend § 170.200 by removing the phrase ''Complete EHRs and''.

§ 170.202 [Amended]

■ 5. Amend § 170.202 by removing and reserving paragraph (a)(1).

§ 170.204 [Amended]

■ 6. Amend § 170.204 by removing and reserving paragraphs (b)(1) and (2) and removing paragraph (c).

■ 7. Amend § 170.205 by:

■ a. Removing and reserving paragraphs (a)(1) and (2);

■ b. Adding paragraphs (a)(5) and (b)(1);

■ c. Removing and reserving paragraphs (d)(3), (e)(3), and (h)(1);

■ d. Adding paragraph (h)(3);

■ e. Removing and reserving paragraphs (i)(1) and (j); and

■ f. Adding paragraph (k)(3).

The additions read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

(a) * * *

(5) *Standard.* HL7 CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 (incorporated by reference in § 170.299).

* * * * *

(b) * * *

(1) *Standard.* National Council for Prescription Drug Programs (NCPDP): SCRIPT Standard Implementation Guide; Version 2017071 (incorporated by reference in § 170.299).

* * * * *

(h) * * *

(3) *Standard.* CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2019 (incorporated by reference in § 170.299).

* * * * *

(k) * * *

(3) *Standard.* CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2019 (incorporated by reference in § 170.299).

* * * * *

§ 170.207 [Amended]

■ 8. Amend § 170.207 by removing and reserving paragraphs (d)(2), (e)(2), (g)(1), (h), and (j).

§ 170.210 [Amended]

■ 9. Amend § 170.210:

■ a. By removing and reserving paragraphs (a)(1) and (c)(1);

■ b. In paragraph (e)(1)(i), by removing the words ''7.2 through 7.4, 7.6, and 7.7'' and adding in their place ''7.1.1 through 7.1.3 and 7.1.6 through 7.1.9''; and

■ c. In paragraph (h), by removing the words ''ASTM E2147–01 (Reapproved 2013)'' and adding in their place ''ASTM E2147–18''.

■ 10. Add § 170.213 to read as follows:

§ 170.213 United States Core Data for Interoperability

Standard. United States Core Data for Interoperability (USCDI), Version 1 (v1) (incorporated by reference in § 170.299).

■ 11. Add § 170.215 to read as follows:

§ 170.215 Application Programming Interface Standards.

The Secretary adopts the following application programming interface (API) standards and associated implementation specifications:

(a)(1) *Standard.* HL7® Fast Healthcare Interoperability Resources (FHIR ®) Release 4.0.1 (incorporated by reference in § 170.299).

(2) *Implementation specification.* HL7 FHIR US Core Implementation Guide STU 3.1.0. (incorporated by reference in § 170.299).

(3) *Implementation specification.* HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for the ''SMART Core Capabilities'' (incorporated by reference in § 170.299).

(4) *Implementation specification.* FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1), including mandatory support for the ''group-export'' ''OperationDefinition'' (incorporated by reference in § 170.299).

(b) *Standard.* OpenID Connect Core 1.0, incorporating errata set 1 (incorporated by reference in § 170.299).

■ 12. Amend § 170.299 by:
■ a. Revising paragraph (c)(1);
■ b. Removing and reserving paragraphs (c)(2) and (3) and (d)(2), (7), and (8);
■ c. Adding paragraphs (e)(4) and (5);
■ d. Removing and reserving paragraphs (f)(3), (6), (7), (10), and (11);
■ e. Adding paragraphs (f)(30) through (34);
■ f. Removing and reserving paragraphs (h)(1) and (j)(1);
■ g. Adding paragraph (k)(3);
■ h. Removing and reserving paragraph (l)(3);
■ i. Adding paragraph (m)(5);
■ j. Redesignating paragraphs (n) through (r) as paragraphs (o) through (s), respectively;
■ k. Adding new paragraph (n); and
■ l. Removing and reserving newly redesignated paragraphs (r)(4) and (5).

The revision and additions read as follows:

§ 170.299 Incorporation by reference.

* * * * *

(c) * * *

(1) ASTM E2147–18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1, 2018, IBR approved for § 170.210(h).

* * * * *

(e) * * *

(4) CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting Implementation Guide for 2019; published May 4, 2018, IBR approved for § 170.205(h).

(5) CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2019; published October 8, 2018, IBR approved for § 170.205(k).

(f) * * *

(30) HL7® CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2–US Realm, October 2019, IBR approved for § 170.205(a).

(31) HL7 FHIR® Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1), August 22, 2019, IBR approved for § 170.215(a).

(32) HL7 FHIR SMART Application Launch Framework Implementation Guide Release 1.0.0, November 13, 2018, IBR approved for § 170.215(a).

(33) HL7 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, Version 4.0.1: R4, October 30, 2019, including Technical Correction #1, November 1, 2019, IBR approved for § 170.215(a).

(34) HL7 FHIR® US Core Implementation Guide STU3 Release 3.1.0, November 06, 2019, IBR approved for § 170.215(a).

* * * * *

(k) * * *

(3) SCRIPT Standard, Implementation Guide, Version 2017071 (Approval Date for ANSI: July 28, 2017), IBR approved for § 170.205(b).

* * * * *

(m) * * *

(5) United States Core Data for Interoperability (USCDI), Version 1, February 2020, IBR approved for § 170.213; available at *https://www.healthit.gov/USCDI.*

* * * * *

(n) OpenID Foundation, 2400 Camino Ramon, Suite 375, San Ramon, CA 94583, Telephone +1 925–275–6639, *http://openid.net/.*

(1) OpenID Connect Core 1.0 Incorporating errata set 1, November 8, 2014, IBR approved for § 170.215(b).

(2) [Reserved]

* * * * *

§ 170.300 [Amended]

■ 13. Amend § 170.300 in paragraphs (a) and (c) by removing the phrase ''Complete EHRs and''.

§ 170.314 [Removed and Reserved]

■ 14. Remove and reserve § 170.314.

■ 15. Amend § 170.315:
■ a. By removing and reserving paragraphs (a)(6) through (8);
■ b. In paragraph (a)(9)(ii)(B)(*1*)(*iii*) by removing ''medication allergy'' and adding in its place ''allergy and intolerance'';
■ c. In paragraph (a)(9)(ii)(B)(*2*) by removing ''medication allergies'' and adding in its place ''allergies and intolerance'';
■ d. By removing and reserving paragraph (a)(11);
■ e. In paragraphs (b)(1)(ii)(A) introductory text, (b)(1)(ii)(A)(*2*) and (*3*), (b)(1)(ii)(B), and (b)(1)(ii)(C) introductory text, by removing the reference ''§ 170.205(a)(3) and § 170.205(a)(4)'' and adding in its place the reference ''§ 170.205(a)(3), (4), and (5)'';
■ f. In paragraph (b)(1)(iii) introductory text, by removing the reference ''§ 170.205(a)(4)'' and adding in its place the reference ''§ 170.205(a)(3), (4), and (5)'';
■ g. By revising paragraphs (b)(1)(iii)(A) and (b)(2) and (3);
■ h. By removing and reserving paragraphs (b)(4) and (5);
■ i. By revising paragraphs (b)(7) through (9);
■ j. By adding paragraph (b)(10);
■ k. By revising paragraph (c)(3);
■ l. By adding paragraphs (d)(12) and (13);
■ m. By revising paragraphs (e)(1)(i)(A)(*1*) through (*5*);
■ n. By adding paragraphs (e)(1)(i)(A)(*6*) and (*7*)
■ o. In paragraph (e)(1)(i)(B)(*1*)(*ii*) and (e)(1)(i)(B)(*2*) introductory text, by removing the reference ''§ 170.205(a)(4)'' and adding in its place the reference ''§ 170.205(a)(4) and (5)'';
■ p. By removing and reserving paragraph (e)(1)(ii)(B);
■ q. By revising paragraphs (f)(5)(iii)(B)(*1*) through (*4*),
■ r. By adding paragraph (f)(5)(iii)(B)(*5*);
■ s. By revising paragraphs (g)(1) and (2), (g)(3)(i), and (g)(6)
■ t. By removing paragraphs (g)(7)(ii)(A)(*3*) and (g)(8)(ii)(A)(*3*);
■ u. By revising paragraph (g)(9)(i)(A);
■ v. By removing paragraph (g)(9)(ii)(A)(*3*); and
■ w. By adding paragraph (g)(10).

The revisions and additions read as follows:

§ 170.315 2015 Edition health IT certification criteria.

* * * * *

(b) * * *

(1) * * *

(iii) * * *

(A)(*1*) The data classes expressed in the standard in § 170.213 and in accordance with § 170.205(a)(4), (5), and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section, or

(*2*) The Common Clinical Data Set in accordance with § 170.205(a)(4) and paragraph (b)(1)(iii)(A)(*3*)(*i*) through (*iv*) of this section for the period until May 2, 2022, and

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4).

(2) *Clinical information reconciliation and incorporation*—(i) *General requirements.* Paragraphs (b)(2)(ii) and (iii) of this section must be completed based on the receipt of a transition of care/referral summary formatted in accordance with the standards adopted in § 170.205(a)(3) through (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates on and after May 2, 2022.

(ii) *Correct patient.* Upon receipt of a transition of care/referral summary formatted according to the standards adopted § 170.205(a)(3) through (5), technology must be able to demonstrate that the transition of care/referral summary received can be properly matched to the correct patient.

(iii) *Reconciliation.* Enable a user to reconcile the data that represent a patient's active medication list, allergies and intolerance list, and problem list as follows. For each list type:

(A) Simultaneously display (*i.e.,* in a single view) the data from at least two sources in a manner that allows a user to view the data and their attributes, which must include, at a minimum, the source and last modification date.

(B) Enable a user to create a single reconciled list of each of the following: Medications; Allergies and Intolerances; and problems.

(C) Enable a user to review and validate the accuracy of a final set of data.

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standard(s) on and after May 2, 2022:

(*1*) *Medications.* At a minimum, the version of the standard specified in § 170.213;

(*2*) *Allergies and intolerance.* At a minimum, the version of the standard specified in § 170.213; and

(*3*) *Problems.* At a minimum, the version of the standard specified in § 170.213.

(iv) *System verification.* Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document template and the standard specified in § 170.205(a)(5) on and after May 2, 2022.

(3) *Electronic prescribing.* (i) For technology certified prior to May 2, 2022, subject to the real world testing provisions at § 170.405(b)(5),

(A) Enable a user to perform the following prescription-related electronic transactions in accordance with, at a minimum, the version of the standard specified in § 170.207(d)(3) as follows:

(*1*) Create new prescriptions (NEWRX).

(*2*) Change prescriptions (RXCHG, CHGRES).

(*3*) Cancel prescriptions (CANRX, CANRES).

(*4*) Refill prescriptions (REFREQ, REFRES).

(*5*) Receive fill status notifications (RXFILL).

(*6*) Request and receive medication history information (RXHREQ, RXHRES).

(B) For each transaction listed in paragraph (b)(3)(i)(A) of this section, the technology must be able to receive and transmit the reason for the prescription using the diagnosis elements in the DRU Segment.

(C) *Optional:* For each transaction listed in paragraph (b)(3)(i)(A) of this section, the technology must be able to receive and transmit the reason for prescription using the indication elements in the SIG Segment.

(D) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.,* not cc).

(E) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

(ii) For technology certified subsequent to June 30, 2020:

(A) Enable a user to perform the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(1) and, at a minimum, the version of the standard specified in § 170.207(d)(3) as follows:

(*1*) Create new prescriptions (NewRx).

(*2*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*3*) Request and respond to cancel prescriptions (CancelRx, CancelRxResponse).

(*4*) Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(*5*) Receive fill status notifications (RxFill).

(*6*) Request and receive medication history (RxHistoryRequest, RxHistoryResponse).

(*7*) Relay acceptance of a transaction back to the sender (Status).

(*8*) Respond that there was a problem with the transaction (Error).

(*9*) Respond that a transaction requesting a return receipt has been received (Verify).

(B) Optionally, enable a user to perform the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(1) and, at a minimum, the version of the standard specified in § 170.207(d)(3) as follows:

(*1*) Create and respond to new prescriptions (NewRxRequest, NewRxResponseDenied).

(*2*) Receive fill status notifications (RxFillIndicator).

(*3*) Ask the Mailbox if there are any transactions (GetMessage).

(*4*) Request to send an additional supply of medication (Resupply).

(*5*) Communicate drug administration events (DrugAdministration).

(*6*) Request and respond to transfer one or more prescriptions between pharmacies (RxTransferRequest, RxTransferResponse, RxTransferConfirm).

(*7*) Recertify the continued administration of a medication order (Recertification).

(*8*) Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(*9*) Electronic prior authorization transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse).

(C) For the following prescription-related transactions, the technology must be able to receive and transmit the

reason for prescription using the diagnosis elements: <Diagnosis> <Primary> or <Secondary>:

(*1*) *Required transactions:*

(*i*) Create new prescriptions (NewRx).

(*ii*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*iii*) Cancel prescriptions (CancelRx).

(*iv*) Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(*v*) Receive fill status notifications (RxFill).

(*vi*) Receive medication history (RxHistoryResponse).

(*2*) *Optional transactions:*

(*i*) Request to send an additional supply of medication (Resupply)

(*ii*) Request and respond to transfer one or more prescriptions between pharmacies (RxTransferRequest, RxTransferResponse)

(*iii*) Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(*iv*) Electronic prior authorization (ePA) transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse and PACancelRequest, PACancelResponse).

(D) *Optional:* For each transaction listed in paragraph (b)(3)(ii)(C) of this section, the technology must be able to receive and transmit reason for prescription using the <IndicationforUse> element in the SIG segment.

(E) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (*i.e.,* not cc).

(F) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

* * * * *

(7) *Security tags—summary of care—send.* Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the:

(i) Document, section, and entry (data element) level; or

(ii) Document level for the period until May 2, 2022.

(8) *Security tags—summary of care—receive.* (i) Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the:

(A) Document, section, and entry (data element) level; or

(B) Document level for the period until May 2, 2022; and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

(9) *Care plan.* Enable a user to record, change, access, create, and receive care plan information in accordance with:

(i) The Care Plan document template, including the Health Status Evaluations and Outcomes Section and Interventions Section (V2), in the standard specified in § 170.205(a)(4); and

(ii) The standard in § 170.205(a)(5)) on and after May 2, 2022.

(10) *Electronic Health Information export*—(i) *Single patient electronic health information export.* (A) Enable a user to timely create an export file(s) with all of a single patient's electronic health information that can be stored at the time of certification by the product, of which the Health IT Module is a part.

(B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(C) Limit the ability of users who can create export file(s) in at least one of these two ways:

(*1*) To a specific set of identified users

(*2*) As a system administrative function.

(D) The export file(s) created must be electronic and in a computable format.

(E) The publicly accessible hyperlink of the export's format must be included with the exported file(s).

(ii) *Patient population electronic health information export.* Create an export of all the electronic health information that can be stored at the time of certification by the product, of which the Health IT Module is a part.

(A) The export created must be electronic and in a computable format.

(B) The publicly accessible hyperlink of the export's format must be included with the exported file(s).

(iii) *Documentation.* The export format(s) used to support paragraphs (b)(10)(i) and (ii) of this section must be kept up-to-date.

(c) * * *

(3) *Clinical quality measures—report.* Enable a user to electronically create a data file for transmission of clinical quality measurement data in accordance with the applicable implementation specifications specified by the CMS implementation guides for Quality Reporting Document Architecture (QRDA), category I, for inpatient measures in § 170.205(h)(3) and CMS implementation guide for QRDA, category III for ambulatory measures in § 170.205 (k)(3).

* * * * *

(d) * * *

(12) *Encrypt authentication credentials.* Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

(i) Yes—the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) No—the Health IT Module does not encrypt stored authentication credentials. When attesting ''no,'' the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

(13) *Multi-factor authentication.* Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

(i) Yes—the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting ''yes,'' the health IT developer must describe the use cases supported.

(ii) No—the Health IT Module does not support authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting ''no,'' the health IT developer may explain why the Health IT Module does not support authentication, through multiple elements, of the user's identify with the use of industry-recognized standards.

(e) * * *

(1) * * *

(i) * * *

(A) * * *

(*1*) The data classes expressed in the standards in § 170.213 (which should be in their English (*i.e.,* non-coded) representation if they associate with a vocabulary/code set), and in accordance with § 170.205(a)(4) and (a)(5), and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section, or

(*2*) The Common Clinical Data Set in accordance with § 170.205(a)(4) and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iv*) of this section for the period until May 2, 2022.

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or in accordance with the ''Assessment

Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standards specified in § 170.205(a)(4).

(*4*) Ambulatory setting only. Provider's name and office contact information.

(*5*) Inpatient setting only. Admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization.

(*6*) Laboratory test report(s). Laboratory test report(s), including:

(*i*) The information for a test report as specified all the data specified in 42 CFR 493.1291(c)(1) through (7);

(*ii*) The information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and

(*iii*) The information for corrected reports as specified in 42 CFR 493.1291(k)(2).

(*7*) Diagnostic image report(s).

* * * * *

(f) * * *

(5) * * *

(iii) * * *

(B) * * *

(*1*) The data classes expressed in the standards in § 170.213, and in accordance with § 170.205(a)(4) and (5), or

(*2*) The Common Clinical Data Set in accordance with § 170.205(a)(4) for the period until May 2, 2022.

(*3*) *Encounter diagnoses.* Formatted according to at least one of the following standards:

(*i*) The standard specified in § 170.207(i).

(*ii*) At a minimum, the version of the standard specified in § 170.207(a)(4).

(*4*) The provider's name, office contact information, and reason for visit.

(*5*) An identifier representing the row and version of the trigger table that triggered the case report.

* * * * *

(g) *Design and performance*—(1) *Automated numerator recording.* For each Promoting Interoperability Programs percentage-based measure, technology must be able to create a report or file that enables a user to review the patients or actions that would make the patient or action eligible to be included in the measure's numerator. The information in the report or file created must be of sufficient detail such that it enables a user to match those patients or actions to meet the measure's denominator limitations when necessary to generate an accurate percentage.

(2) *Automated measure calculation.* For each Promoting Interoperability Programs percentage-based measure that is supported by a capability included in a technology, record the numerator and denominator and create a report including the numerator, denominator, and resulting percentage associated with each applicable measure.

(3) * * *

(i) User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: Paragraphs (a)(1) through (5), (9), and (14), and (b)(2) and (3).

* * * * *

(6) *Consolidated CDA creation performance.* The following technical and performance outcomes must be demonstrated related to Consolidated CDA creation. The capabilities required under paragraphs (g)(6)(i) through (v) of this section can be demonstrated in tandem and do not need to be individually addressed in isolation or sequentially.

(i) This certification criterion's scope includes:

(A) The data classes expressed in the standard in § 170.213, and in accordance with § 170.205(a)(4) and (5) and paragraphs (g)(6)(i)(C)(*1*) through (*3*) of this section; or

(B) The Common Clinical Data Set in accordance with § 170.205(a)(4) and paragraphs (g)(6)(i)(C)(*1*) through (*4*) of this section for the period until May 2, 2022.

(C) The following data classes:

(*1*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(*2*) *Goals.* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4).

(*3*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4).

(*4*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standard specified in § 170.205(a)(4).

(ii) *Reference C–CDA match.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) and (5) that matches a gold-standard, reference data file.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) that matches a gold-standard, reference data file.

(iii) *Document-template conformance.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) and (5) that demonstrates a valid implementation of each document template applicable to the certification criterion or criteria within the scope of the certificate sought.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) that demonstrates a valid implementation of each document template applicable to the certification criterion or criteria within the scope of the certificate sought.

(iv) *Vocabulary conformance.* (A) For health IT certified to (g)(6)(i)(A) of this section, create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) and (5) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(B) For health IT certified to (g)(6)(i)(B) of this section, create a data file formatted in accordance with the standard adopted in § 170.205(a)(4) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(v) *Completeness verification.* Create a data file for each of the applicable document templates referenced in paragraph (g)(6)(iii) of this section without the omission of any of the data included in either paragraph (g)(6)(i)(A) or (B) of this section, as applicable.

* * * * *

(9) * * *

(i) * * *

(A)(*1*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iii*) of this section, or

(*2*) The Common Clinical Data Set in accordance with paragraphs (g)(9)(i)(A)(*3*)(*i*) through (*iv*) of this section for the period until May 2, 2022, and

(*3*) The following data classes:

(*i*) *Assessment and plan of treatment.* In accordance with the ''Assessment and Plan Section (V2)'' of the standards specified in § 170.205(a)(4); or in accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standards specified in § 170.205(a)(4).

(*ii*) *Goals.* In accordance with the ''Goals Section'' of the standards specified in § 170.205(a)(4).

(*iii*) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standards specified in § 170.205(a)(4).

(*iv*) *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the ''Product Instance'' in the ''Procedure Activity Procedure Section'' of the standards specified in § 170.205(a)(4).

* * * * *

(10) *Standardized API for patient and population services.* The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) *Data response.* (A) Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted in § 170.215(a)(2), including the mandatory capabilities described in ''US Core Server CapabilityStatement,'' for each of the data included in the standard adopted in § 170.213. All data elements indicated as ''mandatory'' and ''must support'' by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standard adopted in § 170.215(a)(1), and implementation specifications adopted in § 170.215(a)(2) and (4), for each of the data included in the standard adopted in § 170.213. All data elements indicated as ''mandatory'' and ''must support'' by the standards and implementation specifications must be supported.

(ii) *Supported search operations.* (A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(2), specifically the mandatory capabilities described in ''US Core Server CapabilityStatement.''

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) *Application registration.* Enable an application to register with the Health IT Module's ''authorization server.''

(iv) *Secure connection.* (A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(a)(2) and (3).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(a)(4).

(v) *Authentication and authorization*—(A) *Authentication and authorization for patient and user scopes*—(*1*) *First time connections*—(*i*) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b).

(*ii*) An application capable of storing a client secret must be issued a refresh token valid for a period of no less than three months.

(*2*) *Subsequent connections.* (*i*) Access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

(*ii*) An application capable of storing a client secret must be issued a new refresh token valid for a new period of no less than three months.

(B) *Authentication and authorization for system scopes.* Authentication and authorization must occur during the process of granting an application access to patient data in accordance with the ''SMART Backend Services: Authorization Guide'' section of the implementation specification adopted in § 170.215(a)(4) and the application must be issued a valid access token.

(vi) *Patient authorization revocation.* A Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction.

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued.

(viii) *Documentation.* (A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(*3*) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(B) The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

* * * * *

■ 16. Add subpart D to part 170 to read as follows:

Subpart D—Conditions and Maintenance of Certification Requirements for Health IT Developers

Sec.

Subpart D—Conditions and Maintenance of Certification Requirements for Health IT Developers

§ 170.400 Basis and scope.

This subpart implements section 3001(c)(5)(D) of the Public Health Service Act by setting forth certain Conditions and Maintenance of Certification requirements for health IT developers participating in the ONC Health IT Certification Program.

§ 170.401 Information blocking.

(a) *Condition of Certification requirement.* A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103 on or after November 2, 2020.

(b) [Reserved]

§ 170.402 Assurances.

(a) *Condition of Certification requirement.* (1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj–52 and § 171.103 on and after November 2, 2020, unless for legitimate purposes as specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.

(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.

(3) A health IT developer must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the full scope of the technology's certification.

(4) A health IT developer of a certified Health IT Module that is part of a heath IT product which electronically stores EHI must certify to the certification criterion in § 170.315(b)(10).

(b) *Maintenance of Certification requirements.* (1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:

(i) A period of 10 years beginning from the date a developer's Health IT Module(s) is first certified under the Program; or

(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.

(2)(i) Within 36 months of May 1, 2020, a health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10).

(ii) On and after 36 months from May 1, 2020, a health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10).

§ 170.403 Communications.

(a) *Condition of Certification requirements.* (1) A health IT developer may not prohibit or restrict any communication regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology.

(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.

(i) *Unqualified protection for certain communications.* A health IT developer must not prohibit or restrict any person or entity from communicating any information whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes:

(A) Making a disclosure required by law;

(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;

(C) Communicating information about cybersecurity threats and incidents to government agencies;

(D) Communicating information about information blocking and other unlawful practices to government agencies; or

(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification requirement, or with any other requirement of this part, to ONC or an ONC–ACB.

(ii) *Permitted prohibitions and restrictions.* For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (E) of this section.

(A) *Developer employees and contractors.* (*1*) A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

(*2*) A self-developer must not prohibit or restrict communications of users of their health IT who are also employees or contractors.

(B) *Non-user-facing aspects of health IT.* A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

(C) *Intellectual property.* A health IT developer may prohibit or restrict communications that involve the use or disclosure of intellectual property existing in the developer's health IT (including third-party intellectual property), provided that any prohibition or restriction imposed by a developer must be no broader than necessary to protect the developer's legitimate intellectual property interests and consistent with all other requirements of paragraph (a)(2)(ii) of this section. A restriction or prohibition is deemed broader than necessary and inconsistent with the requirements of paragraph (a)(2)(ii) of this section if it would restrict or preclude a public display of a portion of a work subject to copyright protection (without regard to whether the copyright is registered) that would reasonably constitute a ''fair use'' of that work.

(D) *Screenshots and video.* A health IT developer may require persons who communicate screenshots or video to—

(*1*) Not alter the screenshots or video, except to annotate the screenshots or video or resize the screenshots or video;

(*2*) Limit the sharing of screenshots to the relevant number of screenshots needed to communicate about the health IT regarding one or more of the six subject areas in paragraph (a)(1) of this section; and

(*3*) Limit the sharing of video to:

(*i*) The relevant amount of video needed to communicate about the health IT regarding one or more of the six subject areas in paragraph (a)(1) of this section; and

(*ii*) Only videos that address temporal matters that cannot be communicated through screenshots or other forms of communication.

(E) *Pre-market testing and development.* A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.

(b) *Maintenance of Certification requirements*—(1) *Notice.* Health IT developers must issue a written notice to all customers and those with which it has contracts or agreements containing provisions that contravene paragraph (a) of this section annually, beginning in calendar year 2020, until

paragraph (b)(2)(ii) of this section is fulfilled, stating that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(2) *Contracts and agreements.* (i) A health IT developer must not establish, renew, or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence as of November 2, 2020, that contravenes paragraph (a) of this section, then the developer must amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section whenever the contract is next modified for other reasons or renewed.

(c) *Communication, defined.* ''Communication'' as used in this section means any communication, irrespective of the form or medium. The term includes visual communications, such as screenshots and video.

§ 170.404 Application programming interfaces.

The following Condition and Maintenance of Certification requirements apply to developers of Health IT Modules certified to any of the certification criteria adopted in § 170.315(g)(7) through (10).

(a) *Condition of certification requirements*—(1) *General.* A Certified API Developer must publish APIs and allow electronic health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) *Transparency conditions*—(i) *Complete business and technical documentation.* A Certified API Developer must publish complete business and technical documentation, including the documentation described in paragraph (a)(2)(ii) of this section, via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(ii) *Terms and conditions*—(A) *Material information.* A Certified API Developer must publish all terms and conditions for its certified API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be:

(*1*) Needed to develop software applications to interact with the certified API technology;

(*2*) Needed to distribute, deploy, and enable the use of software applications in production environments that use the certified API technology;

(*3*) Needed to use software applications, including to access, exchange, and use electronic health information by means of the certified API technology;

(*4*) Needed to use any electronic health information obtained by means of the certified API technology;

(*5*) Used to verify the authenticity of API Users; and

(*6*) Used to register software applications.

(B) *API fees.* Any and all fees charged by a Certified API Developer for the use of its certified API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(*1*) The persons or classes of persons to whom the fee applies;

(*2*) The circumstances in which the fee applies; and

(*3*) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

(3) *Fees conditions*—(i) *General conditions*—(A) *All fees.* All fees related to certified API technology not otherwise permitted by this section are prohibited from being imposed by a Certified API Developer. The permitted fees in paragraphs (a)(3)(ii) and (iv) of this section may include fees that result in a reasonable profit margin in accordance with § 171.302.

(B) *Permitted fees requirements.* For all permitted fees, a Certified API Developer must:

(*1*) Ensure that such fees are based on objective and verifiable criteria that are uniformly applied to all similarly situated API Information Sources and API Users;

(*2*) Ensure that such fees imposed on API Information Sources are reasonably related to the Certified API Developer's costs to supply certified API technology to, and if applicable, support certified API technology for, API Information Sources;

(*3*) Ensure that such fees to supply and, if applicable, support certified API technology are reasonably allocated among all similarly situated API Information Sources; and

(*4*) Ensure that such fees are not based on whether API Information Sources or API Users are competitors, potential competitors, or will be using the certified API technology in a way that facilitates competition with the Certified API Developer.

(C) *Prohibited fees.* A Certified API Developer is prohibited from charging fees for the following:

(*1*) Costs associated with intangible assets other than actual development or acquisition costs of such assets;

(*2*) Opportunity costs unrelated to the access, exchange, or use of electronic health information; and

(*3*) The permitted fees in this section cannot include any costs that led to the creation of intellectual property if the actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.

(D) *Record-keeping requirements.* A Certified API Developer must keep for inspection detailed records of any fees charged with respect to the certified API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(ii) *Permitted fee—development, deployment, and upgrades.* A Certified API Developer is permitted to charge fees to an API Information Source to recover the costs reasonably incurred by the Certified API Developer to develop, deploy, and upgrade certified API technology.

(iii) *Permitted fee—recovering API usage costs.* A Certified API Developer is permitted to charge fees to an API Information Source related to the use of certified API technology. The fees must be limited to the recovery of incremental costs reasonably incurred by the Certified API Developer when it hosts certified API technology on behalf of the API Information Source.

(iv) *Permitted fee—value-added services.* A Certified API Developer is permitted to charge fees to an API User for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.

(4) *Openness and pro-competitive conditions; general condition.* A Certified API Developer must grant an API Information Source the independent ability to permit an API User to interact with the certified API technology deployed by the API Information Source.

(*i*) *Non-discrimination.* (A) A Certified API Developer must provide certified API technology to an API Information Source on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

(B) The terms on which a Certified API Developer provides certified API technology must be based on objective and verifiable criteria that are uniformly applied to all substantially similar or similarly situated classes of persons and requests.

(C) A Certified API Developer must not offer different terms or services based on:

(*1*) Whether a competitive relationship exists or would be created;

(*2*) The revenue or other value that another party may receive from using the API technology.

(ii) *Rights to access and use certified API technology*—(A) *Rights that must be granted.* A Certified API Developer must have and, upon request, must grant to API Information Sources and API Users all rights that may be reasonably necessary to:

(*1*) Access and use the Certified API Developer's certified API technology in a production environment;

(*2*) Develop products and services that are designed to interact with the Certified API Developer's certified API technology; and

(*3*) Market, offer, and distribute products and services associated with the Certified API Developer's certified API technology.

(B) *Prohibited conduct.* A Certified API Developer is prohibited from conditioning the receipt of the rights described in paragraph (a)(4)(ii)(A) of this section on:

(*1*) Receiving a fee, including but not limited to a license fee, royalty, or revenue-sharing arrangement;

(*2*) Agreeing to not compete with the Certified API Developer in any product, service, or market;

(*3*) Agreeing to deal exclusively with the Certified API Developer in any product, service, or market;

(*4*) Obtaining additional licenses, products, or services that are not related to or can be unbundled from the certified API technology;

(*5*) Licensing, granting, assigning, or transferring any intellectual property to the Certified API Developer;

(*6*) Meeting any Certified API Developer-specific testing or certification requirements; and.

(*7*) Providing the Certified API Developer or its technology with reciprocal access to application data.

(iii) *Service and support obligations.* A Certified API Developer must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of certified API technology by API Information Sources and API Users in production environments.

(A) *Changes and updates to* certified *API technology.* A Certified API Developer must make reasonable efforts to maintain the compatibility of its certified API technology and to otherwise avoid disrupting the use of certified API technology in production environments.

(B) *Changes to terms and conditions.* Except as exigent circumstances require, prior to making changes to its certified API technology or to the terms and conditions thereof, a Certified API Developer must provide notice and a reasonable opportunity for API Information Sources and API Users to update their applications to preserve compatibility with certified API technology and to comply with applicable terms and conditions.

(b) *Maintenance of certification requirements*—(1) *Authenticity verification and registration for production use.* The following apply to a Certified API Developer with a Health IT Module certified to the certification criterion adopted in § 170.315(g)(10):

(i) *Authenticity verification.* A Certified API Developer is permitted to institute a process to verify the authenticity of API Users so long as such process is objective and the same for all API Users and completed within ten business days of receipt of an API User's request to register their software application for use with the Certified API Developer's Health IT Module certified to § 170.315(g)(10).

(ii) *Registration for production use.* A Certified API Developer must register and enable all applications for production use within five business days of completing its verification of an API User's authenticity, pursuant to paragraph (b)(1)(i) of this section.

(2) *Service base URL publication.* A Certified API Developer must publish the service base URLs for all Health IT Modules certified to § 170.315(g)(10) that can be used by patients to access their electronic health information. The Certified API Developer must publicly publish the service base URLs:

(i) For all of its customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source; and

(ii) In a machine-readable format at no charge.

(3) *Rollout of (g)(10)-certified APIs.* A Certified API Developer with certified API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Information Sources with such certified API technology deployed with certified API technology certified to the certification criterion in § 170.315(g)(10) by no later than May 2, 2022.

(4) *Compliance for existing certified API technology.* By no later than November 2, 2020, a Certified API Developer with Health IT Module(s) certified to the certification criteria in § 170.315(g)(7), (8), or (9) must comply with paragraph (a) of this section, including revisions to their existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(c) *Definitions.* The following definitions apply to this section:

API Information Source means an organization that deploys certified API technology created by a ''Certified API Developer;''

API User means a person or entity that creates or uses software applications that interact with the ''certified API technology'' developed by a ''Certified API Developer'' and deployed by an ''API Information Source;''

Certified API Developer means a health IT developer that creates the ''certified API technology'' that is certified to any of the certification criteria adopted in § 170.315(g)(7) through (10); and

Certified API technology means the capabilities of Health IT Modules that are certified to any of the API-focused certification criteria adopted in § 170.315(g)(7) through (10).

§ 170.405 Real world testing.

(a) *Condition of Certification requirement.* A health IT developer with Health IT Module(s) certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b) *Maintenance of Certification requirements*—(1) *Real world testing plan submission.* A health IT developer with Health IT Module(s) certified to any one or more of the criteria referenced in paragraph (a) of this section must submit to its ONC–ACB an annual real world testing plan addressing each of those certified Health IT Modules by a date determined by the ONC–ACB that enables the ONC–ACB to publish a publicly available hyperlink to the plan on CHPL no later than December 15 of each calendar year.

(i) The plan must be approved by a health IT developer authorized representative capable of binding the

health IT developer for execution of the plan and include the representative's contact information.

(ii) The plan must include all health IT certified to any one or more of the criteria referenced in paragraph (a) of this section as of August 31 of the year in which the plan is submitted, and address the real world testing to be conducted in the calendar year immediately following plan submission.

(iii) The plan must address the following for each of the certification criteria identified in paragraph (a) of this section that are included in each Health IT Module's scope of certification:

(A) The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability and conformance to the full scope of the certification criterion's requirements, including scenario- and use case-focused testing;

(B) The care setting(s) that will be tested for real world interoperability and an explanation for the health IT developer's choice of care setting(s) to test;

(C) For any standards and implementation specifications referenced by the criterion that the developer has chosen to certify to National Coordinator-approved newer versions pursuant to paragraph (b)(8) or (9) of this section, a description of how the developer will test and demonstrate conformance to all requirements of the criterion using all versions of the adopted standards to which each Health IT Module was certified as of August 31 of the year in which the real world testing plan is due.

(D) A schedule of key real world testing milestones;

(E) A description of the expected outcomes of real world testing;

(F) At least one measurement/metric associated with the real world testing; and

(G) A justification for the health IT developer's real world testing approach.

(2) *Real world testing results reporting.* (i) If in the course of conducting real world testing the developer discovers one or more non-conformities with the full scope of any certification criterion under the Program, the developer must report that non-conformity to the ONC–ACB within 30 days.

(ii) For real world testing activities conducted during the immediately preceding calendar year, a health IT developer must submit to its ONC–ACB an annual real world testing results report addressing each of its certified Health IT Modules that include certification criteria referenced in paragraph (a) of this section by a date determined by the ONC–ACB that enables the ONC–ACB to publish a publicly available hyperlink to the results report on CHPL no later than March 15 of each calendar year. The real world testing results must report the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

(A) The method(s) that was used to demonstrate real world interoperability;

(B) The care setting(s) that was tested for real world interoperability;

(C) The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process;

(D) A list of the key milestones met during real world testing;

(E) The outcomes of real world testing including a description of any challenges encountered during real world testing; and

(F) At least one measurement/metric associated with the real world testing.

(3) *USCDI Updates for C–CDA.* A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (e)(1), (g)(6), (f)(5), and/or (g)(9) on May 1, 2020, must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(3)(i) of this section by May 2, 2022.

(4) *C–CDA Companion Guide Updates.* A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (b)(9), (e)(1), (g)(6), and/or (g)(9) prior to May 1, 2020, must:

(i) Update their certified health IT to be compliant with the revised versions of the Program criteria in the 2015 Edition; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(4)(i) of this section by May 2, 2022.

(5) *Electronic prescribing.* A health IT developer with health IT certified to § 170.315(b)(3) prior to November 2, 2020, must:

(i) Update their certified health IT to be compliant with the revised versions of this criteria adopted in § 170.315(b)(3)(ii); and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(5)(i) of this section by May 2, 2022

(6) *Security tags.* A health IT developer with health IT certified to § 170.315(b)(7) and/or § 170.315(b)(8) prior to May 1, 2020, must:

(i) Update their certified health IT to be compliant with the revised versions of the criteria adopted in § 170.315(b)(7) and/or the revised versions of the criteria adopted in § 170.315(b)(8); and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(6)(i) of this section by May 2, 2022.

(7) *ASTM updates.* A health IT developer with health IT certified to § 170.315(d)(2), (3), and/or (d)(10) prior to May 1, 2020, must:

(i) Update their certified health IT to be compliant with § 170.210(e)(1) and the standard specified in § 170.210(h); and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(7)(i) of this section by May 2, 2022.

(8) *Standards Version Advancement Process—voluntary updates of certified health IT to newer versions of standards and implementation specifications.* A health IT developer subject to this paragraph (b) is permitted to update Health IT Module(s) certified to any one or more of the certification criteria referenced in paragraph (a) of this section to a newer version of any adopted standard or implementation specification included in the criterion, provided that newer version is approved by the National Coordinator for use in certifications issued under the ONC Health IT Certification Program. A developer that pursues such updates to its certified Health IT Module(s) must:

(i) Provide advance notice to all affected customers and its ONC–ACB—

(A) Expressing its intent to update the certified Health IT Module(s) to the National Coordinator-approved advanced version of the standard implementation specification;

(B) The developer's expectations for how the update(s) will affect real world interoperability for the Health IT Module(s);

(C) Whether the developer intends to continue to support the certificate(s) for the existing certified Health IT Module(s) version(s) for some period of time and how long or if the existing certified Health IT Module(s) version(s) will be deprecated; and

(ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in each certification criterion under which the developer chooses to update its certified Health IT Module(s).

(iii) Maintain the updated certified Health IT Module(s) in full conformance

with all applicable Program requirements.

(9) *Standards Version Advancement Process—voluntary certification to newer versions of standards and implementation specifications.* A Health IT developer is permitted to seek certification for its Health IT Module(s) to any one or more of the certification criteria referenced in paragraph (a) of this section using a newer version of any adopted standard(s) or implementation specification(s) included in the criterion without first obtaining certification to the version of that adopted standard or implementation specification that is incorporated by reference in § 170.299, provided that the newer version is approved by the National Coordinator for use in certifications issued under the ONC Health IT Certification Program. Developers may, for each standard and implementation specification included in each criterion, choose on an itemized basis whether to seek certification to the version incorporated by reference in § 170.299, or to one or more newer version(s) approved by the National Coordinator for use in Health IT Module certifications issued pursuant to section 3001(c)(5) of the Public Health Service Act, or to both.

§ 170.406 Attestations.

(a) *Condition of Certification requirement.* A health IT developer, or its authorized representative that is capable of binding the health IT developer, must provide the Secretary an attestation of compliance with the following Conditions and Maintenance of Certification requirements:

(1) Section 170.401;

(2) Section 170.402, but only for § 170.402(a)(4) and (b)(2) if the health IT developer certified a Health IT Module(s) that is part of a health IT product which can store electronic health information;

(3) Section 170.403;

(4) Section 170.404 if the health IT developer has a Health IT Module(s) certified to any of the certification criteria adopted in § 170.315(g)(7) through (10); and such health IT developer must also ensure that health IT allows for health information to be exchanged, accessed, and used, in the manner described in § 170.404; and

(5) Section 170.405 if a health IT developer has a Health IT Module(s) certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h).

(b) *Maintenance of Certification requirement.* (1) A health IT developer, or its authorized representative that is capable of binding the health IT developer, must provide the attestation specified in paragraph (a) of this section semiannually for any Health IT Modules that have or have had an active certification at any time under the ONC Health IT Certification Program during the prior six months.

(2) [Reserved].

Subpart E—ONC Health IT Certification Program

§ 170.501 [Amended]

■ 17. Amend § 170.501:

■ a. In paragraph (a), by removing the phrase ''Complete EHRs,'';

■ b. In paragraph (b), by removing the phrase ''Complete EHRs and''; and

■ c. By removing and reserving paragraph (c).

§ 170.502 [Amended]

■ 18. Amend § 170.502:

■ a. In the definition of ''Deployment site'', by removing the phrase ''Complete EHR,'';

■ b. In the definition of ''Development site'', by removing the phrase ''Complete EHR,'';

■ c. In the introductory text to the definition of ''Gap certification'', by removing the phrase ''Complete EHR or'';

■ d. By removing the definition of ''ONC-Approved Accreditor or ONC–AA'';

■ e. In the definition of ''ONC-Authorized Certification Body or ONC–ACB'', by removing the phrase ''Complete EHRs,''; and

■ f. In the definition of ''ONC-Authorized Testing Lab or ONC–ATL,'' by removing the phrase ''Complete EHRs and''.

§§ 170.503 and 170.504 [Removed and Reserved]

■ 19. Remove and reserve §§ 170.503 and 170.504.

■ 20. Revise § 170.505 to read as follows:

§ 170.505 Correspondence.

(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified.

(1) Consideration for providing notice beyond email, such as by regular, express, or certified mail, will be based on, but not limited to, whether: The party requests use of correspondence beyond email; the party has responded via email to our communications; we have sufficient information from the party to ensure appropriate delivery of any other method of notice; and the matter involves an alleged violation within ONC's purview under § 170.580 that indicates a serious violation under the ONC Health IT Certification Program with potential consequences of suspension, certification termination, or a certification ban.

(2) The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC–ACB status, an applicant for ONC–ATL status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.

(b) In circumstances where it is necessary for an applicant for ONC–ACB status, an applicant for ONC–ATL status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the official date of receipt for all parties will be the date of the delivery confirmation to the address on record.

§ 170.510 [Amended]

■ 21. Amend § 170.510 by removing paragraph (a) and redesignating paragraphs (b) and (c) as paragraphs (a) and (b).

■ 22. Amend § 170.520 by revising paragraph (a)(3) to read as follows:

§ 170.520 Application.

(a) * * *

(3) Documentation that confirms that the applicant has been accredited to ISO/IEC 17065 (for availability, see § 170.599), with an appropriate scope, by any accreditation body that is a signatory to the Multilateral Recognition Arrangement (MLA) with the International Accreditation Forum (IAF).

* * * * *

■ 23. Amend § 170.523:

■ a. By revising paragraph (a);

■ b. By adding subject headings to paragraphs (b), (c), (d) introductory text, and (e);

■ c. In paragraph (f) introductory text, by adding a subject heading and removing the phrase, ''Complete EHRs,'' and;

■ d. By removing and reserving paragraph (f)(2);

■ e. Revising paragraphs (g) and (h);

■ f. Adding subject headings to paragraphs (i) introductory text and (j) introductory text;

■ g. In paragraph (k) introductory text, by adding a subject heading and removing the phrase ''Complete EHRs and'';

■ h. In paragraph (k)(1), by removing the phrase ''Complete EHR or'';

■ i. By revising paragraphs (k)(1)(ii) and (iii);
■ j. By removing and reserving paragraphs (k)(1)(iv)(B) and (C) and (k)(2) and (3);
■ k. By revising paragraph (k)(4);
■ l. By adding a subject heading to paragraph (l);
■ m. By revising paragraph (m);
■ n. In paragraph (o), by adding a subject heading and removing the phrase ''Complete EHR or''; and
■ o. By adding paragraphs (p) through (t).

The revisions and additions read as follows:

§ 170.523 Principles of proper conduct for ONC–ACBs.

* * * * *

(a) *Accreditation.* Maintain its accreditation in good standing to ISO/IEC 17065 (incorporated by reference in § 170.599).

(b) *Mandatory training.* * * *

* * * * *

(c) *Training program.* * * *

* * * * *

(d) *Reporting.* * * *

* * * * *

(e) *Onsite observation.* * * *

(f) *Certified product listing.* * * *

* * * * *

(g) *Records retention.* (1) Retain all records related to the certification of Complete EHRs and Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (g)(1) of this section;

(h) *Certification decision.* Only certify Health IT Modules that have been:

(1) Tested, using test tools and test procedures approved by the National Coordinator, by an:

(i) ONC–ATL;

(ii) ONC–ATL, National Voluntary Laboratory Accreditation Program-accredited testing laboratory under the ONC Health IT Certification Program, and/or an ONC–ATCB for the purposes of performing gap certification; or

(2) Evaluated by it for compliance with a conformance method approved by the National Coordinator.

(i) *Surveillance.* * * *

* * * * *

(j) *Refunds.* * * *

* * * * *

(k) *Disclosures.* * * *

(1) * * *

(ii) For a Health IT Module certified to the 2015 Edition health IT certification criteria, the information specified by paragraphs (f)(1)(i), (vi) through (viii), (xv), and (xvi) of this section as applicable for the specific Health IT Module.

(iii) In plain language, a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities, whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification. The additional types of costs or fees required to be disclosed include but are not limited to costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

* * * * *

(4) A certification issued to a Health IT Module based solely on the applicable certification criteria adopted by the ONC Health IT Certification Program must be separate and distinct from any other certification(s) based on other criteria or requirements.

(l) *Certification and Design Mark.*

* * *

(m) *Adaptations and updates.* On a quarterly basis each calendar year, obtain a record of:

(1) All adaptations of certified Health IT Modules;

(2) All updates made to certified Health IT Modules affecting the capabilities in certification criteria to which the ''safety-enhanced design'' criteria apply;

(3) All uses cases for § 170.315(d)(13);

(4) All updates made to certified Health IT Modules in compliance with § 170.405(b)(3); and

(5) All updates to certified Health IT Modules and all certifications of Health IT Modules issued including voluntary use of newer standards versions per § 170.405(b)(8) or (9). Record of these updates may be obtained by aggregation of ONC–ACB documentation of certification activity.

* * * * *

(o) *Scope reduction.* * * *

(p) *Real world testing.* (1) Review and confirm that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1).

(2) Review and confirm that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2).

(3) Submit real world testing plans by December 15 of each calendar year and results by March 15 of each calendar year to ONC for public availability.

(q) *Attestations.* Review and submit health IT developer Conditions and Maintenance of Certification requirements attestations made in accordance with § 170.406 to ONC for public availability.

(r) *Test results from ONC–ATLs.* Accept test results from any ONC–ATL that is:

(1) In good standing under the ONC Health IT Certification Program, and

(2) Compliant with its ISO/IEC 17025 accreditation requirements as required by 170.524(a).

(s) *Information for direct review.* Report to ONC, no later than a week after becoming aware of, any information that could inform whether ONC should exercise direct review under § 170.580(a).

(t) *Health IT Module voluntary standards and implementation specifications updates notices.* Ensure health IT developers opting to take advantage of the flexibility for voluntary updates of standards and implementation specifications in certified Health IT Modules per § 170.405(b)(8) provide timely advance written notice to the ONC–ACB and all affected customers.

(1) Maintain a record of the date of issuance and the content of developers' § 170.405(b)(8) notices; and

(2) Timely post content or make publicly accessible via the CHPL each § 170.405(b)(8) notice received, publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies.

■ 24. Amend § 170.524:
■ a. By adding subject headings to paragraphs (a) through (c), (d) introductory text, and (e);
■ b. By revising paragraph (f);
■ c. By adding a subject heading to paragraph (g) and paragraph (h) introductory text; and
■ d. In paragraph (h)(3), by removing the phrase ''Complete EHRs and/or''.

The additions and revisions read as follows:

§ 170.524 Principles of proper conduct for ONC–ATLs.

* * * * *

(a) *Accreditation.* * * *
(b) *Mandatory training.* * * *
(c) *Training program.* * * *
(d) *Reporting.* * * *
* * * * *
(e) *Onsite observation.* * * *
(f) *Records retention.* (1) Retain all records related to the testing of Complete EHRs and/or Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of three years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (f)(1) of this section;

(g) *Approved testing methods.* * * *
(h) *Refunds.* * * *
* * * * *

§ 170.545 [Removed and Reserved]

■ 25. Remove and reserve § 170.545.
■ 26. Amend § 170.550 by:
■ a. Adding subject headings to paragraphs (a),(b), and (d), and adding paragraph (e);
■ b. Removing and reserving paragraph (f);
■ c. Adding a subject heading to paragraph (g) introductory text and adding paragraph (g)(5);
■ d. Revising paragraph (h); and
■ e. Adding paragraphs (l) and (m).

The additions and revisions read as follows:

§ 170.550 Health IT Module certification.

(a) *Certification scope.* * * *
(b) *Health IT product scope options.* * * *
* * * * *
(d) *Upgrades and enhancements.* * * *
(e) *Standards updates.* ONC–ACBs must provide an option for certification of Health IT Modules consistent with § 171.405(b)(7) or (8) to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification.
* * * * *
(g) *Health IT module dependent criteria.* * * *

(5) Section 170.315(b)(10) when a health IT developer presents a Health IT Module for certification that can store electronic health information at the time of certification by the product, of which the Health IT Module is a part.

(h) *Privacy and security certification framework*—(1) *General rule.* When certifying a Health IT Module to the 2015 Edition health IT certification criteria, an ONC–ACB can only issue a certification to a Health IT Module if the privacy and security certification criteria in paragraphs (h)(3)(i) through (ix) of this section have also been met (and are included within the scope of the certification).

(2) *Testing.* In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion in paragraphs (h)(3)(i) through (ix) of this section so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification, except for the following:

(i) A Health IT Module presented for certification to § 170.315(e)(1) must be separately tested to § 170.315(d)(9); and

(ii) A Health IT Module presented for certification to § 170.315(e)(2) must be separately tested to § 170.315(d)(9).

(3) *Applicability.* (i) Section 170.315(a)(1) through (3), (5), (12), (14), and (15) are also certified to the certification criteria specified in § 170.315(d)(1) through (7), (d)(12), and (13).

(ii) Section 170.315(a)(4), (9), (10), and (13) are also certified to the certification criteria specified in § 170.315(d)(1) through (3), and (d)(5) through (7), (d)(12), and (13).

(iii) Section 170.315(b)(1) through (3) and (6) through (9) are also certified to the certification criteria specified in § 170.315(d)(1) through (3) and (d)(5) through (8), (12), and (13);

(iv) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A), (B), (d)(2)(ii) through (v), (d)(3), (5), (12), and (13);

(v) Section 170.315(e)(1) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5), (7), (9), (12), and (13);

(vi) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), (d)(3), (5), (9), (12), and (13);

(vii) Section 170.315(f) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (7), (12), and (13);

(viii) Section 170.315(g)(7) through (10) is also certified to the certification criteria specified in § 170.315(d)(1), (9), (12), and (13); and (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), or (d)(10);

(ix) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), (d)(3), (12), and (13); and
* * * * *

(l) *Conditions of certification attestations.* Ensure that the health IT developer of the Health IT Module has met its responsibilities under subpart D of this part.

(m) *Time-limited certification and certification status for certain 2015 Edition certification criteria.* An ONC–ACB may only issue a certification to a Health IT Module and permit continued certified status for:

(1) Section 170.315(a)(10) and (13) and § 170.315(e)(2) until January 1, 2022.

(2) Section 170.315(b)(6) until May 1, 2023.

(3) Section 170.315(g)(8) until May 2, 2022.

■ 27. Amend § 170.555:
■ a. In paragraph (a) by removing the words ''Complete EHRs and/or''; and
■ b. By revising paragraph (b)(1).

The revision reads as follows:

§ 170.555 Certification to newer versions of certain standards.

* * * * *
(b) * * *

(1) ONC–ACBs are not required to certify Health IT Module(s) according to newer versions of standards adopted and named in subpart B of this part, unless:

(i) The National Coordinator approves a newer version for use in certification and a health IT developer voluntarily elects to seek certification of its health IT in accordance with § 170.405(b)(9) or update its certified health IT to the newer version in accordance with § 170.405(b)(8); or

(ii) The new version is incorporated by reference in § 170.299.
* * * * *

■ 28. Amend § 170.556:
■ a. By removing the phrases ''certified Complete EHR or'' and ''Complete EHR or'', wherever they occur;
■ b. By revising paragraph (a) introductory text and paragraph (c) introductory text;
■ c. By removing and reserving paragraph (c)(2);
■ d. In paragraph (c)(3), by removing the phrase ''certified Complete EHRs''; and
■ e. By removing paragraphs (c)(5) and (6).

The revisions read as follows:

§ 170.556 In-the-field surveillance and maintenance of certification for Health IT.

(a) *In-the-field surveillance.* Consistent with its accreditation under 170.523(a) to ISO/IEC 17065 and the requirements of this subpart, an ONC–

ACB must initiate surveillance ''in the field'' as necessary to assess whether a certified Health IT Module continues to conform to the requirements in subparts A, B, C and E of this part once the certified Health IT Module has been implemented and is in use in a production environment.

* * * * *

(c) *Randomized surveillance.* During each calendar year surveillance period, an ONC–ACB may conduct in-the-field surveillance for certain randomly selected Health IT Modules to which it has issued a certification.

* * * * *

§§ 170.560, 170.565, and 170.570 [Amended]

■ 29. In the table below, for each section and paragraph indicated in the first two columns, remove the phrase indicated in the third column:

Section	Paragraphs	Remove
§ 170.560	(a)(2)	''Complete EHRs and/or''
§ 170.565	(d)(1)(ii) and (iii)	''Complete EHRs or''
§ 170.565	(h)(2)(iii)	''Complete EHRs and''
§ 170.570	(a), (b)(2), (c) introductory text, and (c)(1) and (2)	''Complete EHRs and/or''

§ 170.575 [Removed and Reserved]

■ 30. Remove and reserve § 170.575.

■ 31. Amend § 170.580:

■ a. By revising paragraph (a)(1) and the subject headings to paragraphs (a)(2)(i) and(ii);

■ b. By adding paragraph (a)(2)(iii);

■ c. By revising paragraphs (a)(3)(i), (iv), and (v);

■ d. By adding paragraph (a)(4);

■ e. By revising paragraphs (b)(1)(i) and (b)(1)(iii)(D), (b)(2)(i), and (b)(3)(i) and (ii);

■ f. By adding paragraphs (b)(3)(iii) and (iv);

■ g. By revising paragraph (c)(1);

■ h. In paragraphs (d)(1), (d)(2)(i)(C), and (d)(4), by removing the phrase ''Complete EHR or'';

■ i. In paragraph (d)(5), by removing the phrase ''Complete EHRs or'';

■ j. By revising paragraphs (e)(1) introductory text and (f)(1);

■ k. In paragraph (f)(2)(i)(C), by removing the phrase ''Complete EHR or''; and

■ l. Revising paragraphs (g)(1) introductory text, (g)(1)(i), (g)(2), (g)(3)(i), (g)(4), (g)(5)(i), and (g)(6)(v).

The revisions and additions read as follows:

§ 170.580 ONC review of certified health IT or a health IT developer's actions.

(a) * * *

(1) *Purpose.* ONC may directly review certified health IT or a health IT developer's actions or practices to determine whether either conform to the requirements of the ONC Health IT Certification Program.

(2) * * *

(i) *Certified health IT causing or contributing to unsafe conditions.* * * *

(ii) *Impediments to ONC–ACB oversight of certified health IT.* * * *

(iii) *Noncompliance with a Condition and Maintenance of Certification requirement.* ONC may initiate direct review under this section if it has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement under subpart D of this part.

(3) * * *

(i) ONC's review of certified health IT or a health IT developer's actions or practices is independent of, and may be in addition to, any surveillance of certified health IT conducted by an ONC–ACB.

* * * * *

(iv) An ONC–ACB and ONC–ATL shall provide ONC with any available information that ONC deems relevant to its review of certified health IT or a health IT developer's actions or practices.

(v) ONC may end all or any part of its review of certified health IT or a health IT developer's actions or practices under this section at any time and refer the applicable part of the review to the relevant ONC–ACB(s) if ONC determines that doing so would serve the effective administration or oversight of the ONC Health IT Certification Program.

(4) *Coordination with the Office of Inspector General.* (i) ONC may coordinate its review of a claim of information blocking with the Office of Inspector General or defer to the Office of Inspector General to lead a review of a claim of information blocking.

(ii) ONC may rely on Office of Inspector General findings to form the basis of a direct review action.

(b) * * *

(1) * * *

(i) *Circumstances that may trigger notice of potential non-conformity.* At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of potential non-conformity if it has a reasonable belief that certified health IT or a health IT developer's actions or practices may not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(iii) * * *

(D) Issue a notice of proposed termination if the health IT is under review in accordance with paragraph (a)(2)(i) or (ii) of this section.

(2) * * *

(i) *Circumstances that may trigger notice of non-conformity.* At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of non-conformity to the health IT developer if it determines that certified health IT or a health IT developer's actions or practices does not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(*3*) * * *

(i) All records related to the development, testing, certification, implementation, maintenance and use of its certified health IT;

(ii) Any complaint records related to the certified health IT;

(iii) All records related to the Condition(s) and Maintenance of Certification requirements, including marketing and distribution records, communications, and contracts; and

(iv) Any other relevant information.

(c) * * *

(1) *Applicability.* If ONC determines that certified health IT or a health IT developer's action or practice does not conform to requirements of the ONC Health IT Certification Program, ONC shall notify the health IT developer of its determination and require the health IT developer to submit a proposed corrective action plan.

* * * * *

(e) * * *

(1) *Applicability.* Excluding situations of noncompliance with a Condition or Maintenance of Certification

requirement under subpart D of this part, ONC may propose to terminate a certification issued to a Health IT Module if:

* * * * *

(f) * * *

(1) *Applicability.* The National Coordinator may terminate a certification if:

(i) A determination is made that termination is appropriate after considering the information provided by the health IT developer in response to the proposed termination notice;

(ii) The health IT developer does not respond in writing to a proposed termination notice within the timeframe specified in paragraph (e)(3) of this section; or

(iii) A determination is made that the health IT developer is noncompliant with a Condition or Maintenance of Certification requirement under subpart D of this part or for the following circumstances when ONC exercises direct review under paragraph (a)(2)(iii) of this section:

(A) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

(*1*) Fact-finding;

(*2*) A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(*3*) of this section; or

(*3*) A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(*3*) of this section.

(B) The information or access provided by the health IT developer in response to any ONC communication, including, but not limited to: Fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete;

(C) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(D) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(E) The health IT developer fails to timely submit a corrective action plan that adequately addresses the elements required by ONC as described in paragraph (c) of this section;

(F) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(G) ONC concludes that the non-conformity(ies) cannot be cured.

* * * * *

(g) * * *

(1) *Basis for appeal.* A health IT developer may appeal an ONC determination to suspend or terminate a certification issued to a Health IT Module and/or an ONC determination to issue a certification ban under § 170.581(a)(2) if the health IT developer asserts:

(i) ONC incorrectly applied ONC Health IT Certification Program requirements for a:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

* * * * *

(2) *Method and place for filing an appeal.* A statement of intent to appeal followed by a request for appeal must be submitted to ONC in writing by an authorized representative of the health IT developer subject to the determination being appealed. The statement of intent to appeal and request for appeal must be filed in accordance with the requirements specified in the notice of:

(i) Termination;

(ii) Suspension; or

(iii) Certification ban under § 170.581(a)(2).

(3) * * *

(i) A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

* * * * *

(4) *Effect of appeal.* (i) A request for appeal stays the termination of a certification issued to a Health IT Module, but the Health IT Module is prohibited from being marketed, licensed, or sold as ''certified'' during the stay.

(ii) A request for appeal does not stay the suspension of a Health IT Module.

(iii) A request for appeal stays a certification ban issued under § 170.581(a)(2).

(5) * * *

(i) The hearing officer may not review an appeal in which he or she participated in the initial suspension, termination, or certification ban determination or has a conflict of interest in the pending matter.

* * * * *

(6) * * *

(v) ONC will have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf that clarifies, as necessary, its determination to suspend or terminate the certification or issue a certification ban.

* * * * *

■ 32. Revise § 170.581 to read as follows:

§ 170.581 Certification ban.

(a) *Circumstances that may trigger a certification ban.* The certification of any of a health IT developer's health IT is prohibited when:

(1) The certification of one or more of the health IT developer's Health IT Modules is:

(i) Terminated by ONC under the ONC Health IT Certification Program;

(ii) Withdrawn from the ONC Health IT Certification Program by an ONC–ACB because the health IT developer requested it to be withdrawn (for reasons other than to comply with Program requirements) when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(iii) Withdrawn by an ONC–ACB because of a non-conformity with any of the certification criteria adopted by the Secretary under subpart C of this part;

(iv) Withdrawn by an ONC–ACB because the health IT developer requested it to be withdrawn (for reasons other than to comply with Program requirements) when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary under subpart C of this part, including notice of pending surveillance; or

(2) ONC determines a certification ban is appropriate per its review under § 170.580(a)(2)(iii).

(b) *Notice of certification ban.* When ONC decides to issue a certification ban to a health IT developer, ONC will notify the health IT developer of the certification ban through a notice of certification ban. The notice of certification ban will include, but may not be limited to:

(1) An explanation of the certification ban;

(2) Information supporting the certification ban;

(3) Instructions for appealing the certification ban if banned in accordance with paragraph (a)(2) of this section; and

(4) Instructions for requesting reinstatement into the ONC Health IT Certification Program, which would lift the certification ban.

(c) *Effective date of certification ban.* (1) A certification ban will be effective immediately if banned under paragraph (a)(1) of this section.

(2) For certification bans issued under paragraph (a)(2) of this section, the ban will be effective immediately after the following applicable occurrence:

(i) The expiration of the 10-day period for filing a statement of intent to appeal in § 170.580(g)(3)(i) if the health IT

developer does not file a statement of intent to appeal.

(ii) The expiration of the 30-day period for filing an appeal in § 170.580(g)(3)(ii) if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(iii) A final determination to issue a certification ban per § 170.580(g)(7) if a health IT developer files an appeal timely.

(d) *Reinstatement.* The certification of a health IT developer's health IT subject to the prohibition in paragraph (a) of this section may commence once the following conditions are met.

(1) A health IT developer must request ONC's permission in writing to participate in the ONC Health IT Certification Program.

(2) The request must demonstrate that the customers affected by the certificate termination, certificate withdrawal, or noncompliance with a Condition or Maintenance of Certification requirement have been provided appropriate remediation.

(3) For noncompliance with a Condition or Maintenance of Certification requirement, the noncompliance must be resolved.

(4) ONC is satisfied with the health IT developer's demonstration under paragraph (d)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

■ 33. Amend § 170.599 by:

■ a. Redesignating paragraph (b)(4) as paragraph (b)(5);

■ b. Adding new paragraph (b)(4); and

■ c. Revising newly redesignated paragraph (b)(5).

The addition and revision read as follows:

§ 170.599 Incorporation by Reference

* * * * *

(b) * * *

(4) ISO/IEC 17025:2017(E)—General requirements for the competence of testing and calibration laboratories (Third Edition), 2017–11, ''ISO/IEC 17025,'' IBR approved for §§ 170.520(b), and 170.524(a).

(5) ISO/IEC 17065:2012(E)—Conformity assessment—Requirements for bodies certifying products, processes and services (First Edition), 2012, ''ISO/IEC 17065,'' IBR approved for §§ 170.503 and 170.523(a).

■ 34. Add part 171 to read as follows:

PART 171—INFORMATION BLOCKING

Subpart A—General Provisions

Subpart B—Exceptions That Involve Not Fulfilling Requests to Access, Exchange, or use Electronic Health Information

Subpart C—Exceptions That Involve Procedures for Fulfilling Requests to Access, Exchange, or use Electronic Health Information

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

Subpart A—General Provisions

§ 171.100 Statutory basis and purpose.

(a) *Basis.* This part implements section 3022 of the Public Health Service Act, 42 U.S.C. 300jj–52.

(b) *Purpose.* The purpose of this part is to establish exceptions for reasonable and necessary activities that do not constitute information blocking as defined by section 3022(a)(1) of the Public Health Service Act, 42 U.S.C. 300jj–52.

§ 171.101 Applicability.

(a) This part applies to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks, as those terms are defined in § 171.102.

(b) Health care providers, health IT developers of certified health IT, health information exchanges, and health information networks must comply with this part on and after November 2, 2020.

§ 171.102 Definitions.

For purposes of this part:

Access means the ability or means necessary to make electronic health information available for exchange or use.

Actor means a health care provider, health IT developer of certified health IT, health information network or health information exchange.

API Information Source is defined as it is in § 170.404(c).

API User is defined as it is in § 170.404(c).

Certified API Developer is defined as it is in § 170.404(c).

Certified API technology is defined as it is in § 170.404(c).

Electronic health information (EHI) means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include:

(1) Psychotherapy notes as defined in 45 CFR 164.501; or

(2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Exchange means the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks.

Fee means any present or future obligation to pay money or provide any other thing of value.

Health care provider has the same meaning as ''health care provider'' in 42 U.S.C. 300jj.

Health information network or *health information exchange* means an individual or entity that determines,

controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information:

(1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and

(2) That is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164.

Health IT developer of certified health IT means an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj–11(c)(5) (ONC Health IT Certification Program).

Information blocking is defined as it is in § 171.103.

Interfere with or *interference* means to prevent, materially discourage, or otherwise inhibit.

Interoperability element means hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that:

(1) May be necessary to access, exchange, or use electronic health information; and

(2) Is/Are controlled by the actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of electronic health information.

Permissible purpose means a purpose for which a person is authorized, permitted, or required to access, exchange, or use electronic health information under applicable law.

Person is defined as it is in 45 CFR 160.103.

Practice means an act or omission by an actor.

Use means the ability for electronic health information, once accessed or exchanged, to be understood and acted upon.

§ 171.103 Information blocking.

(a) Information blocking means a practice that—

(1) Except as required by law or covered by an exception set forth in subpart B or subpart C of this part, is likely to interfere with access, exchange, or use of electronic health information; and

(2) If conducted by a health information technology developer, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; or

(3) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

(b) Until May 2, 2022, electronic health information for purposes of paragraph (a) of this section is limited to the electronic health information identified by the data elements represented in the USCDI standard adopted in § 170.213.

Subpart B—Exceptions That Involve Not Fulfilling Requests To Access, Exchange, or Use Electronic Health Information

§ 171.200 Availability and effect of exceptions.

A practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision as set forth in this subpart B by meeting all applicable requirements and conditions of the exception at all relevant times.

§ 171.201 Preventing harm exception—when will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking?

An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when the practice meets the conditions in paragraphs (a) and (b) of this section, satisfies at least one condition from each of paragraphs (c), (d), and (f) of this section, and also meets the condition in paragraph (e) of this section when applicable.

(a) *Reasonable belief.* The actor engaging in the practice must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information affected by the practice. For purposes of this section, ''patient'' means a natural person who is the subject of the electronic health information affected by the practice.

(b) *Practice breadth.* The practice must be no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce.

(c) *Type of risk.* The risk of harm must:

(1) Be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose electronic health information is affected by the determination; *or*

(2) Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

(d) *Type of harm.* The type of harm must be one that could serve as grounds for a covered entity (as defined in § 160.103 of this title) to deny access (as the term ''access'' is used in part 164 of this title) to an individual's protected health information under:

(1) Section 164.524(a)(3)(iii) of this title where the practice is likely to, or in fact does, interfere with access, exchange, or use (as these terms are defined in § 171.102) of the patient's electronic health information by their legal representative (including but not limited to personal representatives recognized pursuant to 45 CFR 164.502) and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;

(2) Section 164.524(a)(3)(ii) of this title where the practice is likely to, or in fact does, interfere with the patient's or their legal representative's access to, use or exchange (as these terms are defined in § 171.102) of information that references another natural person and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;

(3) Section 164.524(a)(3)(i) of this title where the practice is likely to, or in fact does, interfere with the patient's access, exchange, or use (as these terms are defined in § 171.102) of their own electronic health information, regardless of whether the risk of harm that the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (2) of this section; or

(4) Section 164.524(a)(3)(i) of this title where the practice is likely to, or in fact does, interfere with a legally permissible access, exchange, or use (as these terms are defined in § 171.102) of electronic health information not described in paragraph (d)(1), (2), or (3) of this section, and regardless of whether the risk of harm the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (2) of this section.

(e) *Patient right to request review of individualized determination of risk of harm.* Where the risk of harm is consistent with paragraph (c)(1) of this section, the actor must implement the practice in a manner consistent with any rights the individual patient whose electronic health information is affected may have under § 164.524(a)(4) of this title, or any Federal, State, or tribal law, to have the determination reviewed and potentially reversed.

(f) *Practice implemented based on an organizational policy or a determination specific to the facts and circumstances.* The practice must be consistent with an organizational policy that meets paragraph (f)(1) of this section or, in the absence of an organizational policy applicable to the practice or to its use in particular circumstances, the practice must be based on a determination that meets paragraph (f)(2) of this section.

(1) An organizational policy must:

(i) Be in writing;

(ii) Be based on relevant clinical, technical, and other appropriate expertise;

(iii) Be implemented in a consistent and non-discriminatory manner; and

(iv) Conform each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use.

(2) A determination must:

(i) Be based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and

(ii) Be based on expertise relevant to implementing the practice consistent with the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use in particular circumstances.

§ 171.202 Privacy exception—when will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy not be considered information blocking?

An actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy will not be considered information blocking when the practice meets all of the requirements of at least one of the sub-exceptions in paragraphs (b) through (e) of this section.

(a) *Definitions in this section.* (1) The term *HIPAA Privacy Rule* as used in this section means 45 CFR parts 160 and 164.

(2) The term *individual* as used in this section means one or more of the following—

(i) An individual as defined by 45 CFR 160.103.

(ii) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(iii) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section in making decisions related to health care as a personal representative, in accordance with 45 CFR 164.502(g).

(iv) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(v) An executor, administrator, or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under State or other law.

(b) *Sub-exception—precondition not satisfied.* To qualify for the exception on the basis that State or Federal law requires one or more preconditions for providing access, exchange, or use of electronic health information that have not been satisfied, the following requirements must be met—

(1) The actor's practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either:

(i) Conforms to the actor's organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor to determine when the precondition would be satisfied and, as applicable, the steps that the actor will take to satisfy the precondition; and

(C) Are implemented by the actor, including by providing training on the policies and procedures; or

(ii) Are documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met.

(2) If the precondition relies on the provision of a consent or authorization from an individual and the actor has received a version of such a consent or authorization that does not satisfy all elements of the precondition required under applicable law, the actor must:

(i) Use reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or provide other reasonable assistance to the individual to satisfy all required elements of the precondition; and

(ii) Not improperly encourage or induce the individual to withhold the consent or authorization.

(3) For purposes of determining whether the actor's privacy policies and procedures and actions satisfy the requirements of paragraphs (b)(1)(i) and (b)(2) above when the actor's operations are subject to multiple laws which have inconsistent preconditions, they shall be deemed to satisfy the requirements of the paragraphs if the actor has adopted uniform privacy policies and procedures to address the more restrictive preconditions.

(c) *Sub-exception—health IT developer of certified health IT not covered by HIPAA.* If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, when engaging in a practice that promotes the privacy interests of an individual, the actor's organizational privacy policies must have been disclosed to the individuals and entities that use the actor's product or service before they agreed to use them, and must implement the practice according to a process described in the organizational privacy policies. The actor's organizational privacy policies must:

(1) Comply with State and Federal laws, as applicable;

(2) Be tailored to the specific privacy risk or interest being addressed; and

(3) Be implemented in a consistent and non-discriminatory manner.

(d) *Sub-exception—denial of an individual's request for their electronic health information consistent with 45 CFR 164.524(a)(1) and (2).* If an individual requests electronic health information under the right of access provision under 45 CFR 164.524(a)(1) from an actor that must comply with 45 CFR 164.524(a)(1), the actor's practice

must be consistent with 45 CFR 164.524(a)(2).

(e) *Sub-exception—respecting an individual's request not to share information.* Unless otherwise required by law, an actor may elect not to provide access, exchange, or use of an individual's electronic health information if the following requirements are met—

(1) The individual requests that the actor not provide such access, exchange, or use of electronic health information without any improper encouragement or inducement of the request by the actor;

(2) The actor documents the request within a reasonable time period;

(3) The actor's practice is implemented in a consistent and non-discriminatory manner; and

(4) An actor may terminate an individual's request for a restriction to not provide such access, exchange, or use of the individual's electronic health information only if:

(i) The individual agrees to the termination in writing or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented by the actor; or

(iii) The actor informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual's electronic health information except that such termination is:

(A) Not effective to the extent prohibited by applicable Federal or State law; and

(B) Only applicable to electronic health information created or received after the actor has so informed the individual of the termination.

§ 171.203 Security exception—when will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information not be considered information blocking?

An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information will not be considered information blocking when the practice meets the conditions in paragraphs (a), (b), and (c) of this section, and in addition meets either the condition in paragraph (d) of this section or the condition in paragraph (e) of this section.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to electronic health information; and

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

§ 171.204 Infeasibility exception—when will an actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request not be considered information blocking?

An actor's practice of not fulfilling a request to access, exchange, or use electronic health information due to the infeasibility of the request will not be considered information blocking when the practice meets one of the conditions in paragraph (a) of this section and meets the requirements in paragraph (b) of this section.

(a) *Conditions*—(1) *Uncontrollable events.* The actor cannot fulfill the request for access, exchange, or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.

(2) *Segmentation.* The actor cannot fulfill the request for access, exchange, or use of electronic health information because the actor cannot unambiguously segment the requested electronic health information from electronic health information that:

(i) Cannot be made available due to an individual's preference or because the electronic health information cannot be made available by law; or

(ii) May be withheld in accordance with § 171.201.

(3) *Infeasible under the circumstances.* (i) The actor demonstrates, prior to responding to the request pursuant to paragraph (b) of this section, through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

(A) The type of electronic health information and the purposes for which it may be needed;

(B) The cost to the actor of complying with the request in the manner requested;

(C) The financial and technical resources available to the actor;

(D) Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of electronic health information to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(E) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and

(F) Why the actor was unable to provide access, exchange, or use of electronic health information consistent with the exception in § 171.301.

(ii) In determining whether the circumstances were infeasible under paragraph (a)(3)(i) of this section, it shall not be considered whether the manner requested would have:

(A) Facilitated competition with the actor.

(B) Prevented the actor from charging a fee or resulted in a reduced fee.

(b) *Responding to requests.* If an actor does not fulfill a request for access, exchange, or use of electronic health information for any of the reasons provided in paragraph (a) of this section, the actor must, within ten business days of receipt of the request, provide to the requestor in writing the reason(s) why the request is infeasible.

§ 171.205 Health IT performance exception—when will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information not be considered information blocking?

An actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information will not be considered information blocking when the practice meets a condition in paragraph (a), (b), (c), or (d) of this section, as applicable to the particular practice and the reason for its implementation.

(a) *Maintenance and improvements to health IT.* When an actor implements a practice that makes health IT under that actor's control temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the actor's practice must be—

(1) Implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability or degradation is initiated by a health IT developer of certified health IT, health information exchange, or health information network:

(i) *Planned.* Consistent with existing service level agreements between the individual or entity to whom the health IT developer of certified health IT, health information exchange, or health information network supplied the health IT; or

(ii) *Unplanned.* Consistent with existing service level agreements between the individual or entity; or agreed to by the individual or entity to whom the health IT developer of certified health IT, health information exchange, or health information network supplied the health IT.

(b) *Assured level of performance.* An actor may take action against a third-party application that is negatively impacting the health IT's performance, provided that the practice is—

(1) For a period of time no longer than necessary to resolve any negative impacts;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) Consistent with existing service level agreements, where applicable.

(c) *Practices that prevent harm.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(d) *Security-related practices.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

Subpart C—Exceptions That Involve Procedures for Fulfilling Requests To Access, Exchange, or Use Electronic Health Information

§ 171.300 Availability and effect of exceptions.

A practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision as set forth in this subpart C by meeting all applicable requirements and conditions of the exception at all relevant times.

§ 171.301 Content and manner exception—when will an actor's practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information not be considered information blocking?

An actor's practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information will not be considered information blocking when the practice meets all of the following conditions.

(a) *Content condition—electronic health information.* An actor must respond to a request to access, exchange, or use electronic health information with—

(1) *USCDI.* For up to May 2, 2022, at a minimum, the electronic health information identified by the data elements represented in the USCDI standard adopted in § 170.213.

(2) *All electronic health information.* On and after May 2, 2022, electronic health information as defined in § 171.102.

(b) *Manner condition*—(1) *Manner requested.* (i) An actor must fulfill a request described in paragraph (a) of this section in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

(ii) If an actor fulfills a request described in paragraph (a) of this section in any manner requested:

(A) Any fees charged by the actor in relation to fulfilling the response are not required to satisfy the exception in § 171.302; and

(B) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.

(2) *Alternative manner.* If an actor does not fulfill a request described in paragraph (a) of this section in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner, as follows:

(i) The actor must fulfill the request without unnecessary delay in the following order of priority, starting with paragraph (b)(2)(i)(A) of this section and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph.

(A) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor.

(B) Using content and transport standards specified by the requestor and published by:

(*1*) The Federal Government; or

(*2*) A standards developing organization accredited by the American National Standards Institute.

(C) Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.

(ii) Any fees charged by the actor in relation to fulfilling the request are required to satisfy the exception in § 171.302.

(iii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the exception in § 171.303.

§ 171.302 Fees exception—when will an actor's practice of charging fees for accessing, exchanging, or using electronic health information not be considered information blocking?

An actor's practice of charging fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using electronic health information will not be considered information blocking when the practice meets the conditions in paragraph (a) of this section, does not include any of the excluded fees in paragraph (b) of this section, and, as applicable, meets the condition in paragraph (c) of this section.

(a) *Basis for fees condition.* (1) The fees an actor charges must be—

(i) Based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;

(ii) Reasonably related to the actor's costs of providing the type of access, exchange, or use of electronic health information to, or at the request of, the person or entity to whom the fee is charged;

(iii) Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported; and

(iv) Based on costs not otherwise recovered for the same instance of service to a provider and third party.

(2) The fees an actor charges must not be based on—

(i) Whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor;

(ii) Sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of the electronic health information;

(iii) Costs the actor incurred due to the health IT being designed or implemented in a non-standard way, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the electronic health information;

(iv) Costs associated with intangible assets other than the actual development or acquisition costs of such assets;

(v) Opportunity costs unrelated to the access, exchange, or use of electronic health information; or

(vi) Any costs that led to the creation of intellectual property, if the actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.

(b) *Excluded fees condition.* This exception does not apply to—

(1) A fee prohibited by 45 CFR 164.524(c)(4);

(2) A fee based in any part on the electronic access of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual;

(3) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; and

(4) A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

(c) *Compliance with the Conditions of Certification condition.* Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4), § 170.404, or both of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(d) *Definition of Electronic access.* The following definition applies to this section:

Electronic access means an internet-based method that makes electronic health information available at the time the electronic health information is requested and where no manual effort is required to fulfill the request.

§ 171.303 Licensing exception—when will an actor's practice to license interoperability elements in order for electronic health information to be accessed, exchanged, or used not be considered information blocking?

An actor's practice to license interoperability elements for electronic health information to be accessed, exchanged, or used will not be considered information blocking when the practice meets all of the following conditions.

(a) *Negotiating a license conditions.* Upon receiving a request to license an interoperability element for the access, exchange, or use of electronic health information, the actor must—

(1) Begin license negotiations with the requestor within 10 business days from receipt of the request; and

(2) Negotiate a license with the requestor, subject to the licensing conditions in paragraph (b) of this section, within 30 business days from receipt of the request.

(b) *Licensing conditions.* The license provided for the interoperability element(s) needed to access, exchange, or use electronic health information must meet the following conditions:

(1) *Scope of rights.* The license must provide all rights necessary to:

(i) Enable the access, exchange, or use of electronic health information; and

(ii) Achieve the intended access, exchange, or use of electronic health information via the interoperability element(s).

(2) *Reasonable royalty.* If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements:

(i) The royalty must be non-discriminatory, consistent with paragraph (c)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards developing organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on terms consistent with those in this exception, the actor may charge a royalty that is consistent with such policies.

(iv) An actor may not charge a royalty for intellectual property if the actor recovered any development costs pursuant to § 171.302 that led to the creation of the intellectual property.

(3) *Non-discriminatory terms.* The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements:

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on—

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements.

(4) *Collateral terms.* The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following—

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets

the requirements of the exception in § 171.302.

(5) *Non-disclosure agreement.* The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided—

(i) The agreement states with particularity all information the actor claims as trade secrets; and

(ii) Such information meets the definition of a trade secret under applicable law.

(c) *Additional conditions relating to the provision of interoperability elements.* The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

(3) Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

Alex M. Azar II,

Secretary, Department of Health and Human Services.

[FR Doc. 2020–07419 Filed 4–21–20; 4:15 pm]

BILLING CODE 4150–45–P