DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 170, 171, and 172

RIN 0955–AA06

Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability

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

ACTION: Proposed rule.

SUMMARY: This proposed rule seeks to advance interoperability, improve transparency, and support the access, exchange, and use of electronic health information through proposals for: standards adoption; adoption of certification criteria to advance public health data exchange; expanded uses of certified application programming interfaces, such as for electronic prior authorization, patient access, care management, and care coordination; and information sharing under the information blocking regulations. It proposes to establish a new baseline version of the United States Core Data for Interoperability. The proposed rule would update the ONC Health IT Certification Program to enhance interoperability and optimize certification processes to reduce burden and costs. The proposed rule would also implement certain provisions related to the Trusted Exchange Framework and Common Agreement (TEFCA), which would support the reliability, privacy, security, and trust within TEFCA.

DATES: To be assured consideration, written or electronic comments must be received at one of the addresses provided below, no later than 5 p.m. Eastern Time on October 4, 2024.

ADDRESSES: You may submit comments, identified by RIN 0955–AA06, by any of the following methods (please do not submit duplicate comments). Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

- *Federal eRulemaking Portal:* Follow the instructions for submitting comments. Attachments should be in Microsoft Word, Microsoft Excel, or Adobe PDF; however, we prefer Microsoft Word. *http://www.regulations.gov.*
- *Regular, Express, or Overnight Mail:* Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Attention: Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201. Please submit one original and two copies.
- *Hand Delivery or Courier:* Office of the National Coordinator for Health Information Technology, Attention: Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability Proposed Rule, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Mary E. Switzer Building is not readily available to persons without Federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. Please do not include anything in your comment submission that you do not wish to share with the general public. Such information includes, but is not limited to, the following: a person's social security number; date of birth; driver's license number; state identification number or foreign country equivalent; passport number; financial account number; credit or debit card number; any personal health information; or any business information that could be considered proprietary. We will post all comments that are received before the close of the comment period at *http://www.regulations.gov.*

Docket: For access to the docket to read background documents, comments received, or the plain-language summary of the proposed rule of not more than 100 words in length required by the Providing Accountability Through Transparency Act of 2023, go to *http://www.regulations.gov* or the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Mary E. Switzer Building, Mail Stop: 7033A, 330 C Street SW, Washington, DC 20201 (call ahead to the contact listed below to arrange for inspection).

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

The Secretary of Health and Human Services has delegated responsibilities to the Office of the National Coordinator for Health Information Technology (ONC) for the implementation of certain provisions in Title IV of the 21st Century Cures Act (Pub. L. 114–255, Dec. 13, 2016) (Cures Act) that are designed to: advance interoperability; support the access, exchange, and use of electronic health information (EHI); and identify reasonable and necessary activities that do not constitute information blocking.[1] ONC is responsible for implementation of certain provisions of the Health Information Technology for Economic and Clinical Health Act (Pub. L. 111–5, Feb. 17. 2009) (HITECH Act) including: requirements that the National Coordinator perform duties consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that promotes a more effective marketplace, greater competition, and increased consumer choice, among other goals; and requirements to keep or recognize a program or programs for the voluntary certification of health information technology. This proposed rule seeks to fulfill statutory requirements; provide transparency; advance equity, innovation, and interoperability; and support the access to, and exchange and use of, EHI. Transparency regarding healthcare information and activities—as well as the interoperability and electronic exchange of health information—are all in the best interest of the patient and are central to the efforts of the Department of Health and Human Services to enhance and protect the health and well-being of all Americans.

In addition to addressing the HITECH Act's and Cures Act's requirements described above and advancing interoperability, the proposed rule aligns with and supports Executive Orders (E.O.) 13994, 13985, 14036, and 14058. The President issued E.O. 13994 on January 21, 2021, to ensure a data-driven response to COVID–19 and future high-consequence public health threats. The Cures Act and the information blocking provisions in the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (85 FR 25642) (ONC Cures Act Final Rule) have enabled critical steps to making data available across the healthcare system. The proposed rule proposes to adopt certification criteria to advance interoperability and support public health reporting and exchange. Because we recognize the need for greater interoperability of public health technology and access to more actionable data by public health authorities (PHA) and their partners, the proposed rule lays out a multi-pronged approach that takes advantage of, and builds upon, the various previous efforts to advance public health reporting, including advancements in HL7® Fast Healthcare Interoperability Resources-based (FHIR®) solutions and evolving standards related to public health interoperability. We have proposed this approach to allow for systems to mature and advance in an aligned fashion, reduce the need for manual workarounds and intervention, and lead to wider adoption of advanced standards-based capabilities.

The proposed adoption of the United States Core Data for Interoperability Standard Version 4 (USCDI v4) would promote the establishment and use of interoperable data sets of EHI for interoperable health data exchange. As discussed in section III.B.1, USCDI v4 would facilitate the collection, access and exchange of data for use in public health and emergency response (*e.g.,* the COVID–19 pandemic) by capturing and promoting the sharing of key data elements related to public health. The proposal to adopt a new certification criterion for standardized FHIR-based application programming interfaces (APIs) for public health reporting, as discussed in section III.B.13.f, reflects ONC's continued efforts to develop and standardize APIs and facilitate exchange of public health data between health care providers and public health agencies, to securely access EHI through the broader adoption of standardized APIs.[2] [3]As discussed in section III.B, adopting USCDI v4 and the proposals in § 170.315(g)(20) are intended to facilitate core public health missions including detecting and monitoring, investigating and responding, informing and disseminating, and being response-ready. We also expect our proposed changes to improve patient access to more complete, standardized, immunization information stored in certified health IT products.

We are committed to advancing health equity, and this proposed rule is consistent with E.O. 13985 of January 20, 2021, Advancing Racial Equity and Support for Underserved Communities Through the Federal Government.[4] Section 1 of E.O. 13985 states that ''the Federal Government should pursue a comprehensive approach to advancing equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality.'' Section 1 of E.O. 13985 also states that because ''advancing equity requires a systematic approach to embedding fairness in decision-making processes, executive departments and agencies must recognize and work to redress inequities in any policies and programs that serve as barriers to equal opportunity.'' We believe USCDI v4 and proposals in § 170.315(f) and § 170.315(g)(20) would not only support identifying and responding to public health threats, but also support advancing equity. As noted above, we propose to modify current certification

[1] Reasonable and necessary activities that do not constitute information blocking, also known as information blocking exceptions, are identified in 45 CFR part 171 subparts B, C and D. ONC's official website, HealthIT.gov, offers a variety of resources on the topic of Information Blocking, including fact sheets, recorded webinars, and frequently asked questions. To learn more, please visit: *https://www.healthit.gov/topic/information-blocking/.*

[2] ONC. (2022, October 18). *API Resource Guide.* ONC Health IT Certification Program API Resource Guide. Retrieved March 16, 2023, from *https://onc-healthit.github.io/api-resource-guide/.*

[3] Section 4002 of the 21st Century Cures Act (Cures Act) established a condition of certification that requires health IT developers to publish application programming interfaces (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 API Conditions and Maintenance of Certification requirements and certification criteria are identified in 45 CFR part 170.

[4] United States, Executive Office of the President [Joseph Biden]. Executive Order 13985: Advancing Racial Equity and Support for Underserved Communities Through the Federal Government. Jan 20, 2021. 86 FR 7009 through 7013, *https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government.*

criteria in § 170.315(f) and adopt new criteria in § 170.315(f) for Health IT Modules supporting public health data exchange that would help increase the data shared between health care providers, laboratories, and PHAs, and would increase interoperability among the different systems in place at each entity. Our proposed changes focus on providing more complete patient-level information for contact tracing and further case investigation, patient outreach, direct care, and other clinical and public health activities. For example, some of the proposed standards would require the exchange of available patient demographic information, including race, ethnicity, sex, and contact information; and may allow PHAs to get more complete data when providers and laboratories have these data elements and can appropriately fill the fields. Additionally, if finalized as proposed, the adoption of USCDI v4 would update the USCDI standard to include new data elements under the Health Status Assessments, Medications, Allergies and Intolerances, Goals and Preferences, Encounter Information, Vital Signs, and Laboratory data classes, and a new data class, Facility Information, as discussed in section III.B.1 of this proposed rule. Expanding the data elements included in USCDI would increase the amount and type of data available to be used and exchanged through certified health IT. Our proposed standards update for public health and USCDI v4 could help capture more accurate and complete patient characteristics that are reflective of patient diversity and could potentially help data users address disparities in health outcomes for all patients, including those who may be marginalized and underrepresented. This could also support data users' abilities to identify, assess, and analyze gaps in care, which could in turn be used to inform and address the quality of healthcare through interventions and strategies. This could lead to better patient care, experiences, and health outcomes.

As discussed in section III.B.1, the proposal to adopt USCDI v4 also supports the concept of ''health equity by design,'' where health equity considerations are identified and incorporated from the beginning and throughout the technology design, build, and implementation processes, and health equity strategies, tactics, and patterns are guiding principles for developers, enforced by technical architecture, and built into the technology at every layer. With every successive USCDI version supported by certified health IT, the capabilities and workflows included will help support equity and efforts to reduce disparities.

President Biden's E.O. 14036, Promoting Competition in the American Economy,[5] issued on July 9, 2021, established a whole-of-government effort to promote competition in the American economy and reaffirmed the policy stated in E.O. 13725 of April 15, 2016 (Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy).[6] This proposed rule would foster competition by advancing foundational standards for certified API technology, which enable—through applications (apps) and without special effort—improved legally permissible sharing of EHI among clinicians, patients, researchers, and others. As described throughout the proposed rule, competition would be advanced through these improved API standards that can help individuals connect to their information and can help health care providers involved in the patient's care to securely access information. For example, these standards are designed to foster an ecosystem of new applications that can connect through the API technology to provide patients with improved electronic access to EHI and more choices in their health care providers. This is similar to how APIs have impacted other sectors of the economy, such as travel, banking, and commerce.

Further, as described in section IV of this proposed rule, we propose enhancements to support information sharing under the information blocking regulations and promote innovation and competition, while ensuring patients' privacy and access to care remain protected. As we have noted, addressing information blocking is critical for promoting innovation and competition in health IT and for the delivery of healthcare services to individuals, as discussed in both the ONC Cures Act Proposed (84 FR 7508) and Final (85 FR 25790 through 25791) Rules, and reiterated in the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI–1) Final Rule (89 FR 1192). Specifically, we described how the information blocking provisions provide a comprehensive response to the issues identified by empirical and economic research that suggested that information blocking may weaken competition, encourage consolidation, and create barriers to entry for developers of new and innovative applications and technologies that enable more effective uses of EHI to improve population health and the patient experience.[7] We explained that the information blocking provision of the Public Health Service Act (PHSA) itself expressly addresses practices that impede innovation and advancements in EHI access, exchange, and use, including care delivery enabled by health IT (89 FR 1195, citing section 3022(a)(2) of the PHSA). Actors subject to the information blocking provisions may, among other practices, attempt to 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 (85 FR 25820).[8] Information blocking may also harm competition not just in health IT markets, but also in markets for healthcare services (85 FR 25820). In the ONC Cures Act Final Rule, we described practices that dominant market providers may leverage and use to control access and use of their technology, resulting in technical dependence and possibly leading to barriers to entry by would-be competitors, as well as making some market providers vulnerable to acquisition or inducement into arrangements that enhance the market power of incumbent providers to the detriment of consumers and purchasers

[5] United States, Executive Office of the President [Joseph Biden]. Executive Order 14036: Promoting Competition in the American Economy. Jul 9, 2021. 86 FR 36987 through36999, *https://www.federalregister.gov/documents/2021/07/14/2021-15069/promoting-competition-in-the-american-economy*.

[6] **Federal Register**: Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy.

[7] *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*; 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).

[8] *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*.

of healthcare services (85 FR 25820). The implementation of the new information blocking provisions proposed and discussed in section IV of this proposed rule would continue to promote innovation and support the lawful access, exchange, and use of EHI, while strengthening support for individuals' privacy and EHI sharing preferences.

Lastly, in support of E.O. 14058, Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government, issued on December 16, 2021, we are committed to advancing the equitable and effective delivery of services with a focus on the experience of individuals, health IT developers, and health care providers.[9] The proposed rule supports the Department of Health and Human Services' agency-wide approach to electronic prior authorization that meets the Department's interoperability and burden reduction goals, such as reducing documentation requirements associated with completing prior authorization requests for payers.[10] Proposed certification criteria would make available certified health IT that can enable payers contracting with the Federal government, such as Medicare Advantage plans, to meet Centers for Medicare & Medicaid Services (CMS) requirements for sharing information. Additionally, improving the equitable access, exchange, and use of EHI would help enable patient-centric care, which is expected to improve equity in health outcomes. This proposed rule further recognizes patient feedback and preferences in their care and how patients and their representatives may want to monitor and share EHI with relevant health care providers and entities. The health IT certification provisions of the proposed rule aim to reduce the burden associated with prior authorization processes, which can ensure that patients receive the care they need in a timely manner, lower administrative cost, and reduce the complexity of obtaining a prior authorization for health care providers and patients. Collectively, these provisions of the proposed rule help advance the equitable and effective delivery of services with a focus on the experience of individuals, health IT developers, and health care providers.

We also strive to further advance Federal agency coordination. ONC works with CMS to ensure that our certification criteria and standards support and complement CMS programs that reference ONC regulations, such as the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of the Merit-based Incentive Payment System (MIPS). In addition, a final rule titled ''Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program'' (CMS Interoperability and Prior Authorization final rule, 89 FR 8758) appeared in the **Federal Register** on February 8, 2024, and included requirements for certain payers regulated by CMS to establish APIs that can facilitate electronic prior authorization processes by 2027 (89 FR 8919). CMS also finalized electronic prior authorization measures for eligible clinicians who participate in the Promoting Interoperability performance category of the MIPS; and eligible hospitals and critical access hospitals that participate in the Medicare Promoting Interoperability Program, beginning in the CY 2027 performance period and the EHR reporting period in CY 2027, respectively (89 FR 8760). In this proposed rule, we propose to adopt standards and establish certification criteria to facilitate electronic prior authorization using certified health IT, which providers can use to complete the required actions under the finalized measures. Lastly, we are committed to our continued, collaborative work with the Centers for Disease Control and Prevention (CDC) on improving public health data systems. The proposed updates to the ONC Health IT Certification Program's public health criteria and complementary public health criteria for PHA systems would support CDC's Data Modernization Initiative and Public Health Data Strategy.[11] We believe these approaches would increase efficiency for delivery of services and programs, reduce confusion for participants in these programs, and better serve the public interest.

While this rulemaking does not propose to require entities to adopt any specific standards to ensure that their information and communication technology (ICT), including software, applications, websites, and electronic documents, is accessible for people with disabilities, entities covered by this rule may also be subject to applicable requirements of Federal nondiscrimination laws. For example, Section 504 of the Rehabilitation Act of 1973 (Section 504) prohibits recipients of Federal financial assistance from discriminating on the basis of disability by excluding people with disabilities from participation in, denying them the benefits of, or subjecting them to discrimination in their programs or activities. 29 U.S.C. 794. Section 1557 of the Patient Protection and Affordable Care Act (Section 1557) prohibits certain health programs and activities, including those receiving Federal financial assistance from HHS, from discriminating on the basis of race, color, national origin, sex, age, or disability by excluding them from participation in, denying them the benefits of, or subjecting them to discrimination in their health programs or activities. 42 U.S.C. 18116(a). Newly issued Section 504 regulations require recipients to ensure that web content and mobile apps that a recipient provides or makes available, directly or through contractual, licensing, or other arrangements, be readily accessible to and usable by individuals with disabilities, with some exceptions. *See* 89 FR 40066 and 45 CFR Secs. 84.82-.89(a). The rule requires technical accessibility standards that must be met on May 11, 2026, for entities with fifteen or more employees and May 10, 2027, for entities with fewer than fifteen employees unless the recipient can demonstrate that compliance with this section would result in a fundamental alteration in the nature of a program or activity or in undue financial and administrative burdens or unless an exception applies. 45 CFR Sec. 84.84(b); 84.85. Title III of the Americans with Disabilities Act (ADA) prohibits discrimination on the basis of disability in the full and equal enjoyment of places of public accommodation. 42 U.S.C. 12182. Title II of the ADA prohibits state and local government

[9] United States, Executive Office of the President [Joseph Biden]. Executive Order 14058: Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government. Dec 13, 2021. 86 FR 71357 through71366, *https://www.federalregister.gov/documents/2021/12/16/2021-27380/transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government.*

[10] *Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs (Burden Reduction Report),* February 2020, pages 26–28, *https://www.healthit.gov/sites/default/files/page/2020-02/BurdenReport_0.pdf.*

[11] Public_Health_Data_Strategy-final-P.pdf (cdc.gov).

entities from discriminating on the basis of disability by excluding people with disabilities from participation in, denying them the benefits of, or subjecting them to discrimination in their services, programs, or activities. 42 U.S.C. 12132. On April 24, 2024, the Department of Justice published regulations establishing specific requirements, including the adoption of specific technical standards, for making accessible the services, programs, and activities offered by State and local government entities through the web and mobile applications. 89 FR 31320. More generally, these statutes and their implementing regulations apply to programs, services and activities implemented through or with information and communications technology (ICT). In addition, the Section 1557 implementing regulation addresses ICT specifically, providing that covered entities, including health programs and activities that receive Federal financial assistance from HHS, shall ensure that their health programs or activities provided through ICT are accessible to individuals with disabilities, unless doing so would result in undue financial and administrative burdens or a fundamental alteration in the nature of the health programs or activities. 89 FR 37522 (May 6, 2024) (45 CFR 92.204).

B. Summary of Major Provisions

1. ONC Health IT Certification Program Updates

a. New and Revised Standards and Certification Criteria

i. The United States Core Data for Interoperability Version 4 (USCDI v4)

The USCDI standard in § 170.213 is a baseline set of data that can be commonly exchanged across care settings for a wide range of uses. Certain certification criteria in the ONC Health IT Certification Program (Program) currently require the use of one of the versions of the USCDI standard by in § 170.213. We propose to update the USCDI standard in § 170.213 by adding USCDI v4 and by establishing an expiration date of January 1, 2028, for USCDI v3 for purposes of the Program. We propose to add USCDI v4 in § 170.213(c) and incorporate it by reference in § 170.299. We propose that up to and including December 31, 2027, a Health IT Module certified to certification criteria referencing § 170.213 may use either version of the standard. We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to certification criteria referencing § 170.213 must update its Health IT Module to USCDI v4 and provide the updated version to their customers in order to maintain certification of that Health IT Module. We propose that any Health IT Modules seeking certification to certification criteria referencing § 170.213 on or after January 1, 2028, would need to be capable of exchanging the data elements that the USCDI v4 comprises.

ii. SMART App Launch 2.2

As discussed in section III.B.2, we propose to adopt the HL7® FHIR® SMART Application Launch Framework Implementation Guide release 2.2.0 (SMART v2.2 Guide) in § 170.215(c)(3). We propose that the adoption of the SMART v2 Guide in § 170.215(c)(2) expires on January 1, 2028. We propose that a Health IT Module certified to criteria referencing the implementation specifications in § 170.215(c) may use the SMART v1, SMART v2, or SMART v2.2 guides for the time period up to and including December 31, 2025. Then, by January 1, 2026, when the adoption of SMART v1 expires, a health IT developer of a Health IT Module certified to certification criteria referencing the implementation specifications in § 170.215(c) must update its Health IT Module to either the SMART v2 or SMART v2.2 Guides and provide the updated version to its customers in order to maintain certification of that Health IT Module. Then, by January 1, 2028, when the adoption of the SMART v2 Guide expires, a health IT developer of a Health IT Module certified to certification criteria referencing the implementation specifications in § 170.215(c) must update its Health IT Module to the SMART v2.2 Guide and provide the updated version to its customers in order to maintain certification of that Health IT Module. On and after January 1, 2028, we propose that any Health IT Modules seeking certification to certification criteria referencing the implementation specifications in § 170.215(c), would need to be capable of supporting SMART v2.2 Guide functionality.

iii. User-Access Brands and Endpoints

We propose to adopt the User-access Brands and Endpoints (Brands) specification for our service base URL publication requirements, as explained in section III.B.3. This applies to our current service base URL publication requirements in § 170.404(b)(2), where we propose to reorganize the criterion's paragraphs in a way that places existing service base URL requirements into § 170.404(b)(2)(i) and (ii) and adds the new Brands requirement in § 170.404(b)(2)(iii). We propose in our updated § 170.404(b)(2)(iii) to require that, by January 1, 2028, service base URLs and related API Information Source details, including each organization's name, location, and facility identifier, must be published in an aggregate vendor-consolidated ''FHIR Bundle'' according to the Brands specification. Additionally, in our proposal to revise § 170.404(b)(3) where we propose new requirements for the publication of API discovery details for payer network information, including service base URLs and API Information Source details, we propose to adopt Brands specification.

iv. Standards for Encryption and Decryption of Electronic Health Information

As discussed in section III.B.4, we propose to adopt the updated version of Annex A of the Federal Information Processing Standards (FIPS) 140–2 (Draft, October 12, 2021) in § 170.210(a)(3) and incorporate it by reference in § 170.299. We propose to add an expiration date of January 1, 2026, to the FIPS 140–2 (October 8, 2014) version of the standard presently adopted in § 170.210(a)(2). We also propose to remove the standard found in § 170.210(f), which is no longer referenced in any active certification criteria. Revising § 170.210(a) by adding an expiration date in § 170.210(a)(2) and a new version of the FIPS standard in § 170.210(a)(3) would impact three certification criteria that currently reference the standard in § 170.210(a)(2), including § 170.315(d)(7) ''end-user device encryption;'' (d)(9) ''trusted connection;'' and (d)(12) ''encrypt authentication credentials.'' Note that we also propose to change the names of the certification criteria in § 170.315(d)(7) and (d)(12) to ''health IT encryption'' and ''protect stored authentication credentials'' respectively, as discussed in sections III.B.11 and III.B.12 of this preamble.

v. Minimum Standards Code Sets Updates

Early in ONC's standards and certification rulemakings, we established a policy of adopting newer versions of ''minimum standards'' code sets that update frequently (*e.g.,* 77 FR 54170 and 80 FR 62612). Adopting newer versions of these code sets enables improved interoperability and implementation of health IT with minimal additional burden. If adopted, newer versions of these minimum standards code sets would serve as the baseline for certification, and

developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis. Because these code sets are updated frequently, we will consider whether it may be more appropriate to adopt a version of a minimum standards code set issued after publication of this proposed rule, but before publication of a final rule. In section III.B.5, we discuss our proposals to adopt newer versions of the following minimum standards code sets:

- § 170.207(a)—Problems
- § 170.207(c)—Laboratory tests
- § 170.207(d)—Medications
- § 170.207(e)—Immunizations
- § 170.207(f)—Race and Ethnicity
- § 170.207(n)—Sex
- § 170.207(o)—Sexual orientation and gender information
- § 170.207(p)—Social, psychological, and behavioral data

vi. New Imaging Requirements for Health IT Modules

We propose, as explained in section III.B.6, to revise the certification criteria adopted in § 170.315(b)(1), (e)(1), (g)(9), and (g)(10) to include new certification requirements to support access, exchange, and use of diagnostic images via imaging links. However, we are not proposing a specific standard associated with the support of this functionality, and we note that this requirement can be met with a context-sensitive link to an external application which provides access to images and their associated narrative. We believe that this proposal, if finalized as proposed, will promote more consistent access to images for providers and patients. We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to the certification criteria related to ''transitions of care'' in § 170.315(b)(1), ''view, download, and transmit'' in § 170.315(e)(1), ''application access—all data request,'' in § 170.315(g)(9), and ''standardized API for patient and population services,'' in § 170.315(g)(10) must update their Health IT Module and provide the updated version to their customers to maintain certification of that Health IT Module.

vii. Revised Clinical Information Reconciliation and Incorporation Criterion

We propose, as described in section III.B.7, a primary proposal and an alternative proposal for revising the ''clinical information reconciliation and incorporation'' certification criterion in § 170.315(b)(2) to expand the number and types of data elements that Health IT Modules certified to this criterion would be required to reconcile and incorporate. Our primary proposal would require Health IT Modules certified to § 170.315(b)(2) to be capable of reconciling and incorporating all USCDI data elements according to at least one of the versions of the USCDI standard specified in § 170.213. Our alternative proposal would require Health IT Modules to reconcile and incorporate data elements from six additional USCDI data classes beyond the existing three data classes required as part of the current certification criterion's functionality. We also propose new functional requirements to enable user-driven automatic reconciliation and incorporation. We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to the criterion in § 170.315(b)(2) must update their Health IT Module and provide the updated version to their customers in order to maintain certification of that Health IT Module. We also propose that any Health IT Modules seeking certification for the criterion in § 170.315(b)(2) on or after January 1, 2028, would need to be capable of supporting this functionality.

viii. Revised Electronic Prescribing Certification Criterion

We propose to incorporate the National Council for Prescription Drug Programs (NCPDP) SCRIPT standard [12] version 2023011 in an updated version of the electronic prescribing certification criterion in § 170.315(b)(3)(ii). Under this proposal, as described in section III.B.8 of this proposed rule, health IT developers may maintain health IT certification conformance with the current version of the criterion using NCPDP SCRIPT standard version 2017071 for the time period up to and including December 31, 2027. We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to the criterion in § 170.315(b)(3) must update the Health IT Module to use the NCPDP SCRIPT standard version 2023011 and provide that update to their customers in order to maintain certification of the Health IT Module. We propose that any Health IT Modules for which a health IT developer seeks certification to the criterion in § 170.315(b)(3) on or after January 1, 2028, would need to be able to perform the required prescription-related electronic transaction in accordance with the NCPDP SCRIPT standard version 2023011. We also propose a series of updates to the transactions included in § 170.315(b)(3)(ii) including removing transactions currently identified as optional for the certification criterion.

ix. New Real-Time Prescription Benefit Criterion

Real-time prescription benefit tools empower providers and their patients to compare the patient-specific cost of a drug to the cost of a suitable alternative, compare prescription costs at different pharmacies, view information about out-of-pocket costs, and learn whether prior authorization for a specific drug is required. In order to implement section 119(b)(3) of the Consolidated Appropriations Act, 2021 (Pub. L. 116–260), as discussed in section III.B.9, we propose to establish a real-time prescription benefit certification criterion in § 170.315(b)(4) based on the National Council for Prescription Drug Programs (NCPDP) Real-Time Prescription Benefit (RTPB) standard version 13. We also propose to include this certification criterion in the Base EHR definition in § 170.102.

x. Electronic Health Information (EHI) Export—Single Patient EHI Export Exemption

As explained in section III.B.10, we propose to exempt Health IT Modules that act primarily as intermediaries between systems and, through integration, function without any direct human interaction from the requirement in § 170.315(b)(10)(i)(B) to provide functionality without subsequent developer assistance to operate. We propose that this exemption proposed in § 170.315(b)(10)(i)(F) would be available if the developer of such a Health IT Module receives fewer than ten requests in the immediately preceding calendar year for a single patient EHI export. Relatedly, we propose in § 170.402(b)(2)(iii) that developers of certified health IT with Health IT Modules certified to § 170.315(b)(10) that claim the exemption proposed in § 170.315(b)(10)(i)(F) would need to report the number of requests for single patient EHI export on an annual basis to their ONC-Authorized Certification Bodies (ACBs) by March 1 of each calendar year beginning in 2028.

xi. Revised End-User Device Encryption Criterion

As discussed in section III.B.11, we propose to revise § 170.315(d)(7) to include a new requirement that Health IT Modules certified to this criterion encrypt EHI stored server-side on and after January 1, 2026. To include this new requirement, we propose reorganizing the certification criterion's paragraphs in a way that places existing

[12] *See https://standards.ncpdp.org/.*

end-user device encryption requirements into § 170.315(d)(7)(i) and (d)(7)(ii) and adds the new server encryption requirement in § 170.315(d)(7)(iii). Then, we propose placing the applicable proposed encryption standard and default settings requirements to both the end-user device and server encryption requirements into § 170.315(d)(7)(iii) and (iv) respectively. We also propose to require that personally identifiable information must be encrypted in Health IT Modules certified to this revised certification criterion. Finally, we propose to change § 170.315(d)(7) by renaming it to ''health IT encryption,'' to better describe the end-user and proposed server-side requirements together.

xii. Revised Criterion for Encrypt Authentication Credentials

As explained in section III.B.12, we propose to revise the ''encrypt authentication credentials'' certification criterion in § 170.315(d)(12). We propose to revise the certification criterion by expiring our current ''yes'' or ''no'' attestation requirement and replacing it with a new requirement that Health IT Modules that store authentication credentials protect the confidentiality and integrity of its stored authentication credentials according to the Federal Information Processing Standards (FIPS) 140–2 (October 12, 2021) industry standard. We also propose to change the name of this certification criterion to ''protect stored authentication credentials,'' to better describe how we propose to revise the criterion.

xiii. Health IT Modules Supporting Public Health Data Exchange

Public health promotes and protects the health of all people and their communities. To accomplish this mission, public health authorities (PHAs) rely in part on public health information exchange, including data from healthcare facilities and providers, laboratories, schools, social and community service providers, and other data partners to acquire the information they need. However, PHAs often do not have access to—or, often, the ability to share—the data required to optimally address public health needs (emergent or otherwise) due to the lack of common standards utilized in the reported data, variable reporting requirements, limited interoperability of systems, or inadequate public health data infrastructure and technology. Considering the need for greater interoperability of public health technology and access to more actionable data by PHAs and their partners,[13] as discussed in section III.B.13, we propose: to revise the Program's current certification criteria related to public health in § 170.315(f), including referencing newer versions of respective exchange and vocabulary standards in the current § 170.315(f) certification criteria (§ 170.315(f)(1)–(f)(7)); proposing two additional certification criteria for birth reporting (§ 170.315(f)(8)) and bi-directional exchange with a prescription drug monitoring program (PDMP) (§ 170.315(f)(9)); proposing new certification criteria for Health IT Modules supporting public health data exchange in § 170.315(f)(21)–(25), (28) and (29); and, proposing a new certification criterion for a standardized FHIR®-based API for public health data exchange in § 170.315(g)(20). The new certification criterion in § 170.315(g)(20) would support ongoing and future development of public health FHIR IGs leveraging a core set of existing, modular, and extensible capabilities and standards. The standards referenced in the proposed § 170.315(g)(20) certification criterion support FHIR capabilities such as API-based event notifications (*i.e.,* FHIR Subscriptions), SMART App Launch, Bulk Data Export, and requirements for authorization and authentication, drawing on the Program's requirements for Health IT Modules certified to § 170.315(g)(10).

xiv. Bulk Data Enhancements

We propose, as discussed in section III.B.14, to adopt the HL7® FHIR® Bulk Data Access v2.0.0: STU 2 implementation specification (Bulk v2 IG) in § 170.215(d)(2). We also propose to require, in many of our proposed certification criteria that reference § 170.215(d)(2), server support for the ''group export'' operation and a ''_type'' query parameter for performance improvement. We believe this proposal would better support interoperability with Health IT Modules certified to support FHIR Bulk Data Access and better enable performant exporting of complete sets of FHIR resources for pre-defined cohorts of patients. This would raise the floor from our current Bulk v1 IG requirements for certification, where we require support for the group export operation but do not require support for any of the optional query parameters in the IG. We believe that these new certification requirements, based on additional implementer clarifications included in the Bulk v2 IG, would provide meaningful improvements in the performance of Bulk APIs. Additionally, we welcome comment on the issues hindering the effective exchange of population data using Bulk FHIR APIs and additional steps ONC can take to help address those issues.

xv. New Requirements To Support Dynamic Client Registration Protocol in the Program

We propose, as explained in section III.B.15, to add requirements in the Program to support dynamic client registration and subsequent authentication and authorization for dynamically registered apps for patient-facing, user-facing, and system confidential applications. This includes adding requirements to the following in the Program:

- § 170.315(g)(10) certification criterion
- § 170.315(g)(20), (30), and (32)–(35) proposed certification criteria
- § 170.315(j)(2), (5), (8), (11) proposed certification criteria
- API Conditions and Maintenance of Certification requirements in § 170.404

We propose to adopt the HL7® Unified Data Access Profiles (UDAP™) Security for Scalable Registration, Authentication, and Authorization Implementation Guide Release 1.0.0 implementation guide (UDAP Security IG v1), and we propose to require several specific sections of it to support requirements in the Program criteria listed above. This proposal would facilitate timelier patient, provider, and system access to health information using applications by providing a more uniform, standardized, and automated application registration pathway.

xvi. New Certification Criteria for Modular API Capabilities

We propose, as discussed in section III.B.16, to add a new category of certification criteria to § 170.315 titled ''modular API capabilities'' in § 170.315(j). Several proposals across this proposed rulemaking would establish capabilities necessary to support standardized APIs across clinical, public health, administrative, and other use cases. We propose that the certification criteria in § 170.315(j) would represent API capabilities that are standards-based, including through new standards, such as HL7® Clinical Decision Support (CDS) Hooks, SMART Health Cards, and HL7 FHIR® Subscriptions, as well as standards and functionalities historically referenced in § 170.315(g)(10). These modular API capabilities would be referenced and incorporated into Health IT Modules to support standardized APIs for clinical use cases in § 170.315(g)(10), public

[13] *https://www.gao.gov/products/gao-22-106175.*

health use cases in § 170.315(g)(20), and health insurance and coverage use cases in § 170.315(g)(30)-(36), as well as other future use cases across the health IT landscape.

xvii. Multi-Factor Authentication Criterion

As explained in section III.B.17, we propose to revise the ''multi-factor authentication'' (MFA) certification criterion in § 170.315(d)(13) and accordingly update the privacy and security (P&S) certification framework in § 170.550(h). The proposed update would revise our MFA certification criterion by replacing our current ''yes'' or ''no'' attestation requirement with a specific requirement to support multi-factor authentication and configuration for three certification criteria on and after January 1, 2028. We propose to apply the updated MFA requirements by revising each of the certification criteria in § 170.315(b)(3), (e)(1), (g)(10), and (g)(30) to require that a Health IT Module certified to these criteria also be certified to § 170.315(d)(13)(ii) on and after January 1, 2028. Given our proposal to embed § 170.315(d)(13) references into each applicable certification criterion, § 170.315(d)(13) does not need to be referenced again in § 170.550(h)(3), therefore, we propose to expire all the references to § 170.315(d)(13) in § 170.550(h)(3) by December 31, 2027. We believe these updates would match industry best practices for information security, particularly for important authentication use cases in certified health IT.

xviii. Revised Computerized Provider Order Entry—Laboratory Criterion

We propose, as discussed in section III.B.18, to update the ''computerized provider order entry—laboratory'' certification criterion in § 170.315(a)(2) to require enabling a user to create and transmit laboratory orders electronically according to the standard proposed in § 170.205(g)(2), the HL7® Laboratory Order Interface (LOI) Implementation Guide (IG). We further propose to update § 170.315(a)(2) to require technology to receive and validate laboratory results according to the standard proposed in § 170.205(g)(3), the HL7® Laboratory Results Interface (LRI) IG. Ensuring that systems creating laboratory orders can transmit orders and receive associated results and values electronically, according to national standards, would create more complete patient information available to clinicians throughout the laboratory workflow. We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to the criterion in § 170.315(a)(2) must update its Health IT Module and provide the updated version to its customers in order to maintain certification of that Health IT Module. We propose that any Health IT Modules seeking certification for the criterion in § 170.315(a)(2) on or after January 1, 2028, would need to be capable of supporting this functionality.

xix. Revised Standardized API for Patient and Population Services Criterion To Align With Modular API Capabilities

As discussed in section III.B.19, we propose to revise the certification criterion in § 170.315(g)(10) to reorganize requirements to improve clarity and align with new proposals in this rule, including proposed:

- restructuring of existing requirements to reference the ''modular API capabilities'' certification criteria proposed in § 170.315(j)
- support for dynamic registration and subsequent authentication and authorization of patient-facing, user-facing, and system confidential apps
- support for multi-factor authentication for patient-facing authentication according to requirements proposed in § 170.315(d)(13)(ii)
- support for imaging links in data response requirements
- support for a read and search API for system apps
- support for ''_type'' query parameter for Bulk FHIR API
- support for the issuance of verifiable health records as specified by the requirements proposed in § 170.315(j)(22)
- support for subscriptions as a server according to the requirements specified in proposed § 170.315(j)(23)
- support for workflow triggers for decision support interventions according to the requirements specified in proposed § 170.315(j)(20)
- support for authorization revocation for users (*e.g.,* clinicians)
- moving of the API documentation requirements in § 170.315(g)(10) to the API Conditions and Maintenance of Certification requirements in § 170.404

We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to the criterion in § 170.315(g)(10) must update its Health IT Module and provide the updated version to its customers in order to maintain certification of that Health IT Module. We propose that any Health IT Modules seeking certification for the criterion in § 170.315(g)(10) on or after January 1, 2028, would be to the updated version of the certification criterion.

xx. Patient, Provider, and Payer APIs

The combined exchange of clinical and administrative data among healthcare payers, patients, and providers is a complex challenge that can prevent participants in the healthcare system from gaining insights into the full picture of an individual's care. In order to realize the benefits of a more unified stream of clinical and administrative data, patients and health care providers must be able to more efficiently access and exchange EHI with the entities that steward this information, especially healthcare payers. In the CMS Interoperability and Patient Access Final Rule (85 FR 25510), which appeared in the **Federal Register** on May 1, 2020, and the CMS Interoperability and Prior Authorization Final Rule (89 FR 8758), which appeared in the **Federal Register** on February 8, 2024, CMS finalized policies for certain healthcare payers that it regulates [14] to facilitate patient access to clinical and administrative data held by payers; availability of information about provider networks; exchange of information between payers when beneficiaries patients change coverage; provider access to data held by payers; and electronic prior authorization.

As explained in section III.B.20, we propose a set of certification criteria in § 170.315(g)(30) through (36) that aim to complement and advance the policies that CMS has developed to increase patient, provider, and payer access to information. Health IT developers, including those that support payers, would be able to ensure that Health IT Modules certified to these proposed criteria, when used to satisfy the CMS requirements, have been tested for conformance with widely available industry standards designed to support interoperability for each use case. We propose to adopt a set of HL7® FHIR® IGs in § 170.215 to support these certification criteria, and to incorporate these specifications by reference in § 170.299.

[14] The ''impacted payers'' under the CMS Interoperability and Patient Access Final Rule (85 FR 25510) and the CMS Interoperability and Prior Authorization Final Rule (89 FR 8758) are Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

2. Conditions and Maintenance of Certification Requirements—Insights and Attestations

a. Insights Condition and Maintenance of Certification Requirements

As discussed in section III.C.1, we propose to update the Insights Condition by requiring health IT developers to include health care provider identifiers, for providers included in the data submitted in response for the measures specified in § 170.407, to allow us to better interpret the results of the data received. We also propose updates to the overall process for reporting and newer versions of certified health IT for responses submitted under the Insights Condition in § 170.407(b).

We also propose to update two measures under the Insights Condition. We propose to revise the ''individuals' access to electronic health information through certified health IT'' measure in § 170.407(a)(3)(i) to include both individuals and individuals' authorized representatives accessing their EHI. Additionally, we propose to revise the name of the measure in § 170.407(a)(3)(ii) to ''C–CDA reconciliation and incorporation through certified health IT'' and propose to require developers to submit responses on specific data classes and elements from C–CDA documents reconciled and incorporated both through manual and automated processes in § 170.407(a)(3)(ii)(E). We also intend to make various technical updates to the measure specification sheets accompanying the Insights Condition, including the clarification of certain definitions and terms, as well as adding new metrics.

b. Attestations Condition and Maintenance of Certification Requirements

As discussed in section III.C.2, we propose to revise the Attestations Condition and Maintenance of Certification requirements by adding the requirement in § 170.406(a)(2) that a health IT developer, as a Condition of Certification, attest to compliance with § 170.402(b)(4), if the health IT developer certified a Health IT Module(s) to the ''decision support interventions'' certification criteria in § 170.315(b)(11).

3. Administrative Updates

As discussed in section III.D.1, we propose to revise the Program correspondence provision (§ 170.505) to explicitly specify when applicants for ONC-Authorized Testing Laboratory (ATL) status, applicants for ONC–ACB status, ONC–ACBs, ONC–ATLs, health IT developers or any other party to a proceeding under subpart E of 45 CFR part 170 will be considered to have received correspondence or other written communication from ONC or the National Coordinator.

As discussed in section III.D.2, we propose to expand ONC–ACBs responsibilities under § 170.556 for conducting surveillance of developers' satisfaction of certain Maintenance of Certification requirements under the Program. We also propose new and revised principles of proper conduct (PoPCs) in § 170.523 to support the proposed expanded surveillance responsibilities. Specifically, an ONC–ACB would be required to monitor Program-participating developers' satisfaction of specific requirements applicable to the developers under subpart D of 45 CFR part 170, report results of these surveillance activities to ONC, and engage with developers where applicable to encourage corrective action for identified non-conformities. A new proposed PoPC in § 170.523(x), pursuant to a new proposed requirement in § 170.556(d)(7)(ii), would require ONC–ACBs to report to ONC when a developer fails to establish or to successfully complete an appropriate corrective action plan (CAP) for a Maintenance of Certification non-conformity identified by an ONC–ACB.

To increase efficiency for developers' documentation of their CAPs, and ONC–ACBs' review and monitoring of these plans, we propose in § 170.556(d)(3) to tailor the minimum required CAP elements based on the non-conformities addressed by the CAP. For example, certain CAP elements designed for non-conformities with certification criteria in 45 CFR subpart C would not be required by regulation in a CAP specific to a developer having missed a deadline in subpart D, such as for submission of real world testing documents (§ 170.405) or submission of attestations (§ 170.406).

As discussed in section III.D.3, we propose a requirement in § 170.523(m)(6) for ONC–ACBs, beginning January 1, 2027, to obtain a regular reporting of API discovery details, including service base URLs and related organization details, that are required by § 170.404(b)(2) and (b)(3). In section III.D.4, we propose a new PoPC for ONC–ACBs in § 170.523(y) requiring an ONC–ACB to give the National Coordinator sufficient notice of its intent to withdraw its authorization under the Program.

In section III.D.5, we discuss our proposal to update the ONC direct review regulatory framework in 45 CFR 170.580 to align with the proposed enhancements to the ONC–ACBs' role in surveillance of Program-participating developers' satisfaction of certain Maintenance of Certification requirements. To enhance efficiency for developers and ONC, we propose to revise direct review CAP regulatory requirements to add flexibility to tailor the minimum elements the developer must address in such a plan for a non-conformity substantiated through an ONC direct review. We also propose procedural revisions to § 170.581, suspension and termination of certification procedures in § 170.580(d) and (f), and hearing officer and appeals provisions in § 170.580(g)(5) and (7)(ii), to clarify that certain ''ONC'' decisions are in fact made by the National Coordinator, and explicitly provide for the Secretary to choose to exercise direct oversight of certain National Coordinator and hearing officer decisions before the decisions become final. We also propose to revise wording throughout 45 CFR 170.580 and 45 CFR 170.581 to clarify that certain determinations are made by the National Coordinator (who is appointed by the Secretary) rather than more generally by or within the Office of the National Coordinator (the organizational unit headed by the National Coordinator).

As discussed in section III.D.6, we propose to update paragraphs (a) and (b) of the certification ban provisions in § 170.581 to explicitly provide for the Secretary to review, at the Secretary's discretion, the National Coordinator's determination to impose a certification ban before the ban becomes effective. In section III.D.7, we propose to remove the ''Complete EHR'' and ''EHR Module'' terms from certain sections within subpart E of 45 CFR part 170.

As discussed in section III.D.8, we propose to codify a definition of *serious risk to public health or safety* for purposes of Program regulations in 45 CFR part 170. This definition would enhance understanding among developers and users of certified health IT of the types of conditions, events, or phenomena that would constitute a dangerous non-conformity to Program requirements if caused (or contributed to) by a product certified under the Program, even if the Health IT Modules within such product continued to pass lab testing procedures, in-the-field surveillance testing, or both with respect to the technical standards and certification criteria adopted in subparts B and C of part 170. As discussed in section III.D.9, we propose to remove § 170.550(m) ''time-limited certification and certification status for certain 2015 Edition certification criteria'' and to

remove certification criteria with time-limited certification and certification status, including § 170.315(a)(10), (a)(13), (b)(6), (e)(2), and (g)(8). Additionally, as discussed in section III.D.9, we propose to revise § 170.315(b)(7) and (b)(8) to remove § 170.315(b)(7)(ii) and (b)(8)(i)(B), which were time-limited provisions (now expired) that permitted health IT to demonstrate security tagging of Consolidated-Clinical Document Architecture (C–CDA) documents at the document level. In section III.D.10, we propose to revise § 170.550(h), the Privacy and Security Certification Framework requirements by adding the certification criterion ''decision support interventions'' in § 170.315(b)(11) to the list of certification criteria in § 170.550(h)(3)(ii).

4. Correction—Privacy and Security Certification Framework

We propose to make a correction to the Privacy and Security Certification Framework in § 170.550(h), as discussed in section III.E. We revised § 170.550(h) in the ONC Cures Act Final Rule but intended for § 170.550(h)(4) to remain unchanged. However, when we drafted the amendatory instructions, we erroneously included the instruction to revise all of paragraph (h) (85 FR 25952). Therefore, when the Code of Federal Regulations was updated, § 170.550(h)(4) was removed. We now propose to add the § 170.550(h)(4) that existed prior to the ONC Cures Act Final Rule being finalized.

5. Information Blocking Enhancements

In this rule, we propose revisions to defined terms for purposes of the information blocking regulations, which appear in 45 CFR 171.102. We propose to revise three existing exceptions in subpart B of 45 CFR part 171 and solicit comment on potential revisions to one exception in subpart D. We propose two new exceptions, one in each in subparts B and C of part 171. We propose to codify in § 171.401 definitions of certain terms relevant to the Trusted Exchange Framework and Common Agreement™ (TEFCA™) and in § 171.104 descriptions of certain practices that constitute interference with the access, exchange, and use of electronic health information (EHI).

As discussed in section IV.A.1, we propose to amend the definition of ''health care provider,'' codified in 45 CFR 171.10,2 so that it is explicitly clear that it references 42 U.S.C. 300jj(3) and that for purposes of this definition the terms ''laboratory'' and ''pharmacist'' have the meanings established for these terms in 42 U.S.C. 300jj(10) and (12), respectively. In IV.A.2, we propose that for purposes of the information blocking regulations in 45 CFR part 171 both ''health information technology'' and its shorter form, ''health IT,'' have the same meaning as ''health information technology'' in 42 U.S.C. 300jj(5).

For purposes of the information blocking definition (§ 171.103), the term ''interfere with or interference'' is currently defined in § 171.102. Informed by the concerns and questions that interested parties have brought to our attention, we propose in section IV.A.3 to add a section (§ 171.104) to the information blocking regulations that would codify certain practices (acts and omissions) that constitute interferences for purposes of the information blocking definition (codified in § 171.103). The proposed codified practices are not an exhaustive list; additional practices not described in the proposed § 171.104 that are likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI may also be considered to rise to the level of an interference. The proposed codification of these specific practices is intended to provide actors, and those who seek to engage in EHI access, exchange, or use with actors, certainty that these specific practices constitute interference. The codification of these practices may also help regulated entities and other interested parties to consider the likelihood that any practice an actor might contemplate or engage in may also meet the definition of ''interference'' and ''interfere with'' (as defined in § 171.102) for purposes of the information blocking regulations (45 CFR part 171).

For purposes of the information blocking Privacy Exception, the term ''individual'' is defined in § 171.202(a)(2). As currently worded, this text includes cross-references to incorrect citations within § 171.202(a)(2). The text also includes one unnecessary cross-reference citation within § 171.202(a)(2). We do not propose to change the substance of the definition, but in section IV.B.1.a, we propose technical corrections to the cross-reference citations within § 171.202(a)(2)(iii), (iv), and (v).

In section IV.B.1.b, to clearly establish coverage of the § 171.202(d) sub-exception for all actors' practices under the same requirements, we propose to change the name of the sub-exception to: ''interfering with individual access based on unreviewable grounds.'' This proposed change to the header text is intended to express the expansion of its availability to actors who are not Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities or business associates (as defined in 45 CFR 160.103). As explained in section IV.B.1.c, we propose to slightly modify the header of § 171.202(e) for ease of reference to ''Individual's request not to share EHI.'' More importantly, we propose to revise the § 171.202(e) sub-exception to remove the existing limitation that allows the exception to be used only for individual-requested restrictions on EHI sharing that are permitted by other applicable law. The proposal would extend the availability of the § 171.202(e) sub-exception to an actor's practice of applying restrictions the individual has requested on the access, exchange, or use of an individual's EHI even when the actor may have concern that another law applicable to some or all of the actor's operations could compel the actor to provide access, exchange, or use of EHI contrary to the individual's expressed wishes.

We propose, as discussed in section IV.B.2, revisions to three conditions of the Infeasibility Exception (45 CFR 171.204). Specifically, we propose to modify the § 171.204(a)(2) *segmentation* condition to enhance clarity and certainty, and to provide for its application to additional specific situations. We propose to revise the condition to specifically cross-reference additional information blocking exceptions under which an actor may choose to withhold EHI that the actor could, under applicable law, make available.

We propose to modify the § 171.204(a)(3) *third party seeking modification use* condition by changing the words ''health care provider'' to ''covered entity as defined in 45 CFR 160.103'' in the exclusion from applicability of this condition. We also propose in § 171.204(a)(3)(ii) to extend the exclusion from applicability of the *third party seeking modification use* condition requests for modification use from health care providers, as defined in § 171.102 and who are not covered entities, requesting such use from actors whose activities would make them a business associate of that same health care provider if the healthcare provider (actor) was covered by HIPAA.

We propose to modify the § 171.204(b) *responding to requests* condition by establishing different timeframes for sending written responses to the requestor based on the § 171.204(a) condition under which fulfilling the requested access, exchange, or use of EHI is infeasible. The proposed revision would retain the requirement that actors communicate to requestors ''in writing the reason(s) why the request is infeasible'' that we

finalized in the ONC Cures Act Final Rule. We discuss these proposals further in sections IV.B.2.a through c of this proposed rule.

In section IV.B.3, we propose a new Protecting Care Access Exception that would, under specified conditions (see sections IV.B.3.b through d and the draft regulatory text of proposed § 171.206), apply to acts or omissions likely to interfere with access, exchange, or use of particular EHI that an actor believes could create a risk of exposing patients, care providers, and other persons who assist in access or delivery of health care to potential administrative, civil, or criminal investigations or other actions on certain bases. A summary of these bases follows below in this section. (Please see section IV.B.3 of this proposed rule for detailed discussion.)

The proposed Protecting Care Access Exception (§ 171.206) would be a new exception in addition to the other information blocking exceptions. The proposed new exception is designed to create certainty for actors that certain practices for which no other exception would apply will not be considered ''information blocking'' under the information blocking statute (PHSA section 3022) and regulations (45 CFR part 171). Like any existing or proposed information blocking exception in 45 CFR part 171, the proposed Protecting Care Access Exception (§ 171.206) is not intended to override any provision of another law that is independently applicable to the actor.

The practices that the proposed Protecting Care Access Exception (§ 171.206) would except from the information blocking definition would be those implemented based on the actor's good faith belief that sharing EHI indicating that any person(s) sought, received, provided, or facilitated the provision or receipt of reproductive health care that was lawful under the circumstances in which it was provided could result in a risk of potential exposure to legal action for those persons and that the risk could be reduced by practices likely to interfere with particular access, exchange, or use of specific EHI. For purposes of the Protecting Care Access Exception, we propose to rely on the same definition of ''reproductive health care'' (which can be found in 45 CFR 160.103) that is used for purposes of the HIPAA regulations. In addition, we discuss in section IV.B.3.b how we would interpret whether care is ''lawful under the circumstances in which it is provided.''

To satisfy the proposed new Protecting Care Access (§ 171.206) Exception, an actor's practice would need to satisfy the threshold condition (§ 171.206(a)), and at least one of the other two conditions in the exception: the patient protection condition (§ 171.206(b)) or the care access condition (§ 171.206(c)). The combination of conditions required to satisfy the proposed new Protecting Care Access Exception and the definition of ''legal action'' (in § 171.206(d)) for purposes of the exception would, together, ensure that the exception would not apply to an actor's attempts to shield any person from legal action based on allegations that health care items or services the person provided are substandard.

These provisions together would also ensure that the exception focuses on the specific situation where an actor limits the sharing of EHI because the actor believes it could result in a risk of potentially exposing the patient or another person to an investigation or other civil, criminal, or administrative action based on the mere fact that the person sought, obtained, provided, or facilitated reproductive health care that was lawful under the circumstances in which it was provided. For instance, the exception would not apply to an actor's attempt to interfere with EHI sharing in order to reduce a patient's or other person's risk of exposure to a criminal investigation or charges not related to the act of seeking, obtaining, providing, or facilitating reproductive health care. For example, the act of not sharing information because of the risk of a criminal investigation related to operating a vehicle while intoxicated or committing fraud would not be covered under this exception.

The Protecting Care Access Exception's threshold condition (§ 171.206(a)), proposed in section IV.B.3.b, includes requirements that the practice be: undertaken based on the actor's belief as specified in § 171.206(a)(1), no broader than necessary as specified in § 171.206(a)(2), and be implemented consistent with a written organizational policy or case-by-case determination contemporaneously documented in writing as specified in § 171.206(a)(3). Meeting the threshold condition would be necessary, but not alone sufficient, for an actor's practice to be covered by the proposed Protecting Care Access (§ 171.206) exception. To satisfy the exception, any actor's practice likely to interfere with access, exchange, or use of EHI would also need to satisfy at least one of the other two conditions (in paragraphs (b) and (c)) of the proposed exception.

In section IV.B.3.c, we propose a patient protection condition (§ 171.206(b)), that can be met by practices implemented by the actor for the purpose of reducing a risk of potential legal action that the actor believes a patient could otherwise face because the EHI shows or invites a reasonable inference that the patient has or has done any of the following (see proposed § 171.206(b)(1)):

(i) obtained reproductive health care that was lawful under the circumstances in which it was provided;

(ii) Inquired about or expressed an interest in seeking reproductive health care; or

(iii) Particular demographic characteristics or any health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated.

The proposed patient protection condition would specify (§ 171.206(b)(2)) that to meet the condition the actor's practice must be subject to nullification by explicit request or directive from the patient. We also clarify (in proposed § 171.206(b)(3)) that for purposes of the patient protection condition's other paragraphs that ''patient'' means the natural person who is the subject of the EHI or another natural person referenced in, or identifiable from, the EHI as having sought or received reproductive health care.[15]

In section IV.B.3.d, we propose a care access condition (§ 171.206(c)) that can be met by practices an actor might choose to implement for the purpose of reducing a risk of potential exposure to legal action for licensed health care professionals, other health care providers, or persons involved in providing or in facilitating the provision or receipt of reproductive health care that is lawful under the circumstances in which such health care is provided. We request comment on multiple, potentially non-exclusive, alternative proposals for additional requirements under the care access condition that would function to restrict the exception's coverage of practices that interfere with access, exchange, or use in scenarios that also implicate the HIPAA Privacy Rule's individual right of access provisions (45 CFR 164.524). In order to satisfy this proposed condition, if finalized, the practice would need to meet the requirements finalized in § 171.206(c).

We propose clarifying provisions in § 171.206(d) (discussed in section

[15] The definition of ''person'' for purposes of 45 CFR part 171 is codified in § 171.102 and is, by cross-reference to 45 CFR 160.103, the same definition used for purposes of the HIPAA Privacy Rule (45 CFR part 160 and subpart E of 45 CFR part 164). The § 160.103 definition of ''person'' clarifies the meaning of ''natural person'' within it. We use ''natural person'' in this proposed rule with that same meaning.

IV.B.3.b of this proposed rule) and § 171.206(e) (discussed in section IV.B.3.e of this proposed rule). Proposed § 171.206(d) would clarify when reproductive health care sought, obtained, provided, or facilitated by someone other than the actor will be presumed to have been lawful for purposes of assessing whether an actor's practice meets the exception's patient protection or care access condition. In § 171.206(e) we propose to define ''legal action'' for purposes of § 171.206. We propose in section IV.B.4, a new information blocking exception: ''Requestor Preferences'' in 45 CFR 171.304. This exception would stand separate from and independent of other exceptions and would apply where an actor honors or adheres to a requestor's preference(s) expressed or confirmed in writing for: (1) limitations on the amount of EHI made available to the requestor; (2) the conditions under which EHI is made available to the requestor; and (3) when EHI is made available to the requestor for access, exchange, or use. The exception would offer an actor certainty that, so long as the actor's practices meet the conditions of the exception, the actor can honor or adhere to a requestor's preferences related to these specific preferences without concern that the actor may be engaging in ''information blocking'' as defined in 45 CFR 171.103.

We propose to add a new definitions section in § 171.401 for certain terms used in Subpart D, which we propose to align with the definitions used in the proposed 45 CFR 172. We seek comment on some aspects of the TEFCA Manner Exception in 45 CFR 171.403, including the limitation on its use for requests made via a FHIR API and the application of the Fees and Licensing Exceptions to practices that satisfy the exception.

6. Trusted Exchange Framework and Common Agreement™

Section 3001(c)(9) of PHSA, as added by the 21st Century Cures Act (Pub. L. 114–255, Dec. 13, 2016) (Cures Act), calls for the development or support of a ''trusted exchange framework, including a common agreement among health information networks nationally.'' On January 19, 2022, ONC published in the **Federal Register** the Notice of Publication of the Trusted Exchange Framework and Common Agreement (87 FR 2800), in which ONC published the Trusted Exchange Framework (TEF): Principles for Trusted Exchange and the Common Agreement for Nationwide Health Information Interoperability Version 1. ONC published in the **Federal Register** a notice titled Trusted Exchange Framework and Common Agreement Version 1.1 on November 7, 2023 (88 FR 76773), in which ONC published the Common Agreement for Nationwide Health Information Interoperability Version 1.1 (November 2023), and published version 2.0 implementing the latest industry standards among other changes on May 1, 2024 (89 FR 35107). Section 3001(c)(9)(A) of the PHSA states that the overall goal for TEFCA™ is to ensure full network-to-network exchange of health information. ONC intends to accomplish this by establishing a floor for interoperability under TEFCA across the country. The Common Agreement [16] is authorized by section 3001(c)(9)(B)(i) of the statute, which addresses: baseline legal and technical requirements for the Common Agreement, organizational and operational policies to enable exchange, minimum conditions for exchange, and a process for filing and adjudicating noncompliance with its terms. The Common Agreement addresses all of these to enable users in different health information networks (HINs) to securely share information with each other—all under commonly agreed-to expectations and terms. The Trusted Exchange Framework,[17] authorized under the same provision of the PHSA, describes a common set of principles for policies and practices to facilitate data-sharing.

The Recognized Coordinating Entity® (RCE™) is an ONC contractor that is charged with helping ONC to develop, operationalize, and update the Common Agreement, as well as assist ONC in stewarding the Qualified Health Information Network™ (QHIN™) Technical Framework (QTF),[18] which provides the technical specifications for how QHINs connect to one another. The RCE also helps ONC to oversee QHIN-facilitated network operations and QHIN compliance with the Common Agreement.

As explained in the proposed part 172 of subchapter D of title 45 of the Code of Federal Regulations, by standardizing health information exchange across many different networks, TEFCA will help to ensure full network-to-network exchange of health information. Doing so will simplify exchange by significantly reducing the number of connections (*e.g.,* portals) that individuals, health care providers, and other interested parties need to make to get the health information they seek. It does so by creating baseline governance, legal, and technical requirements that will enable secure information sharing across different networks nationwide, including: a common method for authenticating trusted network participants, a common set of rules for trusted exchange, organizational and operational policies to enable the exchange of health information among networks, and a process for filing and adjudicating noncompliance with the terms of the Common Agreement. As explained in proposed part 172, we believe that TEFCA will help lower the cost and expand the nationwide availability of secure health information exchange capabilities. The availability of TEFCA-based services, such as electronic address directories and patient record location, will also help scale health information exchange nationwide and usher in new support for FHIR API usage and adoption. FHIR API usage and adoption has become a centerpiece of the interoperability initiatives of ONC and other U.S. government agencies such as CDC,[19] CMS,[20] Health Resources and Services Administration (HRSA),[21] and the Veteran's Administration (VA).[22]

In section V of this proposed rule, we propose to implement certain provisions related to TEFCA in order to provide greater process transparency and further implement section 3001(c)(9) of the PHSA, as added by the Cures Act. We propose to add a new part, part 172, to subchapter D of title 45 of the Code of Federal Regulations to implement certain provisions related to the TEFCA. These proposed provisions would establish the processes associated with the qualifications necessary for an entity to receive and maintain Designation (as we propose to define that term in § 172.102) as a QHIN capable of trusted exchange under the Common

[16] Common Agreement for Nationwide Health Information Interoperability, Version 1.1 (November 2023), *available at* **Federal Register**:: Trusted Exchange Framework and Common Agreement Version 1.1.

[17] The Trusted Exchange Framework (TEF): Principles for Trusted Exchange (January 2022), *available at https://www.healthit.gov/sites/default/files/page/2022-01/Trusted_Exchange_Framework_0122.pdf.*

[18] Qualified Health Information Network (QHIN) Technical Framework, Version 1.0 (January 2022), *available at https://rce.sequoiaproject.org/wp-content/uploads/2022/01/QTF_0122.pdf.*

[19] *See* CDC, Public Health Informatics Office (PHIO), *https://www.cdc.gov/csels/phio/it_takes_practice.html.*

[20] *See* CMS, Policies and Technology for Interoperability and Burden Reduction, *https://www.cms.gov/policies-and-technology-interoperability-and-burden-reduction.*

[21] *See* HRSA, Uniform Data System (UDS) Modernization Initiative, *https://bphc.hrsa.gov/data-reporting/uds-training-and-technical-assistance/uniform-data-system-uds-modernization-initiative.*

[22] *See* VA, VA Technical Reference Model v 23.12, *https://www.oit.va.gov/Services/TRM/StandardPage.aspx?tid=8233.*

Agreement. The proposals would also establish the procedures governing Onboarding (as we propose to define that term in § 172.102) of QHINs and Designation of QHINs, suspension, termination, and administrative appeals to ONC, as described in the sections below. We believe establishing these provisions in regulation would support reliability, privacy, security, and trust within TEFCA, which would further TEFCA's ultimate success.

In subpart A, we propose the statutory basis, purpose, and scope of the TEFCA provisions in part 172; the applicability of the TEFCA provisions in part 172; and relevant definitions. In subpart B, we propose requirements related to the qualifications needed to be Designated, as proposed to be defined in § 172.102. In subpart C, we describe the proposed QHIN Onboarding and Designation processes. In subpart D, we propose RCE and QHIN suspension rights, notice requirements for suspension, and the requirements related to the effect of suspension. In subpart E, we propose RCE and QHIN termination rights, notice requirements for termination, and requirements related to the effect of termination. In subpart F, we propose to establish QHIN appeal rights and the process for filing an appeal to ONC. These appeal rights would ensure that a QHIN, or Applicant QHIN, that (1) disagrees with certain RCE determinations or (2) believes an action or inaction by a QHIN or the RCE could threaten TEFCA's integrity will have recourse to appeal such determination, action, or inaction to ONC.

In subpart G, we propose requirements related to QHIN attestation for the Adoption of TEFCA. This subpart implements section 3001(c)(9)(D) of the PHSA. Section 3001(c)(9)(D)(i) requires the publication on ONC's website of those HINs that have adopted the Common Agreement and are capable of trusted exchange pursuant to the Common Agreement. Section 3001(c)(9)(D)(ii) requires HHS to establish, through notice and comment rulemaking, a process for HINs that voluntarily elect to adopt TEFCA to attest to such adoption.

C. Severability

It is our intent that if any provision of this rule were, if or when finalized, held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or stayed pending further judicial or agency action, such provision shall be severable from other provisions of this rule, and from rules and regulations currently in effect, and not affect the remainder of this rule. It is also our intent that, unless such provision shall be held to be utterly invalid or unenforceable, it be construed to give the provision maximum effect permitted by law including in the application of the provision to other persons not similarly situated or to other, dissimilar circumstances from those where the provision may be held to be invalid or unenforceable.

In this rule, we propose provisions that are intended to and will operate independently of each other, even if multiple of them serve the same or similar general purpose(s) or policy goal(s). Where a provision is necessarily dependent on another, the context generally makes that clear (such as by cross-reference to a particular standard, requirement, condition, or pre-requisite). Where a provision that is dependent on one that is stayed or held invalid or unenforceable (as described in the preceding paragraph) is included in a subparagraph, paragraph, or section within part 170, 171, or 172 of 45 CFR, we intend that other provisions of such subparagraph(s), paragraph(s), or section(s) that operate independently of said provision would remain in effect.

To ensure our intent for severability of provisions is clear in the CFR, we propose to add to existing § 170.101 and § 171.101, and to include in the proposed new § 172.101 a paragraph stating our intent that if any provision is held to be invalid or unenforceable it shall be construed to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

D. Costs and Benefits

Executive Orders 12866 and 13563 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). Executive Order 14094 entitled ''Modernizing Regulatory Review'' (hereinafter, the Modernizing E.O.) amends section 3(f) of Executive Order 12866 (Regulatory Planning and Review). The amended section 3(f) of Executive Order 12866 defines a ''significant regulatory action'' as an action that is likely to result in a rule that may: (1) have an annual effect on the economy of $200 million or more (adjusted every 3 years by the Administrator of the Office of Information and Regulatory Affairs (OIRA) for changes in gross domestic product); or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, territorial, or Tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise legal or policy issues for which centralized review would meaningfully further the President's priorities or the principles set forth in this Executive Order, as specifically authorized in a timely manner by the Administrator of OIRA in each case. OMB has determined that this proposed rule is a significant regulatory action, as the potential economic impacts associated with this proposed rule could be greater than $200 million per year. Accordingly, we have prepared a Regulatory Impact Analysis (RIA) that, to the best of our ability, presents the costs and benefits of this proposed rule. We have estimated the potential monetary costs and benefits of this proposed rule for the health IT community, including costs and benefits as they relate to health IT developers, health care providers, patients, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out by section. In accordance with E.O. 12866, we have included the RIA summary table as Table 82.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2022 dollars as it is the most recent data available to address all cost and benefit estimates consistently. The wages used to derive the cost estimates are from the May 2022 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics.[23] We also note that estimates presented in sections titled ''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 Proposed Regulations'' are used throughout this RIA.

We estimate that the total annual cost for this proposed rule for the first year

[23] May 2022 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. *https://www.bls.gov/oes/current/oes_nat.htm.*

after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would result in $431.1 million. The total undiscounted perpetual cost over a 10-year period for this proposed rule (starting in year two), based on the cost estimates outlined above, would result in $398.1 million. We estimate the total costs to health IT developers to be $829.2 million.

We estimate the total annual benefit across all entities for this proposed rule beginning in Year 3, when the associated policies are required to be implemented and expected benefits to be realized, would be on average $22.2 million. We estimate the total benefits across all entities to be $177.6 million. We estimate the total undiscounted perpetual annual net benefit for this proposed rule (starting in year three), based on the estimates outlined above, would result in a net benefit of $75.4 million.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (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 healthcare quality, safety, and efficiency through the promotion of health IT and EHI exchange.

The 21st Century Cures Act (Pub. L. 114–255) (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, through Title IV—Delivery, amended the HITECH Act by modifying or adding certain provisions to the PHSA relating to health IT.

Section 119 of Title I, Division CC of the Consolidated Appropriations Act, 2021, Public Law 116–260 (CAA), enacted on December 27, 2020, requires sponsors of prescription drug plans to implement one or more real-time benefit tools (RTBTs) that meet the requirements described in the statute, after the Secretary has adopted a standard for RTBTs and at a time determined appropriate by the Secretary. For purposes of the requirement to implement a real-time benefit tool in section 1860D–4(o)(1) of the Social Security Act, described above, the CAA provides that one of the requirements for an RTBT is that it can integrate with electronic prescribing and EHR systems of prescribing healthcare professionals for the transmission of formulary and benefit information in real time to such professionals. The statute requires incorporation of RTBTs within both the Medicare Part D prescription drug program and the ONC Health IT Certification Program (Program). Specifically, the law amends the definition of a ''qualified electronic health record'' (qualified EHR) in section 3000(13) of the PHSA to require that a qualified EHR must include (or be capable of including) an RTBT.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two Federal advisory committees, the Health IT Policy Committee (HITPC) and the Health IT 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 4003(e) of the Cures Act amended sections 3002 and 3003 of the PHSA by replacing, in an amended section 3002, the HITPC and HITSC with one committee named the Health Information Technology Advisory Committee (Health IT Advisory Committee or HITAC). Section 3002(a) of the PHSA, as added by the Cures Act, establishes that the HITAC recommends to the National Coordinator policies and standards, implementation specifications, and certification criteria, relating to the implementation of a health information technology infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information. Further described in section 3002(b)(1) of the PHSA, this includes recommending to the National Coordinator a policy framework to advance interoperable health information technology infrastructure, updating recommendations to the policy framework, and making new recommendations, as appropriate. Section 3002(b)(2)(A) of the PHSA specifies that in general, the HITAC shall recommend to the National Coordinator for purposes of adoption under section 3004, standards, implementation specifications, and certification criteria and an order of priority for the development, harmonization, and recognition of such standards, specifications, and certification criteria. Like the process previously required of the former HITPC and HITSC, section 3002(b)(5) of the PHSA requires the HITAC to develop a schedule, updated annually, for the assessment of policy recommendations, which the Secretary publishes in the **Federal Register**.

Section 3004 of the PHSA establishes 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 such standards, implementation specifications, or certification criteria. Section 3004(a)(3) requires the Secretary to publish all such determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA, 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 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. ONC Health IT Certification Program Rules

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. 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 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. Section 13201(b) of the HITECH Act requires that, with respect to the development of

standards and implementation specifications, the Director of NIST shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. 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 4003(b) of the Cures Act added section 3001(c)(9)(B)(i) to the PHSA, which requires the National Coordinator ''to convene appropriate public and private stakeholders'' with the goal of developing or supporting a Trusted Exchange Framework and a Common Agreement (collectively, ''TEFCA'') for the purpose of ensuring full network-to-network exchange of health information. Section 3001(c)(9)(B) outlines provisions related to the establishment of a Trusted Exchange Framework for trust policies and practices and a Common Agreement for exchange between health information networks (HINs)—including provisions for the National Coordinator, in collaboration with the NIST, to provide technical assistance on implementation and pilot testing of TEFCA. Section 3001(c)(9)(C) requires the National Coordinator to publish TEFCA on its website and in the **Federal Register**. Section 3001(c)(9)(D)(i) requires the National Coordinator to publish a list of HINs that have adopted TEFCA. Section 3001(c)(9)(D)(ii) requires the Secretary to establish a process for HINs to attest that they have adopted TEFCA.

Section 4002(a) of the Cures Act amended section 3001(c)(5) of the PHSA by adding section 3001(c)(5)(D), which requires the Secretary, through notice and comment rulemaking, to require conditions of certification and maintenance of certification for the Program. Specifically, the health IT developers or entities with technology certified under the Program must, in order to maintain such certification status, adhere to certain conditions and maintenance of certification requirements concerning information blocking; assurances regarding 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 in accordance with section 3009A(b) of the PHSA.

B. Regulatory History

The Secretary issued an interim final rule with request for comments on January 13, 2010, ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology'' (75 FR 2014), which adopted an initial set of standards, implementation specifications, and certification criteria. On March 10, 2010, the Secretary issued a proposed rule, ''Proposed Establishment of Certification Programs for Health Information Technology'' (75 FR 11328), that proposed both temporary and permanent certification programs for the purposes of testing and certifying health IT. A final rule establishing the temporary certification program was published on June 24, 2010, ''Establishment of the Temporary Certification Program for Health Information Technology'' (75 FR 36158), and a final rule establishing the permanent certification program was published on January 7, 2011, ''Establishment of the Permanent Certification Program for Health Information Technology'' (76 FR 1262).

We have engaged in multiple rulemakings to update standards, implementation specifications, certification criteria, and the Program, a history of which can be found in the October 16, 2015 final rule ''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). The history can be found at 80 FR 62606. A final rule making corrections and clarifications 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 minimum capabilities and specified the related minimum standards and implementation specifications that Certified EHR Technology (CEHRT) would need to include to 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 Programs and the Promoting Interoperability performance category under MIPS) when the 2015 Edition is required for use under these and other programs referencing the CEHRT definition. The final rule also 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 Principles of Proper Conduct (PoPC) for ONC–ACBs.

After issuing a proposed rule on March 2, 2016, ''ONC Health IT Certification Program: Enhanced Oversight and Accountability'' (81 FR 11056), we published a final rule by the same title (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 set forth processes for us to authorize and oversee accredited testing laboratories under the Program. In addition, it included 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) (ONC Cures Act 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. We also requested comment in the ONC Cures Act Proposed Rule (84 FR 7467) as to whether certain health IT developers should be required to participate in 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, with the goal of developing or

supporting TEFCA for the purpose of ensuring full network-to-network exchange of health information.

On May 1, 2020, a final rule was published titled, ''21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program'' (85 FR 25642) (ONC Cures Act Final Rule). The final rule implemented certain provisions of the Cures Act, including Conditions and Maintenance of Certification requirements for 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 implemented certain parts of the Cures Act to support patients' access to their EHI, and the implementation of information blocking policies that support patient electronic access. Additionally, the final rule modified the 2015 Edition health IT certification criteria and Program in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs, as well as improving patient and health care provider access to EHI and promoting competition. On November 4, 2020, the Secretary published an interim final rule with comment period titled, ''Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency'' (85 FR 70064) (Cures Act Interim Final Rule). The interim final rule extended certain compliance dates and timeframes adopted in the ONC Cures Act Final Rule to offer the healthcare system additional flexibilities in furnishing services to combat the COVID–19 pandemic, including extending the applicability date for information blocking provisions to April 5, 2021.

On April 18, 2023, the Secretary published a proposed rule titled, ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing'' (88 FR 23746) (HTI–1 Proposed Rule). The HTI–1 Proposed Rule proposed to implement the Electronic Health Record (EHR) Reporting Program provision of the Cures Act by establishing new Conditions and Maintenance of Certification requirements for health IT developers under the Program. The HTI–1 Proposed Rule also proposed to make several updates to certification criteria and implementation specifications recognized by the Program, including revised certification criterion for: ''clinical decision support'' (CDS), ''patient demographics and observations'', and ''electronic case reporting.'' The HTI–1 Proposed Rule also proposed to establish a new baseline version of the United States Core Data for Interoperability (USCDI). Additionally, the HTI–1 Proposed Rule proposed enhancements to support information sharing under the information blocking regulations.

On January 9, 2024, the Secretary issued the ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing'' final rule (HTI–1 Final Rule), which implemented the EHR Reporting Program provision of the 21st Century Cures Act and established new Conditions and Maintenance of Certification requirements for health IT developers under the Program (89 FR 1192). The HTI–1 Final Rule also made several updates to certification criteria and standards recognized by the Program. The Program updates included revised certification criteria for ''decision support interventions,'' ''patient demographics and observations,'' and ''electronic case reporting,'' as well as adopted a new baseline version of the USCDI standard, USCDI Version 3. Additionally, the HTI–1 Final Rule provided enhancements to support information sharing under the information blocking regulations. Through these provisions, we sought to advance interoperability, improve algorithm transparency, and support the access, exchange, and use of EHI. The HTI–1 Final Rule also updated numerous technical standards in the Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs for health IT developers and users of health IT.

On November 15, 2023, the Secretary issued a proposed rule titled, ''Medicare Program; Contract Year 2025 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly; Health Information Technology Standards and Implementation Specifications'' (88 FR 78476). This proposed rule proposed to adopt the National Council for Prescription Drug Programs (NCPDP) Real-Time Prescription Benefit standard version 13.

On June 17, 2024, the Secretary issued the Part D and Health IT Standards final rule (89 FR 51238 through 51265). This final rule adopted the NCPDP Real-Time Prescription Benefit standard version 13 in 45 CFR 170.205(c)(1) and to incorporate this standard by reference in 45 CFR 170.299. In this final rule, CMS also adopted requirements for Part D sponsors to use the standard in in 45 CFR 170.205(c)(1) when implementing an RTBT.

III. ONC Health IT Certification Program Updates

A. Standards and Implementations 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 [24] 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 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 it is 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. In this proposed rule, we use voluntary consensus standards except for:

- The USCDI v4 standard. We propose to adopt USCDI v4 in § 170.213. This standard is a hybrid of government 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);
- The Federal Information Processing Standard (140–2) related to the

[24] *https://www.whitehouse.gov/wp-content/uploads/2020/07/revised_circular_a-119_as_of_1_22.pdf.*

protection of electronic health information adopted in § 170.210;

- The CMS standards for QRDA I and III respectively adopted in § 170.205(h)(2) and (k)(3).

We are not aware of any voluntary consensus standards that could serve as an alternative for the purposes we describe in further detail throughout this proposed rule, including for establishing a baseline set of data that can be commonly exchanged across care settings for a wide range of uses. We refer readers to section III.B.1 of this preamble for a discussion of the USCDI.

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 implementation specifications in any subsequent 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 implementation specification includes the entire document unless we specify otherwise. For example, if we adopted the SMART Application Launch Framework Implementation Guide Release 2.2 (SMART v2.2) proposed in this proposed rule (see section III.B.2), 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 supersede 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(a)). To comply with these requirements, in section VI (''Incorporation by Reference'') of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we propose to adopt and subsequently incorporate by reference in the Code of Federal Regulations. To note, we also provide relevant information about these standards and implementation specifications throughout the relevant sections of the proposed rule.

B. New and Revised Standards and Certification Criteria

1. The United States Core Data for Interoperability Version 4 (USCDI v4)

a. Background and USCDI v4 Update

The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and data elements for the sharing of electronic health information.[25] We established USCDI as a standard in the ONC Cures Act Final Rule (85 FR 25670), adopting USCDI Version 1 (USCDI v1) in § 170.213 and incorporating it by reference in § 170.299.[26] In a final rule titled ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing'' (HTI–1 Final Rule) and published on January 9, 2024, we adopted USCDI Version 3 (USCDI v3) in § 170.213 and incorporated it by reference in § 170.299 (89 FR 1210 through 1223).

The USCDI standard in § 170.213 is a baseline set of data that can be commonly exchanged across care settings for a wide range of uses. Certain certification criteria in § 170.315 currently require the use of one of the versions of the USCDI standard in § 170.213. USCDI is also referenced by HHS programs and used by the healthcare community to align interoperability requirements and national priorities for health IT across industry initiatives. For the overall structure and organization of USCDI, including data classes and data elements, please see *www.healthIT.gov/USCDI.*

As described in the ONC Cures Act Final Rule, we use a predictable, transparent, and collaborative process to expand the USCDI standard, including providing the opportunity for public comment (85 FR 25670). Additionally, as described in the ONC Cures Act Final Rule, health IT developers can use the Standards Version Advancement Process (SVAP) to voluntarily implement and use the most recent National Coordinator-approved version of USCDI without waiting for ONC to require that newer version via rulemaking (85 FR 25669). ONC uses a public comment process to identify newer versions of standards for approval by the National Coordinator as part of SVAP.[27] USCDI v3 was available for voluntary implementation through SVAP as of September 2023.

Based on feedback ONC received through the ONC New Data Element and Class submission system, ONC identified a set of data elements and data classes for a draft version of USCDI v4, which was released in January 2023. The draft version of USCDI v4 included 20 new data elements and one new data class as well as updates to minimum standard code set versions. ONC then finalized and released USCDI v4 in July 2023.

We propose to update the USCDI standard in § 170.213 by adding USCDI v4. We propose that for purposes of the Program, the adoption of USCDI v3 expires on January 1, 2028. We propose to add USCDI v4 in § 170.213(c) and incorporate it by reference in § 170.299. We propose that as of January 1, 2028, any Health IT Modules seeking certification to criteria referencing § 170.213 would need to be capable of exchanging the data elements that the USCDI v4 comprises. The additional data elements in USCDI v4 reflect many of the recommendations expressed by the Health IT Advisory Committee in their report to the National Coordinator.[28] As finalized in the HTI–1 Final Rule, beginning on January 1, 2026, only USCDI v3 will be available in § 170.213 as the USCDI standard for use by developers of certified health IT (89 FR 1215). This proposed rule would advance the USCDI standard to USCDI v4, continuing ONC's commitment to a transparent and predictable schedule for health IT developers with respect to updates to the USCDI's regulatory baseline. If finalized, this proposal would provide significant clarity and certainty to health IT developers who would have substantial time to update certified health IT to support USCDI v4.

For certification to a criterion in § 170.315 that references the USCDI standard adopted in § 170.213, we propose that a Health IT Module must use at least one of the versions of the USCDI standard that is (1) adopted in § 170.213 or approved by SVAP at the time the Health IT Module seeks certification and (2) not expired at the time of use. When a Health IT Module certified to a criterion in § 170.315 that references the USCDI standard adopted in § 170.213 is using a version with an

[25] *https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.*

[26] *https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-170#p-170.213.*

[27] *https://www.healthit.gov/isa/standards-version-advancement-process.*

[28] *https://www.healthit.gov/sites/default/files/page/2023-05/2023-04-12_IS_WG_USCDI_v4_Transmittal_Letter_508.pdf.*

upcoming expiration date or is using an interim version approved by SVAP, we propose that the health IT developer must update the Module to either a new version of the standard adopted in § 170.213 or a subsequent version approved by SVAP prior to the expiration date or dates defined in order to maintain certification of that Health IT Module as described in § 170.315. Consistent with the health IT developer must provide the updated Health IT Module to their customers by the expiration date or dates defined in order to maintain certification of that Health IT Module as described in § 170.315. We describe these proposals further in section III.B.1.b below.

b. Certification Criteria That Reference USCDI

The USCDI standard is currently cross-referenced in certain certification criteria (see § 170.213). A Health IT Module can be certified to any of these criteria by ensuring that it complies with any unexpired version of the USCDI included in § 170.213 or a version of the USCDI standard that is approved through SVAP at the time the Health IT Module seeks certification. The certification criteria that currently cross-reference to USCDI via § 170.213 are as follows:

- ''Care coordination—Transitions of care—Create'' (§ 170.315(b)(1)(iii)(A)(*1*) and (*2*));
- ''Care coordination—Clinical information reconciliation and incorporation—Reconciliation'' (§ 170.315(b)(2)(iii)(D)(*1*)–(*3*));
- ''Decision support interventions—Decision support configuration'' (§ 170.315(b)(11)(ii)(A) and (B), and (iv)(A)(*5*)–(*13*)));
- ''Patient engagement—View, download, and transmit to 3rd party—View'' (§ 170.315(e)(1)(i)(A)(*1*) and (*2*), and (iii));
- ''Transmission to public health agencies—electronic case reporting'' (§ 170.315(f)(5)(i)(C)(*2*)(*i*));
- ''Design and performance—Consolidated CDA creation performance'' (§ 170.315(g)(6)(i)(A) and (B));
- ''Design and performance—Application access—all data request—Functional requirements'' (§ 170.315(g)(9)(i)(A)(*1*) and (*2*)); and
- ''Design and performance—Standardized API for patient and population services—Data response'' (§ 170.315(g)(10)(i)(A) and (B)).

We propose that up to and including December 31, 2027, a Health IT Module certified to criteria referencing § 170.213 may use either USCDI v3 or USCDI v4. We propose that by January 1, 2028, a health IT developer of a Health IT Module certified to criteria referencing § 170.213 must update to USCDI v4 and provide the updated version to their customers in order to maintain certification of that Health IT Module. We also note that if these proposals are finalized, for any time before January 1, 2026, USCDI v1 could still be used to meet the applicable certification criteria as well (see 89 FR 1211 through 1223).

Further, we propose that Health IT Modules certified to certification criteria that reference § 170.213 would need to update their Health IT Modules to accommodate USCDI v4 data elements using the FHIR® US Core Implementation Guide Version 7.0.0 proposed in § 170.215(b)(1)(iii) and the HL7 CDA R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes, Edition 3—US Realm, proposed in § 170.205(a)(1). We also propose that adoption of the standards in § 170.205(a)(6) and § 170.215(b)(1)(ii) expire on January 1, 2028. As stated in the HTI–1 Final Rule, our intent would be to adopt the version of these standards necessary for developers of certified health IT to have appropriate implementation guidance to meet the certification criteria that reference USCDI v4, and these updated implementation guides best align with and support effective implementation of USCDI v4. Based on public comments on HTI–1 and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such determinations so that the adopted version of standards are the most up-to-date available and are feasible for real-world implementation (see 89 FR 1215).

2. SMART App Launch 2.2

In the ONC HTI–1 Final Rule, we adopted the HL7® FHIR® SMART Application Launch Framework Implementation Guide Release 2.0.0 (SMART v2 Guide), a profile of the OAuth 2.0 specification, in § 170.215(c)(2) (89 FR 1291 through 1295). Public comments received during the HTI–1 rulemaking process indicated near universal support for the adoption of the SMART v2 Guide, with the caveat that several of these commenters suggested we adopt the newest balloted version of the SMART App Launch IG, which at the time of the HTI–1 public comment period was version 2.1. We declined to adopt the newest balloted version of the SMART App Launch IG in the HTI–1 Final Rule, noting that the SMART v2 Guide had ''already been an established part of the Program via SVAP and rigorously tested . . .'' (89 FR 1292). However, we also noted that ''[w]e will consider potential ways the SMART v2.1 IG could be included in the Program in the future . . .'' (89 FR 1292).

We note that current ONC policy as established in the ONC Cures Act Final Rule (85 FR 25741) and reiterated in the HTI–1 Final Rule (89 FR 1293) is that as part of supporting the SMART App Launch ''permission-patient'' capability, 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. Furthermore, we finalized in the HTI–1 Final Rule (89 FR 1294) that as part of supporting the SMART App Launch ''permission-v2'' capability Health IT Modules must support certain sub-resource scopes for the Condition and Observation resources. Specifically, we established minimal conformance requirements at the category level for the Condition and Observation resources using specifications and guidance from the SMART v2 Guide and FHIR US Core 6.1.0 implementation guides to ensure that Health IT Modules required to support the SMART v2 Guide are capable of supporting the finer-grained resource constraints capability without being overly prescriptive in setting expectations for how the Health IT Module implements such capabilities.

In this proposed rule, we clarify the existing Program requirements to support patient authorization using SMART App Launch capabilities. Specifically, we clarify that if both the ''permission-patient'' and ''permission-v2'' capabilities are required in support of patient authorization for certification to a criterion in the Program, then a Health IT Module must support the following:

- Support for the ability for patients to authorize an application to receive their EHI based on individual FHIR resource-level and individual sub-resource-level scopes.
- Support for the ability for patients to authorize an application to receive their EHI based on individual sub-resource-level scopes when corresponding resource-level scopes are requested.

These requirements enable patients to have the ability to authorize access to their EHI at a more granular level in alignment with required SMART App Launch authorization capabilities. The capabilities enabled by these requirements empower patients with authorization ability at the individual sub-resource level, and the ability to provide granular authorization at the

individual sub-resource level even if the authorization request from the app is made at the resource level. We note that both the ''permission-patient'' and ''permission-v2'' capabilities are required as part of the ''Permissions'' subsection of the SMART App Launch IGs proposed in § 170.215(c)(2) and § 170.215(c)(3). We propose ''Permissions'' in § 170.315(j)(9), which is cross-referenced in § 170.315(g)(10) and § 170.315(g)(30) in this proposed rule. We anticipate that future certification criteria will also include ''permission-patient'' and ''permission-v2'' support requirements to support of patient authorization and we intend for this clarification to support patient authorization of individual sub-resource level scopes to also apply.

Specific guidance and requirements regarding the implementation of resource and sub-resource scopes are included in the US Core 7.0.0 implementation guide. We clarify for the purposes of certification under the Program, support for the US Core IG includes supporting all SMART App Launch scope requirements included in the US Core IG, including requirements to support resource and sub-resource scopes.

We note throughout this rule we propose revisions to existing API certification criteria and propose new API certification criteria wherein specificity in the requirements regarding the properties of applications is important. To provide a consistent and industry standard definition of app types referenced in Program API certification criteria, we clarify that ''confidential app,'' ''public app,'' and ''native app'' as referenced in this rule and in Program API requirements refers to ''confidential client,'' ''public client,'' and ''native application'' respectively as defined in internet Engineering Task Force (IETF) Request for Comments (RFC) 6749 ''The OAuth 2.0 Authorization Framework.'' [29]

The SMART Application Launch Framework Implementation Guide, Release 2.2 (SMART v2.2 Guide), published at the end of April 2024, is the most recent version available at the time of this proposed rule. The SMART v2.2 Guide includes features that iterate on the features of the SMART v2 Guide, including the enhancements from the SMART v2.1 Guide and the latest industry consensus updates.

Notable enhancements in the SMART v2.2 Guide include a more detailed and standardized ''fhirContext'' parameter, including the ability for servers to include optional ''roles'' for offering a detailed description of included resource references in the ''fhirContext'' parameter; updates to the ''fhirUser'' context parameter to allow the use of the ''PractitionerRole'' resource for representing the current user authorizing the launch; and clarification regarding the ''exp'' field in the token introspection response, ensuring consistency between the ''exp'' field in the token introspection response and the ''expires_in'' interval in the original access token response. Additionally, to eliminate ambiguity in URL resolution, the SMART v2.2 Guide mandates the use of absolute URLs in the Well-Known configuration file, disallowing relative URLs. The SMART v2.2 Guide also introduces a new Cross-Origin Resource Sharing (CORS) security requirement applicable to servers supporting purely browser-based apps. Finally, an important new addition to the SMART v2.2 Guide is the User-Access Brands and Endpoints (Brands) specification, which allows API providers to publish Brands associated with their FHIR Endpoints to enable apps to collect and present these Brands to users (*e.g.,* patients).

Overall, these enhancements to the SMART v2.2 Guide improve standardization and provide clarity to help support consistent implementation and improve interoperability. We welcome comment on our assessment of these SMART v2.2 Guide changes.

Based on HTI–1 public comment feedback and to make use of the new Brands specification in the Program, we propose to adopt the SMART v2.2 Guide in § 170.215(c)(3) and incorporate it by reference as a subparagraph in § 170.299. Additionally, we propose that the adoption of the SMART v2 Guide in § 170.215(c)(2) would expire on January 1, 2028. If we finalize these proposals, developers of certified health IT with Health IT Modules certified to criteria referencing the implementation specifications in § 170.215(c) may use the SMART v1, SMART v2, or SMART v2.2 Guides for the time period up to and including December 31, 2025. Then by January 1, 2026, when the adoption of SMART v1 expires, developers of certified health IT with Health IT Modules certified to criteria referencing the implementation specifications in § 170.215(c) must update to the SMART v2 or SMART v2.2 Guides and provide the updated version to their customers in order to maintain certification of that Health IT Module. Finally, by January 1, 2028, when the adoption of the SMART v2 Guide expires, developers of certified health IT with Health IT Modules certified to criteria referencing the implementation specifications in § 170.215(c) must update to the SMART v2.2 Guide and provide the updated health IT module to their customers in order to maintain certification of that Health IT Module. We propose that any Health IT Modules seeking certification to criteria referencing the implementation specifications in § 170.215(c) on or after January 1, 2028, would need to be capable of supporting the SMART v2.2 Guide.

Our proposal to require health IT developers participating in the program to update and provide to customers Health IT Modules updated to according to the timelines for the implementation specifications in § 170.215(c) includes all certification criteria that reference the implementation specifications in § 170.215(c) directly, or via reference to our proposed modular API capabilities certification criteria in § 170.315(j)(6), (j)(7), (j)(8), (j)(9), and (j)(10) that also reference the implementation specifications in § 170.215(c). In this proposed rule these certification criteria are: § 170.315(g)(10), (g)(20), (g)(30), (g)(32), (g)(33), (g)(34), and (g)(35). We note that § 170.315(g)(20), (g)(30), (g)(32), (g)(33), (g)(34), and (g)(35) are new Program certification criteria proposed in this rule and the only currently finalized certification criterion in the Program that includes a reference to § 170.215(c) is § 170.315(g)(10).

To reference the SMART Guide across these proposed new and revised certification criteria, we propose to move the SMART Guide component references (*e.g.,* specific capabilities and sections) out of the subparagraphs in § 170.215(c), so that only entire SMART Guide references are listed under § 170.215(c). This will enable the SMART Guides to be referenced across Program certification criteria, whilst also enabling references to specific SMART Guide components tailored to the requirements of a specific certification criterion. For example, the proposed § 170.315(j)(9) certification criterion as proposed in the section titled ''New Certification Criteria for Modular API Capabilities'' would reference § 170.215(c) along with a list of applicable SMART Guide components tailored specifically to describe SMART Guide requirements for patient authorization for standalone apps.

We note that later versions of the SMART Guide may be finalized by the time of our final rule. During the time between our proposed rule and our final rule, the FHIR community may, for example, issue technical corrections in a SMART v2.2.x Guide or release a

[29] IETF RFC 6749 ''The OAuth 2.0 Authorization Framework'' available here: *https://datatracker.ietf.org/doc/rfc6749/.*

newer SMART v2.x Guide minor release. We intend to evaluate and potentially adopt in the final rule the most recent available version of the SMART Guide that aligns with the SMART v2.2 Guide changes outlined in this proposed rule. We encourage interested parties to monitor the SMART App Launch IG directory of published versions (*https://hl7.org/fhir/smart-app-launch/history.html*) for all IG iterations, technical corrections, and releases. We welcome comment on this proposal.

3. User-Access Brands and Endpoints

In the ONC HTI–1 Final Rule, we finalized requirements in § 170.404(b)(2) for Certified API Developers to publish certain service base URLs and related organization (*i.e.,* API Information Source) details in a standardized FHIR® format (89 FR 1285 through 1290). Public comments received during the HTI–1 rulemaking process indicated strong support for the ''continued development and standardization of publication formats for FHIR 'service base URLs' '' (89 FR 1286). Many of these commenters suggested we adopt a FHIR implementation guide, with a particular emphasis on the Patient-access Brands (PAB) specification. We declined to adopt PAB or any other FHIR implementation guides for § 170.404(b)(2) at the time, and instead finalized more generalized base FHIR requirements to best ensure compatibility with the emerging industry FHIR implementation guides. Given the particular interest in the PAB specification we noted in HTI–1 that ''[w]e will consider the Patient-access Brands specification for adoption in future rulemaking as it develops'' (89 FR 1288).

Currently, the PAB specification, now referred to as ''User-access Brands and Endpoints,'' (and referred to as Brands herein) is set for publication as a sub-specification in the SMART v2.2 Guide. The Brands specification ''defines FHIR profiles for Endpoint, Organization and Bundle resources that help users connect their apps to health data providers.'' [30] It provides guidelines for API providers to publish Brands associated with their FHIR endpoints that apps can collect and present to users. Each Brand can include information like organization name, location, identifiers, patient portal details, FHIR API Endpoints, and more. These Brands are assembled in FHIR ''Bundle'' format, and these Bundles can made available in two ways: by FHIR servers including a link in their SMART ''.well-known/smart-configuration'' [31] metadata file, or through vendor-consolidated Brand Bundles that are openly published.

We propose to update our current maintenance of certification (MoC) requirements in § 170.404(b)(2) that reference FHIR resources and elements directly and adopt Brands in § 170.404(b)(2)(iii) as a replacement. Specifically, we propose to reorganize the regulation text paragraphs in a way that places existing service base URL requirements into § 170.404(b)(2)(ii) that expire on December 31, 2027. We propose in our updated § 170.404(b)(2)(iii) to require that, by January 1, 2028, service base URLs and related API Information Source details, including each organization's name, location, and facility identifier, must be published in an aggregate vendor-consolidated ''FHIR Bundle'' according to the Brands specification. Additionally, we propose to move our existing publication terms and quarterly review and update requirements, that we have currently finalized in § 170.404(b)(2) and (b)(2)(iii)(B), to subparagraphs under § 170.404(b)(2)(i) that apply broadly to other sub-paragraphs under § 170.404(b)(2), including our new proposed Brands requirements in § 170.404(b)(2)(iii). Finally, we propose that a health IT developer may meet the proposed revised MoC requirements by satisfying the new conformance requirements proposed in § 170.404(b)(2)(i), (iii), and (iv) in lieu of § 170.404(b)(2)(i) and (ii) prior to December 31, 2027.

We believe that our proposed changes to § 170.404(b)(2) logically build on our existing MoC requirements in § 170.404(b)(2) because the Brands specification uses profiles of the same base FHIR resources (*i.e.,* ''Endpoint,'' ''Organization,'' and ''Bundle'') we have finalized in § 170.404(b)(2). Requiring the use of the more standardized FHIR profiles in Brands that are designed specifically for the endpoint publication use case reduces inconsistent and varied implementations leading to increased interoperability. We also believe that our proposed changes to § 170.404(b)(2) align with much of the public feedback we received during the HTI–1 rulemaking process where the Brands precursor PAB specification was cited numerous times (89 FR 1286 through 1289). We welcome comment on this proposal to reference Brands for publication of service base URLs and related organization details in § 170.404(b)(2).

Additionally, in our revised § 170.404(b)(3) where we propose new requirements for the publication of API discovery details for payer network information, including service base URLs and API Information source details, we propose to adopt Brands specification. Please see section III.B.20.d for further details on proposed § 170.404 updates.

We note that the Brands specification is a sub-specification in the SMART v2.2 Guide and we anticipate that subsequent versions of Brands will be included in subsequent versions of the SMART Guide. We also note that our proposed January 1, 2028 date for the SMART v2.2 Guide to be the minimum version in § 170.215(c) (see section III.B.2 for our proposal to adopt the SMART v.2.2 Guide in § 170.215(c)) matches the date that health IT developers subject to the requirements in § 170.404(b)(2) must support Brands for publication of API discovery details for patient access.

As we noted in section III.B.2, later versions of the SMART Guide may be finalized by the time of our final rule. This includes changes to the Brands specification, or potential corrections if identified, and we intend to evaluate and potentially adopt in the final rule the most recent available version of the SMART Guide if doing so would best support interoperability and effective program implementation. We encourage interested parties to monitor the SMART App Launch IG directory of published versions (*https://hl7.org/fhir/smart-app-launch/history.html*) for all IG iterations, technical corrections, and releases. We welcome comment on this proposal.

4. Standards for Encryption and Decryption of Electronic Health Information

a. Background

In the 2015 Edition Final Rule, ONC adopted the October 8, 2014, version of Annex A: Approved Security Functions for Federal Information Processing Standards (FIPS) Publication 140–2. This October 8, 2014, version was the most recent version published by the National Institute of Standards and Technology (NIST) when the 2015 Edition Final Rule published (80 FR 62707).

b. Proposal

Since finalizing the October 8, 2014, version of Annex A: Approved Security Functions for FIPS Publication 140–2 standard in the 2015 Edition Final Rule,

[30] *https://hl7.org/fhir/smart-app-launch/STU2.2/brands.html.*

[31] *https://hl7.org/fhir/smart-app-launch/STU2.2/brands.html#metadata-in-well-knownsmart-configuration.*

encryption techniques and security best practices have continued to advance, and NIST has published several updated versions of Annex A: Approved Security Functions for FIPS Publication 140–2.[32] The most recent version of Annex A for FIPS Publication 140–2 is Draft, October 12, 2021. We propose to adopt the Draft, October 12, 2021, version of Annex A for FIPS Publication 140–2 in § 170.210(a)(3) and incorporate it by reference as a subparagraph in § 170.299. We also propose that the adoption of the FIPS 140–2 October 8, 2014, version in § 170.210(a)(2) expire on January 1, 2026. We note that the FIPS 140–2 October 8, 2014, version was inadvertently removed from § 170.299, therefore we propose to incorporate by reference the standard in § 170.299(m)(3). We welcome comment on these proposals.

We note that revising § 170.210(a) would implicate three certification criteria that reference standards in § 170.210(a):

- § 170.315(d)(7) End-user device encryption, which we propose to revise and rename as ''Health IT encryption'' elsewhere in this preamble;
- § 170.315(d)(9) Trusted connection; and
- § 170.315(d)(12) Encrypt authentication credentials, which we propose to further revise and rename as ''Protect stored authentication credentials'' elsewhere in this preamble.

Given the cross reference to § 170.210(a)(2) in these certification criteria, we propose to revise each certification criterion in § 170.315(d)(7), (d)(9), and (d)(12) to replace ''standard'' with ''at least one version of the standard'' and ''§ 170.210(a)(2)'' with ''§ 170.210(a)'' where appropriate in each certification criterion. At revised § 170.315(d)(7)(iv) we propose to revise both ''standard'' and ''§ 170.210(a)(2)'' in this manner. In § 170.315(d)(9)(i) and (ii); and at revised § 170.315(d)(12)(i)(A), we also propose to revise ''standard'' and ''§ 170.210(a)(2)'' in this manner. As noted, we describe our remaining proposed revisions to § 170.315(d)(7) and § 170.315(d)(12) elsewhere in this preamble at III.B.11 and III.B.12 and we invite readers to review those sections.

Additionally, we propose to remove the standard found in § 170.210(f) that is no longer referenced in any active certification criteria. We welcome comments on our proposals.

Finally, we solicit comment on the transition to the next FIPS standard, FIPS 140–3, that is currently underway.[33] We are monitoring development in this area, and we welcome comment on FIPS 140–3 and any potential impacts to our Program requirements. We note that Annex A for FIPS 140–2 is compatible with current FIPS 140–3 guidance as an ''Approved Security Function,'' and we intend to re-evaluate the latest FIPS 140–3 guidance at the time of the final rule to ensure continued capability with FIPS 140–3.[34] We recognize the potential for changes in FIPS 140–2 and 140–3 by the time of our final rule. Therefore, we intend to consider and potentially finalize the most recent Approved Security Functions that align with current FIPS guidance at the time and that are compatible with the Annex A for FIPS 140–2 update we are proposing in this proposed rule. We welcome comment on this proposal.

5. Minimum Standards Code Sets Updates

We established a policy in the 2015 Edition Final Rule for minimum standards code sets that update frequently (80 FR 62612). In the final rule entitled ''Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology'' (77 FR 54163) we discussed the benefits of adopting newer versions of minimum standards code sets, including the improved interoperability and implementation of health IT with minimal additional burden (77 FR 54170). As we stated in the HTI–1 Final Rule, when determining whether to propose newer versions of minimum standards code sets, we consider the impact on interoperability and whether a newer version would require substantive effort for developers of certified health IT to implement (89 FR 1224). If adopted, newer versions of minimum standards code sets would serve as the baseline for certification and developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis. We reiterate that while minimum standard code sets update frequently, perhaps several times in a single year, these updates are confined to concepts within the code system, not substantive changes to the standards themselves.

For certification to a criterion in § 170.315 that references the standard adopted in § 170.207, we propose that a Health IT Module must use at least one of the versions of the standard that is (1) adopted in § 170.207 or approved by SVAP at the time the Health IT Module seeks certification and (2) not expired at the time of use. We also propose that when a Health IT Module certified to a criterion in § 170.315 that references the standard adopted in § 170.207 is using a version with an upcoming expiration date or is using an interim version approved by SVAP, the health IT developer must update the Module to either a new version of the standard adopted in § 170.207, or a subsequent version approved by SVAP, prior to the expiration date or dates defined in order to maintain certification of that Health IT Module as described in § 170.207. In addition, the health IT developer must provide the updated Health IT Module to their customers by the expiration date or dates defined in § 170.207 in order to maintain certification of that Health IT Module as described in § 170.315.

- § 170.207(a)—Problems

We propose to revise § 170.207(a)(2), which is currently reserved, to reference SNOMED CT®, U.S. Edition, September 2023 Release and incorporate it by reference in § 170.299. We also propose that the adoption of the standard in § 170.207(a)(1), SNOMED CT, U.S. Edition, March 2022 Release, would expire on January 1, 2028, and that the adoption of the standard in § 170.207(a)(4), IHTSDO SNOMED CT, U.S. Edition, September 2015 Release, would expire on January 1, 2026.

- § 170.207(c)—Laboratory tests

We propose to revise § 170.207(c)(2) to reference Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.76, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. and incorporate it by reference in § 170.299. We also propose that the adoption of the standard in § 170.207(c)(1), LOINC Database Version 2.72, would expire on January 1, 2028, and that the adoption of the standard in § 170.207(c)(3), LOINC Database version 2.52, would expire on January 1, 2026.

- § 170.207(d)—Medications

We propose to revise the citations in § 170.207(d) to improve organization of

[32] *See* pages 4–6 of the October 12, 2021 version of Annex A for a revision history of the standard. Available at: *https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.*

[33] *See* FIPS 140–3 Transition Effort page—*https://csrc.nist.gov/projects/fips-140-3-transition-effort.*

[34] The ''10. Approved Security Functions'' requirements in FIPS 140–3 (March 22, 2019 version) state that ''Approved security functions include those that are . . . adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.'' The October 12, 2021 draft version of Annex A for FIPS 140–2 meets that criterion to contain ''Approved Security Functions'' according to FIPS 140–3. *See https://csrc.nist.gov/pubs/fips/140-3/final.*

this section. Specifically, we propose to revise § 170.207(d)(1) to list standards for clinical drugs and to reference multiple releases of RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine. We propose in § 170.207(d)(1)(ii) to reference RxNorm, December 4, 2023 Full Monthly Release and incorporate it by reference in § 170.299. We propose to move the standard adopted in § 170.207(d)(1), RxNorm, July 5, 2022 Release, to § 170.207(d)(1)(i), and that the adoption of this standard would expire on January 1, 2028. We propose to move the standard adopted in § 170.207(d)(3), RxNorm, September 8, 2015 Release, to § 170.207(d)(1)(iii) and that the adoption of this standard would expire on January 1, 2026. Finally, we propose to move National Drug Codes, currently included via cross-reference in § 170.207(d)(4), to § 170.207(d)(2). We note that § 170.207(d)(2) is currently reserved. We also propose to reserve § 170.207(d)(3) and remove § 170.207(d)(4).

- § 170.207(e)—Immunizations

We propose to reference in § 170.207(e)(5) the CDC National Center of Immunization and Respiratory Diseases (NCIRD) Code Set (CVX)—Vaccines Administered, updates through September 29, 2023, and incorporate it by reference in § 170.299. We also propose to reference in § 170.207(e)(6) the National Drug Code (NDC)—Vaccine NDC Linker, updates through November 6, 2023, and incorporate it by reference in § 170.299. We propose that adoption of the standards in § 170.207(e)(1), the HL7® Standard Code Set CVX—Vaccines Administered, dated through June 15, 2022, and § 170.207 (e)(2), NDC—Vaccine NDC Linker, dated July 19, 2022, would expire on January 1, 2028. We also propose that adoption of the standards in § 170.207(e)(3), HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015, and § 170.207(e)(4), NDC—Vaccine NDC Linker, updates through August 17, 2015, would expire on January 1, 2026.

- § 170.207(f)—Race and Ethnicity

We propose to revise § 170.207(f)(1) to include recent updates to the U.S. Office of Management and Budget's Statistical Policy Directive No. 15: Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity (SPD 15). In § 170.207(f)(1)(i) we propose to include The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997 with an expiration date of January 1, 2026 for adoption of that standard. In § 170.207(f)(1)(ii) we propose to include the U.S. Office of Management and Budget's Statistical Policy Directive No. 15: Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity (SPD 15), as revised, March 29, 2024.

We propose to revise § 170.207(f)(2) to include CDC Race and Ethnicity Code Set standards. In § 170.207(f)(2)(i) we propose to include CDC Race and Ethnicity Code Set Version 1.0 (March 2000) with an expiration of January 1, 2026, for adoption of that standard. In § 170.207(f)(2)(ii) we propose to include CDC Race and Ethnicity Code Set Version 1.2 (July 08, 2021) and incorporate it by reference in § 170.299. We propose to remove and reserve § 170.207(f)(3).

- § 170.207(m)—Numerical references

We propose that adoption of the standard in § 170.207(m)(1), The Unified Code of Units of Measure, Revision 1.9, would expire on January 1, 2026.

- § 170.207(n)—Sex

We propose that adoption of the standard in § 170.207(n)(1), HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor, would expire on January 1, 2026. We propose to revise § 170.207(n)(2) to reference use of at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a). We also propose to revise § 170.207(n)(3) to reference use of at least one of the versions of LOINC specified in § 170.207(c).

- § 170.207(o)—Sexual orientation and gender information

We propose to revise § 170.207(o)(1)–(3) to reference use of at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a) instead of § 170.207(a)(4). We also propose to revise § 170.207(o)(4) to reference use of at least one of the versions of LOINC specified in § 170.207(c).

- § 170.207(p)—Social, psychological, and behavioral data

We propose to revise § 170.207(p)(1) through (8) to reference use of at least one of the versions of LOINC specified in § 170.207(c).

We propose to revise § 170.207(p)(4), (5), (6), (7), and (8) to reference use of at least one of the versions of the standard specified in § 170.207(m).

- § 170.207(r)—Provider type

We propose that adoption of the standard in § 170.207(r)(1) would expire on January 1, 2026.

- § 170.207(s)—Patient insurance

We propose that adoption of the standard in § 170.207(s)(1), Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011), would expire on January 1, 2026.

In addition to updating the minimum standards code sets listed above, we propose to update the certification criteria that reference those minimum standards. These certification criteria include §§ 170.315(a)(12), 170.315(b)(1)(iii)(B)(*2*) and (G)(*3*), 170.315(c)(4)(iii)(C), (E), (G), (H), and (I), 170.315(f)(1)(i)(B)–(C), 170.315(f)(3)(ii) and (f)(4)(ii).

6. New Imaging Requirements for Health IT Modules

Diagnostic images are critical to supporting care in a variety of healthcare settings. Clinicians routinely use diagnostic images to support patient care and patients can better facilitate and coordinate care when they have access to their own images. Diagnostic images are often stored in systems external to an EHR, such as picture archiving and communication systems (PACS), vendor neutral archives (VNA), or other imaging platforms. While radiologists, ophthalmologists, dermatologists, pathologists, and other imaging specialists generally have direct access to full diagnostic quality images on these systems, access to both diagnostic quality and lesser quality images for referring providers can be inconsistent, depending on how broadly the hospitals or provider practice deploys access to their imaging infrastructure.

While certain images may be exchanged electronically in an automated manner, patients are often provided their diagnostic quality images on physical media (*e.g.,* compact disc read-only memory (CD–ROM)) to physically transport to their next clinical visit. Some PACS and VNA systems provide access to images through a web-based viewer, but those web-based viewers are often not accessible outside of the hospital or practice's immediate network.

In the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology (2014 Edition Final Rule), ONC adopted an ''Image Results'' certification criterion to

support the CMS EHR Incentive Program requirement, also known as the Meaningful Use or ''MU Stage 2 Objective'' requirement, that required eligible clinicians, eligible hospitals, and critical access hospitals to have access to imaging results and information through Certified EHR Technology (77 FR 54172).[35] The certification criterion required a Health IT Module to indicate the availability of a patient's images and narrative interpretations and enable access to those images and narrative interpretations. ONC stated that the requirements of this certification criterion could be met via the capability to directly link to images stored in the EHR system or providing a context-sensitive link to an external application which provides access to images and their associated narrative. We also stated in the 2014 Edition Final Rule that the use of the Digital Imaging and Communications in Medicine (DICOM) standard (or any other imaging standards) was unnecessary to meet the functional requirement expressed in the imaging results certification criterion (77 FR 54173). Instead, we reiterated our understanding stated in the 2014 Edition Proposed Rule that the adoption of standards was unnecessary to enable users to electronically access images and their narrative interpretations, as required by this certification criterion (77 FR 13838).

In the 2015 Edition Proposed Rule, ONC proposed to maintain the ''Imaging Results'' certification criterion (80 FR 16822) and while some commenters supported this proposal, ONC ultimately removed the ''Imaging Results'' certification criterion in the 2015 Edition Final Rule because the associated CMS EHR Incentive Programs objective (now referred to as Promoting Interoperability objectives) was removed and no longer required technological support (80 FR 62683). Instead, we finalized a certification criterion related to imaging in § 170.315(a)(3) ''Computerized provider order entry—diagnostic imaging,'' which is currently available for certification in the Program and requires that a Health IT Module enable a user to record, change, and access diagnostic imaging orders.

We acknowledge there are certain use cases and circumstances where image access via physical media may be more appropriate than network access (*e.g.,* locations without adequate network capabilities). However, we believe the prevalence of CD–ROMs and other physical media to share diagnostic quality images across healthcare settings indicates a lack of interoperability and access to imaging results that represents a continued burden for patients and clinicians. The widespread use of CD–ROMs and other physical media to share diagnostic quality images persists despite the adoption of PACS and VNA systems, the implementation of web-based viewers for diagnostic imaging, and the emergence of electronic standards and profiles meant to facilitate medical image access and exchange. For instance, the DICOM standard establishes a service-based process for web-based medical imaging, DICOMweb™. The Integrating the Healthcare Enterprise (IHE) XCPD, XCA, and XCA–I profiles support electronic transactions that can be used to facilitate medical imaging access. While these standards and others currently exist, there is not yet a clear consensus or full adoption of these pathways in health IT.

ONC believes that promoting access to and the exchange of images via Program requirements may encourage more widespread adoption and integration of these already existing pathways and reduce burdens caused by physical media exchange. Therefore, we propose to revise three certification criteria by adding new provisions to include support of a link to diagnostic imaging: ''transitions of care'' in § 170.315(b)(1); ''application access—all data request'' in § 170.315(g)(9); and ''standardized API for patient and population services'' in § 170.315(g)(10). We describe in subsequent paragraphs the criterion-specific details of the proposals to require support for imaging links in the Program. We believe that support for imaging links in these certification criteria will promote the availability of electronic image access for patients and providers. To enable a consistent understanding of ''imaging link'' across certification criteria requirements in the Program, we propose to define ''imaging link'' in § 170.102 to be ''technical details which enable the electronic viewing or retrieval of one or more images over a network.'' The proposed definition of ''imaging link'' is intended to be sufficiently broad to include the technical details used by the protocols and technologies implemented by industry to view and retrieve images. We also note that there is no specific standard associated with the support of this link, and that the functionality of this requirement can be met with a context-sensitive link to an external application which provides access to images and their associated narrative. The DICOMweb standard (*e.g.,* DICOM PS3.18 2023d—Web Services) [36] is likely to be among the standards widely used by hospitals and providers to support imaging links, but the Health IT Module certified to these certification criteria is not required to support a specific standard. We also clarify that although this proposal does not include specific security standards, we expect the appropriate authentication and authorization processes to be supported to prevent unauthorized access via the imaging links required in this proposal. For example, health IT developers may consider SMART Health Links as one possible standard by which to generate secure links to patient images.

We propose to revise the § 170.315(b)(1) ''Transitions of care'' certification criterion to support imaging links by adding imaging links to the data required to be supported in the ''Create'' functionality in § 170.315(b)(1)(iii) by adding a new paragraph in § 170.315(b)(1)(iii)(H). The ''Create'' functionality in § 170.315(b)(1)(iii) specifies the requirement to enable a user to create a transition of care/referral summary formatted in accordance with the standard specified in § 170.205(a)(3), (4), and (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates including at a minimum the data described under § 170.315(b)(1)(iii)(A)—(G). We propose specifically to add a paragraph in § 170.315(b)(1)(iii)(H) to indicate on and after January 1, 2028 imaging links are a part of the minimum ''Create'' requirements in § 170.315(b)(1)(iii).

We propose to revise the § 170.315(g)(9) ''Application access—all data request'' certification criterion to support imaging links by adding imaging links to the data required to be supported in responses to requests for patient data in a summary record formatted according to the data response requirements at paragraphs in § 170.315(g)(9)(i)(A)(*1*) and (*2*). Specifically, we propose to add a paragraph § 170.315(g)(9)(i)(A)(*3*)(*v*) that indicates on and after January 1, 2028 imaging links are required to be supported as part of the data response requirements in § 170.315(g)(9)(i)(A)(*1*) and (*2*). We also propose to revise the data response requirements in paragraphs § 170.315(g)(9)(i)(A)(*1*) and (*2*) to reference the data requirements proposed in § 170.315(g)(9)(i)(A)(*3*)(*v*).

[35] For more discussion regarding ONC's support of the CMS EHR Incentive Program, Stage 2 Meaningful Use, please *see: https://www.cms.gov/newsroom/fact-sheets/cms-proposes-definition-stage-2-meaningful-use-certified-electronic-health-records-ehr-technology.*

[36] *https://dicom.nema.org/medical/dicom/2023d/.*

We propose to revise the § 170.315(g)(10) ''Standardized API for patient and population services'' certification criterion to support imaging links by adding imaging links to the data required to be supported for data response for patients and users and for data response for systems. Specifically, we propose to add imaging links as data required to be supported on and after January 1, 2028 in data response for patients and users consistent with FHIR and US Core requirements at the paragraph proposed in § 170.315(g)(10)(ii)(B)(*1*). Additionally, we propose to add imaging links as data required to be supported on and after January 1, 2028 in data response for systems consistent with FHIR and US Core requirements proposed in § 170.315(g)(10)(iii)(B)(*1*), and the Bulk FHIR API data response for systems in accordance with FHIR, US Core, and Bulk Data Access, including the ''_type'' query parameter, requirements proposed in § 170.315(g)(10)(iii)(B)(*2*) and § 170.315(g)(10)(iii)(B)(*2*)(*ii*).

We also propose to revise the ''view, download, and transmit to 3rd party'' certification criterion in § 170.315(e)(1) to add functional support for viewing and download of diagnostic quality and lower quality images as well as inclusion of an imaging link to those diagnostic images in either a downloaded or transmitted Continuity of Care Document (CCD). We propose that Health IT Modules support this functionality on and after January 1, 2028. Specifically, we propose to add both diagnostic quality images and reduced quality images to the data that must be supported for viewing by patients (and their authorized representatives) according to paragraph (e)(1)(i)(A) by including support for diagnostic quality images and reduced quality images at the proposed paragraph (e)(1)(i)(A)(*8*). Furthermore, we propose to include imaging links in the requirements in § 170.315(e)(1)(i)(B)(*2*)(*i*) and (*ii*) specifying the data required to be included at a minimum in ambulatory summaries and inpatient summaries respectively be downloadable in accordance with the requirements specified at paragraph (e)(1)(i)(B)(*2*), which details the download requirements for ambulatory summaries and inpatient summaries downloaded according to the standard specified in § 170.205(a)(4) through (6) following the CCD document template. Finally, we propose that patients (and their authorized representatives) must be able to use technology to download both diagnostic quality and reduced quality images at the proposed § 170.315(e)(1)(i)(B)(*4*). Like broad requirements proposed in § 170.315(e)(1)(i)(A)(*8*), we propose that Health IT Modules certified to § 170.315(e)(1) support these specific scenarios on and after January 1, 2028. Again, there is no standard specified for either the images or the imaging links in the proposed requirements, though we anticipate that DICOM and the DICOMweb standard (such a—DICOM PS3.18 2023d—Web Services) are likely to be among standards widely used by hospitals and providers to support images and imaging links respectively.

We believe it is important to support the ability to view and download both diagnostic and lower quality images. While it is critical for patients to have access to diagnostic imaging, lower quality images are also important and, for example, a patient may decide that it is useful to have the lower quality images for quick reference. This revised certification criterion requires that both types of imaging be supported for viewing and for direct downloading by patients.

The view and download requirements of this certification criterion could be met via the capability to directly link to images stored in the Health IT Module or providing a context-sensitive connection to an external application which provides access to images and their associated narrative. In either case, however, the view and download functionalities must be accessible to the patient through the same internet-based technology as the other functionalities of § 170.315(e)(1). Electronic exchange of the image itself does not need to be included as part of the § 170.315(e)(1)(C) ''Transmit to third party'' functionality. However, similar to the proposals for the other certification criteria discussed above, an imaging link to the images accessible to the patient must be provided.

We propose that on and after January 1, 2028, a Health IT Module seeking certification to any of the certification criteria in § 170.315(b)(1), (e)(1), (g)(9), and (10), must meet the proposed requirements for imaging links. We note that health IT developers are also required to meet the Assurances Condition of Certification maintenance requirement in § 170.402(b)(3) that any health IT developer with a Health IT Module certified to these certification criteria would need to update their Health IT Modules and provide the updated version to their customers, including the most recently adopted capabilities and standards included in the revised certification criteria order to maintain certification of that Health IT Module. We welcome comments on these proposals.

7. Revised Clinical Information Reconciliation and Incorporation Criterion

We propose to revise the ''Clinical information reconciliation and incorporation'' (CIRI) certification criterion in § 170.315(b)(2). These proposed revisions are intended to expand our existing CIRI certification requirements to additional data elements and promote new capabilities that would benefit providers by reducing the burden of reconciliation and incorporation in clinical workflows.

Our requirements for CIRI in the Program were first established in the ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology'' Jan. 13, 2010, interim final rule to enable a user to electronically compare two or more medication lists (75 FR 2014). We subsequently expanded these requirements in the 2014 Edition Final Rule to require clinical information reconciliation and incorporation for three data types: problems, medications, and medication allergies (77 FR 54222). We noted in the 2010 interim final rule that there was, ''. . . great promise in making this [reconciliation] capability more comprehensive'' and that we ''anticipate exploring ways to improve the [reconciliation] utility of this capability. . .'' (75 FR 44613). In the 2014 Edition Final Rule we also noted our agreement with public comments that said providers ''should have some control over how exactly they want to be able to incorporate data into their EHR technology as part of their practice/organization'' (77 FR 54219).

Building on our CIRI strategy and in response to public feedback, we propose to revise § 170.315(b)(2) to require Health IT Modules to support reconciliation and incorporation of all USCDI data elements. In the context of the CIRI workflow in § 170.315(b)(2), we propose that upon receipt of a transition of care/referral summary all USCDI data elements must be supported, at a minimum, for reconciliation and incorporation by a user in § 170.315(b)(2)(v). We also propose in § 170.315(b)(2)(vi) user configuration functionality to enable a user to set individual or organizational rules that allow automatic reconciliation and incorporation for each data class included in at least one of the versions of the USCDI standard in § 170.213, including functionality that allows the

user to select trusted data and trusted data sources for automatic reconciliation and incorporation. Finally, as part of our proposed revision to the CIRI certification criterion in § 170.315(b)(2), we propose system verification functionality in § 170.315(b)(2)(vii) that requires Health IT Modules to be able to create a file formatted according to the Continuity of Care Document template.

We propose to implement this by requiring Health IT Modules certified to § 170.315(b)(2) to meet the requirements in§ 170.315(b)(2)(i), (ii), (iii), and (vii), or the requirements in (iv), (v), (vi) and (vii) for the time period up to and including December 31, 2027. On and after January 1, 2028, we propose that Health IT Modules certified to § 170.315(b)(2) must meet the requirements in § 170.315(b)(2)(iv), (v), (vi), and (vii).

Our proposed revised CIRI requirements in § 170.315(b)(2)(iv), (v), and (vi) include reorganizing and generalizing the CIRI workflow requirements currently in the certification criterion in § 170.315(b)(2)(i), (ii), and (iii). Specifically, we have generalized and combined requirements currently in § 170.315(b)(2)(i) and (ii) in proposed § 170.315(b)(iv) and we have replicated requirements currently in § 170.315(b)(2)(iii) in proposed § 170.315(b)(v) under ''user reconciliation,'' with the aforementioned proposal to reference all data classes and data elements in the USCDI standard in § 170.213 instead of the currently referenced ''medications,'' ''allergies and intolerance,'' and ''problems'' data elements. Additionally, we propose to move our system verification requirements currently finalized in § 170.315(b)(2)(iv) into § 170.315(b)(2)(vii) and we propose, for clarity, to break these system verification requirements up into sub-paragraphs under § 170.315(b)(2)(vii).

Given the goal of USCDI to support ''data elements for nationwide, interoperable health information exchange,'' [37] we believe this proposal supports interoperability and continues to advance our policy objectives for widespread electronic health information exchange. Additionally, we believe that these requirements would help equip providers with additional, relevant, and sometimes critical clinical information that can improve overall patient care. We envision that the ability to reconcile and incorporate both structured and unstructured data elements of the USCDI would be a welcomed functionality to improve patient care, note bloat,[38] and clinician burden.

We note that there can be multiple approaches for supporting user reconciliation and we have stated previously, ''in the event that data is in unstructured form, any method implemented by which the EHR is capable of assisting in reconciliation is acceptable'' (77 FR 54224). We believe that developers have technology readily available for assisting users in reconciling and incorporating data and we maintain that this approach would continue support for innovation.

Alternative Proposal to Revised CIRI Criterion in § 170.315(b)(2)

As an alternative proposal, narrower in scope and on which we seek public comment, we are also considering whether to limit the expansion of our incorporation and reconciliation requirements, that must be met on and after January 1, 2028, to just nine specific USCDI data classes (six new data classes plus the existing three Allergies and intolerance, Medications, and Problems data classes).

The limited data classes in USCDI v4 we have identified for this alternative proposal are: Allergies and Intolerances, Care Team Members, Goals and Preferences, Immunizations, Laboratory, Medications, Medical Devices, Patient Summary and Plan, and Problems. Across these nine data classes, the USCDI v4 includes the following:

- The data elements in the Allergies and Intolerances data class include Substance (Medication), Substance (Drug Class), Substance (Non-Medication) and Reaction.
- The data elements in the Care Team Member(s) data class include Care Team Member Name, Care Team Member Identifier, Care Team Member Role, Care Team Member Location, and Care Team Member Telecom.
- The data elements in the Goals and Preferences data class include Patient Goals, SDOH Goals, Treatment Intervention Preference, and Care Experience Preference.
- The one data element in the Immunizations data class is Immunizations.
- The data elements in the Laboratory data class include Tests, Values/Results, Specimen Type, Result Status, Result Unit of Measure, Result Reference Range, Result Interpretation, Specimen Source Site, Specimen Identifier, and Specimen Condition Acceptability.
- The data elements in Medications include Medications, Dose, Dose Unit of Measure, Indication, Fill Status, Medications Instructions, and Medication Adherence.
- The data element in the Medical Devices data class is Unique Device Identifier—Implantable.
- The data element in the Patient Summary and Plan data class is Assessment and Plan of Treatment.
- The data elements in Problems include Problems, SDOH Problems/Health Concerns, Date of Diagnosis, and Date of Resolution.

We selected these data classes based on feedback from industry and existing industry support as well as our understanding of importance for improved patient care. We believe that the standards referenced for these data elements are mature enough or the information they relay are important enough to patient care to warrant inclusion as part of the CIRI workflow as part of this alternative proposal for a more moderate expansion.

We welcome comment on expanding our CIRI certification requirements to only a limited set of a USCDI data classes versus referencing all USCDI. Additionally, if a limited set of different data elements within the USCDI is preferred, we welcome comments on what subset of USCDI data classes and elements should be referenced in the certification criterion as most necessary for reconciliation and better patient care.

Automatic Reconciliation and Incorporation Capabilities in Revised CIRI Criterion in § 170.315(b)(2)

In addition to our proposed updated CIRI requirements that support all USCDI, we also propose in § 170.315(b)(2)(vi) new functional requirements to enable user-driven automatic reconciliation and incorporation for Health IT Modules certified to § 170.315(b)(2). We believe that users and health care providers are best situated to determine which clinical data and data sources require manual review and which are better suited to automatic reconciliation and incorporation. To ensure that Health IT Modules certified to § 170.315(b)(2) have the capability to support user-driven automatic reconciliation and incorporation, we propose in § 170.315(b)(2)(vi), that Health IT Modules certified to § 170.315(b)(2) would need to provide functionality that would allow automatic reconciliation and incorporation, without manual review, for each of the

[37] *https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.*

[38] Rule A, Bedrick S, Chiang MF, Hribar MR. Length and Redundancy of Outpatient Progress Notes Across a Decade at an Academic Medical Center. *JAMA Netw Open.* 2021;4(7): e2115334. doi:10.1001/jamanetworkopen.2021.15334.

applicable USCDI data elements. We note that nothing in this proposal would compel automatic reconciliation and incorporation for specific workflows or use cases. Rather, our intention is to empower users in determining the circumstances under which clinical data can be automatically reconciled and incorporated, we also propose new configuration requirements in § 170.315(b)(2)(vi) to enable users to set rules indicating specific data and/or specific data sources for automatic reconciliation and incorporation.

We note that automatic incorporation means any process by which USCDI data elements contained within C–CDAs are automatically reconciled with information within certified health IT and incorporated in the health IT without an action by a clinician end user or their delegate. These processes include (1) reconciling new information from the C–CDA into the Health IT Module, for instance, by comparison of medication information in the Health IT Module and information in the C–CDA; or (2) determining that no new information needs to be incorporated into the Health IT Module. We welcome comment on this proposal.

We believe that these revisions would provide users with the ability to configure their workflows in such a way as to maximize patient care while minimizing provider effort to perform reconciliation and incorporation. As we have stated in a previous rule when expanding CIRI requirements, ''we believe that EHR technology can be designed to assist users in remarkable ways and that reconciling information from multiple sources in a way that is assistive to a user is something at which EHR technology should excel'' (77 FR 13849). We believe this proposal is aligned with similar functionalities that many developers are already developing. Our goal is to advance baseline functionality while also leaving room for innovation. We propose that Health IT Modules must support the proposed automatic reconciliation and incorporation capabilities on and after January 1, 2028. We welcome comment on this proposed functionality.

8. Revised Electronic Prescribing Certification Criterion

We propose to update the ''electronic prescribing'' certification criterion in § 170.315(b)(3). The proposed updates include updating the core standard for electronic prescribing to NCPDP SCRIPT standard version 2023011,[39] which is cross-referenced in § 170.205(b)(2) in the proposed text in § 170.315(b)(3)(ii)(A). We also propose revisions to the transactions within the SCRIPT standard that would be required for the updated certification criterion and propose to remove a number of transactions that are currently identified as optional for the criterion. Finally, we propose to remove § 170.315(b)(3)(i) from the CFR upon the effective date of this rule and reserve it as this version of the certification criterion is no longer valid for use in the Program.

a. Electronic Prescribing Standard

In the ''Medicare Program; Medicare Prescription Drug Benefit Program; Health Information Technology Standards and Implementation Specifications'' final rule (Part D and Health IT Standards Final Rule), which appeared in the **Federal Register** on June 17, 2024 (89 FR 51238 through 51265), we adopted NCPDP SCRIPT standard version 2023011 in § 170.205(b)(2). We also finalized an expiration date for NCPDP SCRIPT standard version 2017071 of January 1, 2028, in § 170.205(b)(1), which reflected a delay of one year from the expiration date we had proposed (88 FR 78501). We also finalized the removal of the NCPDP SCRIPT standard version 10.6, which was located in § 170.205(b)(2) (89 FR 51258 and 51259). The finalization of these policies in the Part D and Health IT Standards Final Rule, and CMS' finalization of cross references to § 170.205(b) in their requirements for the Part D Program, reflects a unified approach to aligning standards adoption across HHS programs that impact a common set of participants (88 FR 78486 through 78494).

We note that we previously proposed to adopt NCPDP SCRIPT standard version 2022011 and made other proposals in the ''Medicare Program; Contract Year 2024 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, Medicare Parts A, B, C, and D Overpayment Provisions of the Affordable Care Act and Programs of All-Inclusive Care for the Elderly; Health Information Technology Standards and Implementation Specifications'' proposed rule (2024 Part C/D Proposed Rule), which appeared in the **Federal Register** on December 27, 2022 (87 FR 79555). However, we subsequently withdrew these proposals in the ''Medicare Program; Contract Year 2025 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly; Health Information Technology Standards and Implementation Specifications'' proposed rule (2025 Part C/D Proposed Rule), which appeared in the **Federal Register** on November 15, 2023 (88 FR 78476), and instead proposed to adopt the NCPDP SCRIPT standard version 2023011 in § 170.205(b)(2) (88 FR 78501 through 78502).

In this proposed rule, we propose in § 170.315(b)(3)(ii)(A) that for the time period up to and including December 31, 2027, a Health IT Module certified to the ''electronic prescribing'' certification criterion at 45 CFR 170.315(b)(3) must enable a user to perform the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(1) (NCPDP SCRIPT standard version 2017071) or § 170.205(b)(2) (NCPDP SCRIPT standard version 2023011). We also propose that on and after January 1, 2028, a Health IT Module certified to the ''electronic prescribing'' certification criterion must enable a user to perform the following prescription-related electronic transactions in accordance with only the standard specified in § 170.205(b)(2) (NCPDP SCRIPT standard version 2023011). This means that a health IT developer may continue to maintain health IT certification conformance to NCPDP SCRIPT standard version 2017071 (in § 170.205(b)(1)) for the time period up to and including December 31, 2027. On and after January 1, 2028, consistent with our policy in § 170.402(b), developers of certified health IT with Health IT Modules certified to the ''electronic prescribing'' certification criterion will need update those Health IT Modules to the standard in § 170.205(b)(2) and provide them to customers. This is consistent with the date of January 1, 2028, that we finalized for the expiration of NCPDP SCRIPT standard version 2017071 in § 170.205(b)(1) in the Part D and Health IT Standards Final Rule (89 FR 51259). We also propose in § 170.315(b)(3)(ii)(A) that the Health IT Module must use RxNorm (which we have adopted in § 170.207(d)(1)), and, if using NCPDP SCRIPT standard version 2023011, National Drug Codes (which we cross reference in § 170.207(d)(2)).

b. Proposed Transactions

We propose the following updates and changes to the transactions identified for the ''electronic prescribing'' certification criterion in § 170.315(b)(3)(ii).

[39] *See https://standards.ncpdp.org/Access-to-Standards.aspx.*

New Prescriptions (NewRx) (§ 170.315(b)(3)(ii)(A)(1))

We propose in § 170.315(b)(3)(ii)(A)(*1*) to revise the name used for the NewRx transaction in our regulations from ''Create New Prescriptions (NewRx)'' to ''New Prescriptions (NewRx).'' We propose this change to align with updated terminology used by NCPDP within the SCRIPT standard.

Request and Receive Medication History (§ 170.315(b)(3)(ii)(A)(6))

We propose to remove the request and receive medication history transactions (RxHistoryRequest, RxHistoryResponse) as a requirement for the ''electronic prescribing'' certification criterion in § 170.315(b)(3)(ii)(A)*(6)* and reserve this section.

In the ONC Cures Act Final Rule, ONC finalized the request and receive medication history transactions (RxHistoryRequest, RxHistoryResponse) in the ''electronic prescribing'' certification criterion (85 FR 25682). Since the final rule was published, health IT developers and health care providers have described several challenges meeting this requirement, including development burden; lower than expected adoption and use; and duplicative, overlapping, and sometimes contradictory data from multiple sources. Due in part to these challenges and market forces that have prevented some developers from adopting this functionality natively, developers have had to rely on third-party applications to achieve certification, and in some cases, are unable to achieve certification for electronic prescribing altogether. As such, we propose these transactions would no longer be required for certification to the ''electronic prescribing'' criterion in § 170.315(b)(3)(ii)(A)*(6).* We also propose to reserve section § 170.315(b)(3)(ii)(A)*(6).*

We continue to encourage developers to support these transactions where possible and to follow industry efforts to advance the exchange of patient medication histories through various means such as health information exchanges, health information networks, and prescription drug monitoring programs. We further note that, while health IT developers would not be required to demonstrate compliance with these transactions in order for a Health IT Module to be certified to the updated version of the ''electronic prescribing'' criterion (if our proposals are finalized), CMS still requires use of these transactions when appropriate for electronic exchange of prescription-related information by Part D sponsors and prescribers and dispensers of Part D drugs for Part D eligible individuals (88 FR 78486). Health IT developers would still need to support these transactions when supporting customers who utilize these transactions to exchange electronic Part D medication history information among Part D sponsors and prescribers and dispensers of Part D drugs for Part D eligible individuals in compliance with requirements, currently codified at 42 CFR 423.160(b)(4) and finalized to be codified at 42 CFR 423.160(b)(1)(i)(U) in the Part D and Health IT Standards Final Rule (89 FR 51247).

We request comments on this proposal.

Electronic Prior Authorization Transactions (§ 170.315(b)(3)(ii)(A)(10))

We propose to require the following transactions for electronic prior authorization for the ''electronic prescribing'' certification criterion, at the time a health IT developer presents a Health IT Module for certification using the standard in § 170.205(b)(2) (NCPDP SCRIPT standard version 2023011): PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse.

In the ONC Cures Act Final Rule, ONC adopted these transactions in § 170.315(b)(3)(ii)(B)(*9*) as optional for the ''electronic prescribing'' certification criterion (85 FR 25678). We stated that we adopted these transactions to support alignment with the ''Medicare Program; Secure Electronic Prior Authorization for Medicare Part D'' proposed rule (84 FR 28450), in which CMS proposed to require Part D sponsors to support NCPDP SCRIPT standard version 2017071 for four electronic prior authorization transactions, and proposed that prescribers would be required to use that standard when performing electronic prior authorization transactions for Part D covered drugs they wish to prescribe to Part D eligible individuals (85 FR 25685). CMS subsequently finalized in the ''Medicare Program; Secure Electronic Prior Authorization for Medicare Part D'' final rule in § 423.160(b)(8)(ii) that beginning January 1, 2022, Part D sponsors and prescribers must use the NCPDP SCRIPT standard version 201701 (85 FR 86832). The ONC Cures Act Final Rule allowed health IT developers seeking certification to support these transactions through optional testing but did not require developers to certify to these transactions.

We have received feedback from the public in support of requiring these transactions, most recently in response to the ''Request for Information: Electronic Prior Authorization Standards, Implementation Specifications, and Certification Criteria'' (Electronic Prior Authorization RFI), which was published in the **Federal Register** on January 24, 2022 (87 FR 3475). Commenters stated that requiring these transactions for the certification criterion would help to advance interoperability and reduce administrative burden around prior authorization processes for medications. We agree with this input and believe that it is appropriate to require these transactions at this time. Therefore, we propose to remove PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse in § 170.315(b)(3)(ii)(B)(*9*) as optional and propose to require these transactions in § 170.315(b)(3)(ii)(A)(*10*) for the ''electronic prescribing'' certification criterion at the time a health IT developer presents a Health IT Module for certification using NCPDP SCRIPT standard version 2023011.

ONC also charged the HITAC to establish a Task Force in order to provide input and recommendations in response to the Electronic Prior Authorization RFI; the Task Force's recommendations were approved and submitted to ONC on March 10, 2022.[40] If finalized, the proposals in this rule would implement the Task Force's recommendation to update these prior authorization transactions from ''optional'' in the current version of the ''electronic prescribing'' certification criterion to ''mandatory,'' to better support electronic prior authorization processes for drugs covered under a prescription benefit.

We also propose to adopt the PANotification transaction in § 170.315(b)(3)(ii)(A)(*10*) as a required transaction for the ''electronic prescribing'' certification criterion to further support the exchange of electronic prior authorization information. PANotification is a new transaction introduced since NCPDP SCRIPT standard version 2017071. The PANotification transaction is used to alert the pharmacist or prescriber when a prior authorization has been requested or when a prior authorization

[40] *https://www.healthit.gov/sites/default/files/page/2022-03/2022-03-10_ePA_RFI_Recommendations_Report_Signed_508.pdf.*

determination has been received. The PANotification transaction is intended to improve electronic communication between prescribers and pharmacists, and to reduce duplicate submissions of prior authorization requests to payers. Notification may occur via a NewRx, RxChange or RxRenewal transaction, or as a standalone PANotification. We believe that requiring the PANotification transaction is an important complement to the other proposals related to electronic prior authorization described above.

We request comments on these proposals.

Optional Transactions (NewRxRequest, NewRxResponseDenied, RxFillIndicatorChange, GetMessage, Resupply, DrugAdministration, RxTransferRequest, RxTransferResponse, RxTransferConfirm, Recertification, REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse) (§ 170.315(b)(3)(ii)(B)(1)–(8))

We propose to remove the transactions in § 170.315(b)(3)(ii)(B)(*1*)–(*8*) which are currently identified as ''optional'' for the ''electronic prescribing'' certification criterion. We propose to revise § 170.315(b)(3)(ii)(B) to include requirements related to the exchange of race and ethnicity information in § 170.315(b)(3)(ii)(B)(1)–(4), which is discussed in greater detail below.

Specifically, we propose to remove the following transactions in § 170.315(b)(3)(ii)(B) upon the effective date of the final rule:

- NewRxRequest, NewRxResponseDenied (§ 170.315(b)(3)(ii)(B)(*1*))
- RxFillIndicatorChange (§ 170.315(b)(3)(ii)(B)(*2*))
- GetMessage (§ 170.315(b)(3)(ii)(B)(*3*))
- Resupply (§ 170.315(b)(3)(ii)(B)(*4*))
- DrugAdministration (§ 170.315(b)(3)(ii)(B)(*5*))
- RxTransferRequest, RxTransferResponse, RxTransferConfirm (§ 170.315(b)(3)(ii)(B)(*6*))
- Recertification (§ 170.315(b)(3)(ii)(B)(*7*))
- REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse (§ 170.315(b)(3)(ii)(B)(*8*))

For completeness, we note that § 170.315(b)(3)(ii)(B) currently has transactions listed in § 170.315(b)(3)(ii)(B)(*9)* related to electronic prior authorization. However, we proposed in the section above to remove § 170.315(b)(3)(ii)(B)(*9)* and add the electronic prior authorization transactions currently in § 170.315(b)(3)(ii)(B)(*9)* as required transactions in § 170.315(b)(3)(ii)(A)(*10*).

In reviewing data from the Program, we have found that very few developers have elected to certify to the optional transactions in § 170.315(b)(3)(ii)(B)(*1*)–(*9*). We believe that the low rate of certification to these certification criteria indicates that health IT developers do not see a benefit in obtaining optional certification to these criteria. Accordingly, we believe that removing these optional transactions from the program will reduce the complexity and cost of the Program with minimal impact on health IT developers.

We further note that CMS requires use of these transactions when appropriate for electronic exchange of prescriptions and prescription-related information by Part D sponsors and prescribers and dispensers of Part D drugs for Part D eligible individuals. Accordingly, regardless of whether a health IT developer seeks to certify its Health IT Module(s) to these optional transactions, developers will still need to support them when supporting customers who utilize these transactions to exchange information electronically between prescribers and dispensers of Part D drugs for Part D eligible individuals in compliance with requirements currently codified at 42 CFR 423.160(b)(2)(iv) and finalized to be codified at 42 CFR 423.160(b)(1)(i) in the Part D and Health IT Standards Final Rule (89 FR 51245 through 51247).

We request comment on our proposal to remove the optional transactions in § 170.315(b)(3)(ii)(B)(*1*)–(*8*) from the ''electronic prescribing'' certification criterion. Alternatively, we considered proposing to require the optional transactions in § 170.315(b)(3)(ii)(B)(*1*)–(*8*) rather than removing them from the criterion. However, we did not identify additional reasons to propose to require any of these optional transactions. We request comment on this alternative, including whether commenters believe requiring any of the optional transactions in § 170.315(b)(3)(ii)(B)(*1*)–(*8*) proposed for removal from the ''electronic prescribing'' certification criterion would be important to supporting interoperability between certified Health IT Modules and entities subject to Part D electronic prescribing requirements at 42 CFR 423.160.

We refer readers to Table 1A for a comparison of transactions identified in the existing NCPDP SCRIPT standard version 2017071 and the proposed certification criterion based on NCPDP SCRIPT standard version 2023011.

c. Additional Proposals

Signatura (Sig) (§ 170.315(b)(3)(ii)(D))

In § 170.315(b)(3)(ii)(D), we propose that a Health IT Module certified to the ''electronic prescribing'' criterion must enable a user to enter, receive, and transmit structured and codified prescribing instructions in accordance with the standard specified in § 170.205(b)(2) (NCPDP SCRIPT standard version 2023011), at the time a health IT developer presents a Health IT Module for certification using the NCPDP SCRIPT standard version 2023011.

The Signatura or Sig is the information provided with a prescription to communicate how a prescriber intends for a patient to take a medication. These directions for use are essential for accurate prescription labeling, appropriate patient counseling and education from a pharmacist, and optimal medication use. The NCPDP Structured and Codified Sig Format Implementation Guide,[41] which is embedded in the NCPDP SCRIPT standard, is intended to standardize the portion of an electronic prescription containing the directions for use using existing, accepted electronic transmission standards, such as NCPDP SCRIPT. A ''structured and codified'' Sig conveys instructions in a consistent manner by mapping these directions to a defined set of elements representing the different components of these directions (for instance, dosing schedules and administration instructions). The Structured and Codified Sig Format includes 15 segments, each containing distinct fields to capture potential elements of patient instructions. This is intended to facilitate communication between prescribers and pharmacists, to improve the efficiency of prescribing and dispensing activities, and to help reduce the opportunity for errors. The NCPDP Structured and Codified Sig Format Implementation Guide contains the technical specifications and guidance for implementation of a structured and codified Sig.

When conducting electronic prescribing, prescribers frequently transmit the Sig Text segment as unstructured free text, which introduces inconsistency and limits reusability of the directions contained in the Sig, with potential impacts on patient safety and

[41] *See https://standards.ncpdp.org/Access-to-Standards.aspx.*

clinical outcomes.[42] Moreover, when unstructured free text is used, prescribers and pharmacists may have to engage in back-and-forth communication to clarify what is intended in the Sig instructions, increasing burden. Research has shown more than half of all Sig directions sent in an ambulatory setting can be accurately represented by only 25 standardized concepts (*e.g.* the directions ''take 1 tablet by oral route every day'' and ''Take one (1) tablet by mouth once a day'' can both be represented as the same Sig concept ''Take 1 tablet by mouth once daily''), indicating significant opportunities to reduce variation by expressing these directions through the structured and codified Sig format.[43]

Previously, in the 2015 Edition Final Rule, we did not finalize our proposal to require a Health IT Module certified to the ''electronic prescribing'' criterion to enable a user to enter, receive, and transmit codified Sig instructions in a structured format, based on commenters' concerns regarding the readiness of the standard and other issues such as limitations on the length of a Sig within the version of the NCPDP SCRIPT Structured and Codified Sig Format v1.2 available at the time of the proposal (80 FR 62643). We stated that we would reconsider this stance for future rulemaking based on newer versions of the NCPDP SCRIPT Standard Implementation Guide that may provide implementation improvements and finalized an optional certification provision that technology must be able to receive and transmit the reason for the prescription using the indication elements in the SIG segment in § 170.315(b)(3)(i) (80 FR 62643). In the ONC Cures Act Final Rule, we also finalized this optional provision in § 170.315(b)(3)(ii)(D) (85 FR 25686).

Since the 2015 Edition Final Rule, NCPDP has further advanced the structured and codified Sig format. The most recent version available is the NCPDP Structured and Codified Sig Implementation Guide version 2.2. The structured and codified Sig segment within the NCPDP SCRIPT standard has also been modified; changes to the Sig element from NCPDP SCRIPT standard version 2017017 are discussed in the NCPDP SCRIPT standard version 2023011 Implementation Guide.[44] As a result of additional improvements made to the structured and codified Sig format, as well as the additional time that industry has had to grow familiar with this functionality, we believe that it is appropriate to propose in § 170.315(b)(3)(ii)(D) to require that a Health IT Module certified to the ''electronic prescribing'' criterion must enable a user to enter, receive, and transmit structured and codified prescribing instructions in accordance with the standard specified in § 170.205(b)(2) (where we have adopted NCPDP SCRIPT standard version 2023011), at the time a health IT developer presents a Health IT Module for certification using NCPDP SCRIPT standard version 2023011. We propose to remove the optional provision that is currently in § 170.315(b)(3)(ii)(D).

We request comments on this proposal.

RxNorm and National Drug Codes (NDC)

In § 170.315(b)(3)(ii)(A) we require that a Health IT Module certified to the ''electronic prescribing'' criterion enable a user to perform specified prescription-related electronic transactions in accordance with a specified minimum version of the RxNorm code set for coding medications, among other standards. RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine (RxNorm), is a drug terminology providing a set of normalized medication names and codes based on a collection of commonly used public and commercial vocabularies of drug names and their ingredients. In section III.B.5. of this proposed rule, we propose to adopt an updated release of RxNorm, specifically, the December 4, 2023, Full Monthly Release, in § 170.207(d)(1)(ii). In section III.B.5. of this proposed rule, we also propose to reorganize section § 170.207(d) to include the versions of RxNorm adopted in § 170.207(d)(1), (2), and (3), under § 170.207(d)(1).

For the ''electronic prescribing'' certification criterion, we propose in § 170.315(b)(3)(ii)(A) to remove the existing reference to RxNorm, September 8, 2015 Release in § 170.207(d)(3), and require use of at least one of the versions of the standard adopted in § 170.207(d)(1). If finalized, this reference to § 170.207(d)(1), where we have adopted multiple versions of RxNorm, would permit a health IT developer to use any version of RxNorm that is listed in § 170.207(d)(1) and for which adoption has not expired. This proposal would result in a requirement to use progressively more recent releases of the RxNorm code set as the baseline version of RxNorm which Health IT Modules must use for the ''electronic prescribing'' certification criterion.

We also note that under NCPDP SCRIPT standard version 2020011 and greater, including NCPDP SCRIPT standard version 2023011, the National Drug Codes (NDC) element is required on all non-compounded medication electronic prescriptions.[45] National Drug Codes (NDC) provide a unique identifier for products such as vaccines or medications. Each product is assigned a unique 10- or 11-digit, 3-segment number that identifies the labeler, product, and trade package size. We adopted NDC in § 170.207(d)(4) in the HTI–1 Final Rule (89 FR 1226) via a cross-reference to 45 CFR 162.1002(b)(2) as referenced in 45 CFR 162.1002(c)(1). In section III.B.5 of this proposed rule, we propose to relocate this cross-reference from § 170.207(d)(4) to § 170.207(d)(2) as part of our reorganization of this section. Consistent with the requirement in the NCPDP SCRIPT standard version 2023011 to include NDC with prescriptions, we propose in § 170.315(b)(3)(ii)(A) that a Health IT Module certified to the criterion must enable a user to perform specified prescription-related electronic transactions in accordance with NDC in § 170.207(d)(2). We propose that use of NDC would be required at the time a health IT developer presents a Health IT Module for certification using the NCPDP SCRIPT standard version 2023011 adopted in § 170.205(b)(2).

Diagnoses (§ 170.315(b)(3)(ii)(C))

In § 170.315(b)(3)(ii)(C) we require that a Health IT Module ''must be able to receive and transmit the reason for prescription using the diagnosis elements: <DIAGNOSIS> <PRIMARY> or <SECONDARY>'' for the set of prescription-related transactions identified in § 170.315(b)(3)(ii)(C)(1)–(2).

We propose to make changes to the list of required and optional transactions in § 170.315(b)(3)(ii)(C) to reflect the proposed required transactions for the updated version of

[42] Schiff, G., Mirica, M.M., Dhavle, A.A., Galanter, W.L., Lambert, B., & Wright, A. (2018). A prescription for enhancing electronic prescribing safety. Health Affairs (Project Hope), 37(11), 1877–1883. doi:*https://doi.org/10.1377/hlthaff.2018.0725.*

[43] Yang, Y., Ward-Charlerie, S., Dhavle, A.A., Rupp, M.T., & Green, J. (2018). Quality and Variability of Patient Directions in Electronic Prescriptions in the Ambulatory Care Setting. Journal of managed care & specialty pharmacy, 24(7), 691–699. *https://doi.org/10.18553/jmcp.2018.17404.*

[44] *See https://standards.ncpdp.org/Access-to-Standards.aspx.*

[45] For more information about the updates to NDC in the NCPDP SCRIPT standard *see https://ncpdp.org/NCPDP/media/images/Resources%20Items/NDC-Use-eRx-Fact-Sheet.pdf?ext=.pdf.*

the certification criterion in § 170.315(b)(3)(ii)(A), and our proposal to remove certain optional transactions from the updated version of the criterion in § 170.315(b)(3)(ii)(B). Specifically, we propose in 170.315(b)(3)(ii)(C)(*1*) to rename ''Create New Prescriptions (NewRx)'' to ''New Prescriptions (NewRx).'' We propose in § 170.315(b)(3)(ii)(C)(*1*)(*vi*) to remove the transaction ''Receive medication history'' (RxHistoryResponse) and reserve this section. We propose in § 170.315(b)(3)(ii)(C)(*1*)(*vii*) to require the following electronic prior authorization transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse and PACancelRequest, PACancelResponse, PANotification) if using NCPDP SCRIPT standard version 2023011 (adopted in § 170.205(b)(2)). Lastly, we propose to remove the optional transactions in § 170.315(b)(3)(ii)(C)(*2*)(*i*) through (*iv*) and reserve this section. We refer readers to Table 1A below in this rule for a comparison of required and optional transactions identified in the current certification criterion based on NCPDP SCRIPT standard version 2017071 and the proposed updated criterion based on NCPDP SCRIPT standard version 2023011.

Race and Ethnicity

In 2023, the Pharmacy Interoperability and Emerging Therapeutics Task Force provided a recommendation to the HITAC to support interoperability between pharmacy constituents by including race and ethnicity in the ''electronic prescribing'' certification criterion (PhIET–TF–2023_Recommendation 26).[46] The Task Force stated that demographic data is not always made available through reporting such as case reporting to public health agencies. Yet, in order to support the ability to perform analytics, all data feeds should have relevant race and ethnicity data, and other key demographic data, when available. The Task Force recommended that various prescribing and laboratory results reporting capabilities need to be able to support sharing of the relevant data when an alternative source is not consistently available. Additionally, the Task Force acknowledged that a prescriber will likely already have patient race or ethnicity documented. Exchanging this information through available transactions, such as those included in electronic prescribing, is one way to improve consistency in documentation of demographic data across provider types.

Specifically, the Task Force recommended ONC include the ability to capture and exchange race and ethnicity as part of the ''electronic prescribing'' certification criterion and point to USCDI v4,[47] which references the CDC Race & Ethnicity Code System—CDCREC 1.2 (July 2021).[48] The CDC Race & Ethnicity Code System—CDCREC 1.2 code set facilitates use of Federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. The NCPDP SCRIPT standard version 2023011, which we propose to incorporate in the ''electronic prescribing'' certification criterion in this proposed rule, references reporting of race and ethnicity using the CDCREC 1.2 associated value set ''PHVS_Race_CDC'' version 2 (December 2018 [49]) from the code system code ''PH_RaceAndEthnicity_CDC'' as optional for certain transactions within the standard that we have also proposed to require when using the updated version of the standard. This aligns with the code system code in CDCREC 1.2 which is ''PH_RaceAndEthnicity_CDC,'' and is available on the Public Health Information Network (PHIN) Vocabulary Access and Distribution System (PHIN VADS).[50]

Given the importance of the issues described by the Task Force, and the alignment between the recommendation and NCPDP SCRIPT standard version 2023011, we believe that it is appropriate to implement the Task Force recommendation through updates to the ''electronic prescribing'' certification criterion. Therefore, we propose in § 170.315(b)(3)(ii)(B) that a Health IT Module certified to the ''electronic prescribing'' certification criterion must enable a user to exchange race and ethnicity information for a patient when performing the following prescription-related electronic transactions, if using NCPDP SCRIPT standard version 2023011:

- Receive fill status notifications (RxFill).
- Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).
- Request to cancel prescriptions (CancelRx).
- Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

We believe the transactions above are an appropriate starting place to include race and ethnicity in the electronic prescribing certification criterion. We will continue to monitor changes to the SCRIPT standard for additional updates to transactions to include race and ethnicity data fields.

We invite comments on this proposal and request information on whether there are other SCRIPT transactions that include data fields for race and ethnicity we should consider specifying to enable exchange of race and ethnicity data with providers in pharmacy settings.

Base EHR Definition

We note that, given our proposal in section III.B.9.b. to include the proposed ''real-time prescription benefit'' certification criterion in § 170.315(b)(4) in the Base EHR definition in § 170.102, we have also proposed to add the ''electronic prescribing'' certification criterion in § 170.315(b)(3) to the Base EHR definition. Please see section III.B.9.b. of this proposed rule for further details on this proposal.

Multi-Factor Authentication

We propose in § 170.315(b)(3)(ii)(G) that, on and after January 1, 2028, a Health IT Module certified to § 170.315(b)(3) must meet the multi-factor authentication (MFA) requirements specified in § 170.315(d)(13)(ii) for user-facing authentication. We believe this update is in line with industry information security best practice for an important authentication use case in health IT, and that it is necessary to help better protect electronic health information. We refer readers to section III.B.17 for our proposal to revise our MFA certification criterion § 170.315(d)(13) and for background on the user level authentication use case we are targeting with this requirement.

BILLING CODE 4150–45–P

[46] *See https://www.healthit.gov/sites/default/files/page/2023-11/2023-11-09_PhIET_TF_2023_Recommendations_Transmittal_Letter_508.pdf.*

[47] *See https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.*

[48] *See https://www.cdc.gov/phin/resources/vocabulary/.*

[49] *See https://phinvads.cdc.gov/vads/ViewValueSet.action?id=9152A536-AEEC-E711-ACD6-0017A477041A.*

[50] *See https://phinvads.cdc.gov/vads/ViewCodeSystemConcept.action?oid=2.16.840.1.113883.6.238&code=1579-2.*

Table 1A. Comparison of Transactions Identified in Current Certification Criterion based on NCPDP SCRIPT Standard Version 2017071 and Proposed Criterion based on NCPDP SCRIPT Standard Version 2023011

Transactions	Current Electronic Prescribing Criterion (NCPDP SCRIPT Standard Version 2017071)	Proposed Revised Electronic Prescribing Criterion (NCPDP SCRIPT Standard Version 2023011)
New prescriptions (NewRx).	Required	Required
Receive fill status notifications (RxFill).	Required	Required
Request and receive medication history (RxHistoryRequest, RxHistoryResponse).	Required	Not Included
Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).	Required	Required
Request and respond to cancel prescriptions (CancelRx, CancelRxResponse).	Required	Required
Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).	Required	Required
Relay acceptance of a transaction back to the sender (Status).	Required	Required
Respond that there was a problem with the transaction (Error).	Required	Required
Respond that a transaction requesting a return receipt has been received (Verify).	Required	Required
Electronic prior authorization (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse and PACancelRequest, PACancelResponse).	Optional	Required
PANotification	Not Included	Required
New prescription requests (NewRxRequest, NewRxResponseDenied).	Optional	Not Included
RxTransferRequest, RxTransferResponse, RxTransferConfirm, and RxFillIndicatorChange.	Optional	Not Included
Request to send an additional supply of medication (Resupply).	Optional	Not Included
GetMessage.	Optional	Not Included
Communicate drug administration events (DrugAdministration).	Optional	Not Included
Recertify the continued administration of a medication order (Recertification).	Optional	Not Included
Complete Risk Evaluation and Mitigation Strategy (REMS) transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).	Optional	Not Included

BILLING CODE 4150–45–C

9. New Real-Time Prescription Benefit Criterion

a. Background

The increasing costs of prescription drugs have long been a concern for patients, providers, and policymakers.[51] Increased drug costs can have several negative consequences for patients, including limited access to healthcare,[52] lower healthcare use,[53] medication nonadherence [54] [55] and financial stress, especially among underserved,[56] uninsured and underinsured [57] populations. Merely having health insurance coverage does not necessarily confer medication affordability on patients.[58] These challenges continue to be the focus of legislation, such as the Inflation Reduction Act of 2022 (Pub. L. 117–169, August 16, 2022), which includes several provisions that are expected to decrease prescription drug costs and improve access to prescription drugs for the more than 65 million Americans enrolled in the Medicare program, including allowing Medicare to directly negotiate prescription drug prices for the first time, eliminating cost sharing for adult vaccines, capping out-of-pocket costs for insulin, and capping Part D enrollee out-of-pocket spending at $2,000 annually starting in 2025 (see sections 11406, 11401, 1194, and 11201). E. O. 14087, Lowering Prescription Drug Costs for Americans, directed further actions to lower the cost of prescription drugs.

Research also suggests provider-patient discussions during clinical encounters about costs and affordability may lead to an overall reduction in out-of-pocket costs.[59] Real-time prescription benefit tools empower providers and their patients to compare the patient-specific cost of a drug to the cost of a suitable alternative, compare prescription costs at different pharmacy locations, view information about out-of-pocket costs, and learn whether a specific drug is subject to utilization management restrictions such as prior authorization, step therapy, or quantity limits. We believe, when appropriate, use of these tools can allow the provider and patient to choose among clinically acceptable alternative medication treatments while weighing coverage and point-in-time costs. Access to this data within the electronic prescribing workflow may also help to reduce provider burden associated with coverage determination and prior authorization appeals. We believe widespread adoption of such tools, along with increased awareness of drug cost information among patients and providers will likely spur more robust evaluations over time.

Section 119 of Title I, Division CC of the Consolidated Appropriations Act of 2021, (Pub. L. 116–260, December 27, 2020) (CAA, 2021), requires sponsors of prescription drug plans to implement one or more real-time benefit tools (RTBTs) after the Secretary has adopted a standard for RTBTs and at a time determined appropriate by the Secretary. The law specified that a qualifying RTBT must meet technical standards named by the Secretary, in consultation with ONC. Section 119(b) also amended the definition of a ''qualified electronic health record'' in section 3000(13) of the Public Health Service Act (PHSA) to specify that a qualified electronic health record ''includes, or is capable of including, a real-time benefit tool that conveys patient-specific real-time cost and coverage information with respect to prescription drugs that, with respect to any health information technology certified for electronic prescribing, the technology shall be capable of incorporating the information described in clauses (i) through (iii) of paragraph (2)(B) of section 1860D–4(o) of the Social Security Act.'' The information specified in (2)(B)(i)–(iii) of section 1860D–4(o) of the Social Security Act, as added by section 119(a) of the CAA, 2021, is:

- A list of any clinically appropriate alternatives to such drug included in the formulary of such plan.
- Cost-sharing information and the negotiated price for such drug and such alternatives at multiple pharmacy options, including the individual's preferred pharmacy and, as applicable, other retail pharmacies and a mail order pharmacy; and
- The formulary status of such drug and such alternatives and any prior authorization or other utilization management requirements applicable to such drug and such alternatives included in the formulary of such plan.

The provision further specifies that the change to the definition of a ''qualified electronic health record'' shall be implemented ''at a time specified by the Secretary but not before the Secretary adopts a standard for such tools.''

In the HTI–1 Proposed Rule (88 FR 23848 through 23855), we included a request for information (RFI) about issues related to establishing a real-time prescription benefit certification criterion utilizing the NCPDP Real-Time Prescription Benefit (RTPB) standard, and ways in which the Program could ensure real-time prescription benefit capabilities are implemented effectively for providers. We received many comments on this RFI and appreciate the input provided by commenters.

In order to implement section 119(b) of the CAA, 2021, we propose to establish a ''real-time prescription benefit'' health IT certification criterion in § 170.315(b)(4) and to include this certification criterion in the Base EHR definition in § 170.102(3)(iv).

b. Revision to the Base EHR Definition and Health IT Module Dependent Criteria Requirements

As noted above, section 119(b) of the CAA, 2021, amended the definition of a ''qualified electronic health record'' (Qualified EHR) in section 3000(13) of the PHSA to specify that a qualified electronic health record ''includes, or is capable of including, a real-time benefit tool that conveys patient-specific real-time cost and coverage information with respect to prescription drugs.'' In the 2014 Edition Final Rule, we established the term ''Base EHR,'' based on the Qualified EHR definition in PHSA

[51] A.S. Kesselheim, J. Avorn, A. Sarpatwari, The high cost of prescription drugs in the United States: origins and prospects for reform. JAMA, 316 (8) (2016), pp. 858–871.

[52] Daher, Al Rifai, M., Kherallah, R. Y., Rodriguez, F., Mahtta, D., Michos, E. D., Khan, S. U., Petersen, L. A., & Virani, S. S. (2021). Gender disparities in difficulty accessing healthcare and cost-related medication non-adherence: The CDC behavioral risk factor surveillance system (BRFSS) survey. Preventive Medicine, 153, 106779–106779. *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9291436/.*

[53] Roebuck, Liberman, J. N., Gemmill-Toyama, M., & Brennan, T. A. (2011). Medication adherence leads to lower health care use and costs despite increased drug spending. Health Affairs, 30(1), 91–99. *https://doi-org.ezproxyhhs.nihlibrary.nih.gov/10.1377/hlthaff.2009.1087.*

[54] SG Morgan, A. Lee. Cost-related non-adherence to prescribed medicines among older adults: a cross-sectional analysis of a survey in 11 developed countries. BMJ Open, 7 (1) (2017), Article e014287.

[55] DiMatteo MR, Giordani PJ, Lepper HS, Croghan TW. Patient adherence and medical treatment outcomes: a meta-analysis. Med Care. 2002; 40 (9): 794–811.

[56] Whaley C, Reed M, Hsu J, Fung V (2015) Functional Limitations, Medication Support, and Responses to Drug Costs among Medicare Beneficiaries. PLoS ONE 10(12): e0144236. *https://doi.org/10.1371/journal.pone.0144236.*

[57] Collins SR, Rasmussen PW, Beutel S, Doty MM. The problem of underinsurance and how rising deductibles will make it worse: findings from the Commonwealth Fund Biennial Health Insurance Survey, 2014. New York: Commonwealth Fund; 2015.

[58] Zhao, J., Zheng, Z., Han, X., Davidoff, A. J., Banegas, M. P., Rai, A., Jemal, A., & Yabroff, K. R. (2019). Cancer History, Health Insurance Coverage, and Cost-Related Medication Nonadherence and Medication Cost-Coping Strategies in the United States. Value in health: the journal of the International Society for Pharmacoeconomics and Outcomes Research, 22(7), 762–767. *https://doi.org/10.1016/j.jval.2019.01.015.*

[59] Carroll JK, Farah S, Fortuna RJ, et al. Addressing medication costs during primary care visits: a before-after study of team-based training. Ann Intern Med. 2019;170(suppl 9): S46–S53. doi:10.7326/M18–2011.

section 3000(13), for use within the Program (77 FR 54262). We define Base EHR in § 170.102, and this definition currently includes certification criteria under the Program that align with the elements of the Qualified EHR definition in the PHSA.

Given that the statutory definition of Qualified EHR is implemented in regulation through the Base EHR definition in § 170.102, we believe it is necessary to propose to update the Base EHR definition consistent with Congress' modification of the statutory definition of Qualified EHR to address real-time benefit tool functionality. Specifically, consistent with PHSA section 3000(13), as amended by section 119(b) of the CAA, 2021, we propose to revise the Base EHR definition in § 170.102 to add paragraph (3)(iv) to include the real-time prescription benefit certification criterion proposed in § 170.315(b)(4) on and after January 1, 2028. We believe including the ''real-time prescription benefit'' certification criterion as part of the Base EHR definition will increase the use of real-time prescription benefit tools and promote widespread adoption which will help to lower drug costs for Medicare beneficiaries, consistent with section 119 of the CAA. Use of real-time prescription benefit tools enable Medicare providers and enrollees to make cost-informed decisions about prescriptions, and a standardized approach will ensure that critical drug and drug price data is available to providers when they need it.

We note that in the Part D and Health IT Standards Final Rule CMS finalized to require Part D plan sponsors to adhere to NCPDP RTPB standard version 13 as part of requirements to provide a prescriber real-time benefit tool by January 1, 2027 in the Part D and Health IT Standards Final Rule (89 FR 51259 and 51260). We request comment on whether we should seek to align the date when the ''real-time prescription benefit'' certification criterion in § 170.315(b)(4) would be effective for the Base EHR definition (proposed to be January 1, 2028) with the date finalized in the Part D and Health IT Standards Final Rule for Part D plan sponsors' real-time benefit tools to adhere to the NCPDP RTPB standard version 13 (January 1, 2027) (89 FR 51260).

The amended definition of a Qualified EHR in PHSA section 3000(13)(c) further specifies that ''with respect to any health information technology certified for electronic prescribing, the technology shall be capable of incorporating the information described in clauses (i) through (iii) of paragraph (2)(B).'' We interpret this provision to mean, for the purposes of the Program, that any health IT presented for certification for electronic prescribing capabilities should also be capable of incorporating the real-time benefit information specified in clauses (i) through (iii) of paragraph (2)(B) of section 1860D–4(o) of the Social Security Act, as described above.

Real-time prescription benefit functionality is closely related to electronic prescribing functionality, which provides the basic workflow within which a provider may seek to identify information about a patient's coverage for a certain prescription before transmitting that electronic prescription to the pharmacy. In most cases, we expect health IT developers seeking certification to § 170.315(b)(4) will already be certified to § 170.315(b)(3), though there will be some variation due to the modularity of Program criteria. Accordingly, we propose to revise § 170.550(g) to add paragraph (g)(6) in order to require that any developer that obtains certification for the ''electronic prescribing'' certification criterion in § 170.315(b)(3) must also obtain certification for the proposed ''real-time prescription benefit'' criterion in § 170.315(b)(4).

While we propose to establish this dependency with the ''electronic prescribing'' certification criterion, this certification criterion is not included as part of the current Base EHR definition in § 170.102. Although electronic prescribing is a widely used and fundamental capability of health IT, we have, to date, not included this certification criterion in the Base EHR definition for several reasons. First, the Qualified EHR definition in section 3000(13) of the PHSA does not specify electronic prescribing as a required element of a Qualified EHR and we have generally sought to limit the Base EHR definition in § 170.102, which implements the Qualified EHR definition, to those capabilities that are required for the Qualified EHR definition by statute. Second, many health care providers have historically been required to adopt certified technology for electronic prescribing in order to meet the requirements of the Medicare EHR Incentive Programs, now known as the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of the Merit-Based Incentive Payment System (MIPS).[60] Objectives and measures for eligible professionals, eligible hospitals, and CAHs under these programs have included measures related to electronic prescribing throughout the course of the programs. Section 1848(o)(2)(A)(i) of the Social Security Act also requires that demonstration of use of certified EHR technology in a meaningful manner by an eligible professional ''shall include the use of electronic prescribing.''

However, given our proposal to include the proposed ''real-time prescription benefit'' certification criterion in § 170.315(b)(4) in the Base EHR definition, we believe it is also appropriate to add the ''electronic prescribing'' certification criterion in § 170.315(b)(3) to the Base EHR definition. While we previously did not include this capability in the Base EHR definition for the reasons described above, we believe that the inclusion of closely related ''real-time prescription benefit'' functionality in § 170.315(b)(4) necessitates the inclusion of electronic prescribing functionality. We therefore propose to include the ''electronic prescribing'' certification criterion in § 170.315(b)(3) within the Base EHR definition in § 170.102. We further propose to specify that this criterion would be effective for the Base EHR definition on and after January 1, 2028, which aligns with the date when the proposed ''real-time prescription benefit'' certification criterion in § 170.315(b)(4) would be effective for the Base EHR definition.

We request comment on these proposals, especially regarding the impact of these proposals on health IT developers seeking to ensure their products meet the Base EHR definition that are not currently separately certified to the ''electronic prescribing'' criterion. We seek information on the additional burden to developers of requiring the ''electronic prescribing'' certification criterion as part of the Base EHR definition in addition to the proposed ''real-time prescription benefit'' certification criterion. We also request comment on the implications for interoperability of electronic prescribing if we were to finalize our proposal to include the ''real-time prescription benefit'' certification criterion within the Base EHR definition but not finalize our proposal to include the ''electronic prescribing'' certification criterion in the Base EHR definition.

Lastly, we request comment on the impact this proposed policy would have on any health care providers participating in the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of the Merit-Based Incentive Payment System (MIPS) who have historically been able to claim an exclusion from electronic prescribing

[60] The Medicaid EHR Incentive Program sunset in 2021 (84 FR 42592).

measures in these programs, and, as a result have not adopted certified health IT for electronic prescribing in order to complete the actions associated with these measures. The definitions of certified EHR technology at 42 CFR 495.4 and 42 CFR 414.1305, which define technology requirements for these programs, cross-reference the Base EHR definition at 45 CFR 171.102. Thus, as a result of the statutory change implemented by Congress, and if our proposals to add these certification criteria to the Base EHR definition are finalized, all providers participating in these programs would have to have at a minimum, health IT certified to the proposed ''real-time prescription benefit'' certification criterion and the ''electronic prescribing'' certification criterion. This would include participants that currently successfully participate in these programs without possessing certified health IT that supports these capabilities. We request comment on whether finalizing these proposals would impose significant burden on these health care providers.

c. Real-Time Prescription Benefit Standard

We propose in § 170.315(b)(4)(i) that a Health IT Module certified to the proposed ''real-time prescription benefit'' certification criterion must enable a user to perform certain real-time prescription benefit electronic transactions in accordance with at least one of the versions of the standard adopted in § 170.205(c). Under this paragraph, ONC adopted the NCPDP RTPB standard version 13 [61] on behalf of HHS in § 170.205(c)(1) in the Part D and Health IT Standards Final Rule, which appeared in the **Federal Register** on June 17, 2024 (89 FR 51238 through 51265). If we adopt subsequent versions of the NCPDP RTPB standard in § 170.205(c), our proposal to require the use of at least one of the versions of the standard adopted in § 170.205(c) would enable health IT developers to use any version of the standard adopted under this paragraph, unless we specify an adoption ''expiration'' date which indicates a certain version of the standard may no longer be used after that date.

The NCPDP RTPB standard version 13 enables the exchange of patient eligibility, product coverage, and benefit financials for a chosen product and pharmacy, and identifies coverage restrictions and alternatives when they exist. The benefits of the more recent NCPDP RTPB standard version 13 relative to NCPDP RTPB standard version 12 include improvements to the NCPDP RTPB Patient Segment, Product and Alternative Product Segments, and new elements, new values, and updated values to the schema, as well as administrative corrections that support consistency and clarity.

Because the NCPDP RTPB standard is relatively new and not yet widely implemented, we expect additional enhancements and improvements to the standard over time as more health IT developers adopt and implement the standard and more exchange partners engage in the standards development process with NCPDP. We encourage developers to remain familiar with updates occurring in newer versions of the NCPDP RTPB standard.

d. Sending and Receiving Real-Time Prescription Benefit Information

In order to execute real-time prescription benefit checks in accordance with the NCPDP RTPB standard version 13, a provider originates the request for prescription benefit information for a specific patient from within their health IT. In return, a processor, pharmacy benefit manager, or adjudicator provides the appropriate response. We propose in § 170.315(b)(4)(i) that a Health IT Module certified to the ''real-time prescription benefit'' criterion must enable a user to perform specified transactions in accordance with at least one of the versions of the standard adopted in § 170.205(c) (where we have adopted the NCPDP RTPB standard version 13), as well as one of the versions of the standard in § 170.207(d)(1) (where we have adopted RxNorm) and the standard in § 170.207(d)(2) (where we have cross-referenced National Drug Codes (NDC)).

We propose in § 170.315(b)(4)(i)(A) that a Health IT Module certified to the proposed criterion must enable a user to request patient-specific prescription benefit information, estimated cost information, and therapeutic alternatives, in accordance with the RTPBRequest transaction. We propose in § 170.315(b)(4)(i)(B) that a Health IT Module certified to the proposed criterion must enable a user to receive patient-specific prescription benefit information, estimated cost information, and therapeutic alternatives in response to a request, in accordance with the RTPBResponse transaction. RTPBRequest and RTPBResponse transactions are determined by patient, benefit, and product-specific information. Each request and response are unique with information conditioned on factors associated with each transaction. Health IT Modules certified to the proposed certification criterion should support transaction segments and associated data elements necessary to reflect both the information needed for a successful RTPBRequest and the information contained in a detailed RTPBResponse. As such, a Health IT Module must have the capability to send and receive both mandatory and situational transaction segments and associated data elements for RTPBRequests and RTPBResponse transactions as specified in NCPDP RTPB standard version 13. Finally, we propose in § 170.315(b)(4)(i)(C) that a Health IT Module certified to the proposed criterion must enable a user to be notified of errors when there is a problem with a real-time prescription benefit transaction, in accordance with the RTPBError transaction.

We request comments on these proposals and whether we should consider other capabilities for the certification criterion in the future.

Use of XML Format

We propose in § 170.315(b)(4)(i) that a Health IT module certified to the criterion must enable a user to perform the specified transactions using the XML format. While the NCPDP RTPB standard version 13 supports both EDI and XML formats, in response to the RFI included in the HTI–1 Proposed Rule (88 FR 23746), we received many comments in support of testing the XML format of the RTPB standard alone or with the EDI format as optional. Additionally, commenters recommended that ONC should test the format each individual health IT developer has chosen for its own system to be tested in. Some commentors also shared a desire to move away from XML and EDI altogether, preferring the JSON format instead, noting industry plans for the future retirement of XML and EDI. One commenter suggested certification in either format, with requirements that health IT be capable of demonstrating translation capabilities between EDI and XML.

After considering these comments, we believe that proposing to only require use of the XML format will simplify testing for health IT developers. ONC will continue to monitor syntax and format updates and development for real-time benefit transactions and associated standards.

e. Additional Topics

Display

We propose in § 170.315(b)(4)(ii) that a Health IT Module certified to the criterion must display to a user in

[61] *See https://standards.ncpdp.org/Access-to-Standards.aspx.*

human readable format patient-specific prescription benefit information, estimated cost information, and therapeutic alternatives in accordance with at least one of the versions of the standard in § 170.205(c) (where we have adopted NCPDP RTPB standard version 13). The ability to display RTPB data provides access to this information and is essential for a user to be able to use the information to inform shared decision-making as the provider and patient determine the treatment that will be best for them.

Scope

The NCPDP RTPB standard version 13 supports real-time prescription benefit requests and responses for a variety of items manufactured for sale such as medications, vaccines, and medical devices or supplies.[62] While the majority of products covered by an individual's pharmacy benefit will be medications, Part D drugs, as defined at 42 CFR 423.100, can include prescription medications, vaccines, and supplies associated with the injection of insulin (*e.g.,* syringes, alcohol pads, gauze), and are represented by RXCUIs [63] on the formulary file.

In the HTI–1 Proposed Rule we requested comment on the appropriate scope for a ''real-time prescription benefit'' certification criterion, including whether a ''real-time prescription benefit'' certification criterion should require support for products that are not defined as medications but may also be included in a RTPB transaction, namely vaccines and medical devices or supplies (87 FR 23853). We received several comments in response to our request for information on this topic, with several commenters encouraging an initial focus on medications for the certification criterion.

In addition to medications, we believe it is important to require Health IT Modules certified to the ''real-time prescription benefit'' criterion to be able to support vaccines, and note that under Part D regulations and guidance, plans include most commercially available vaccines on their formularies.[64]

However, we are not proposing to include devices and supplies in the proposed certification criterion at this time. We note that the NCPDP RTPB standard version 13 does yet not support the FDA Unique Device Identification System unique device identifiers (UDIs), which are identified as the standard for the Unique Device Identifier—Implantable data element in the Medical Devices data class in the USCDI.[65] Additionally, devices covered under a pharmacy benefit may be defined as a drug under Section 201(g) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321(h)) rather than a device under Section 201(h) and therefore are not assigned a Unique Device Identifier for Implantable Devices. ONC will continue to monitor advancements to the NCPDP RTPB standard to support unique identifiers for devices, any related developments at the FDA, and updates to the standardization and exchange of device and supplies data.

In summary, we propose in § 170.315(b)(4)(iii) that scope of the criterion is limited to medications and vaccines covered by a pharmacy benefit. We invite comments on this proposal.

Formulary and Benefit

In the HTI–1 Proposed Rule, we requested comment on whether we should further explore capabilities for Health IT Modules to support access to formulary and benefits information and provided detail about how access to formulary and benefits information was previously supported within the Program. We noted that in the 2015 Edition Final Rule, ONC included a ''Drug-formulary and preferred drug list checks'' certification criterion in § 170.315(a)(10). However, ONC did not adopt the proposed NCPDP Formulary and Benefit standard version 3.0 to support this criterion due to comments received in response to the 2015 Edition Proposed Rule (80 FR 16821). The drug formulary and preferred drug list checks § 170.315(a)(10) certification criterion was later removed from the Program in the ONC Cures Act Final Rule (85 FR 25660) because this functionality was widely available, and there was not sufficient reason to justify the burden on developers and providers of meeting Program compliance requirements specific to this criterion. We noted that updates, enhancements, and corrections have been made to the NCPDP Formulary and Benefit standard since we considered adopting version 3.0, and many of these updates addressed concerns commenters expressed previously (87 FR 23854).

Subsequently, in the Part D and Health IT Standards Final Rule, we finalized adoption of NCPDP Formulary and Benefit standard version 60 in § 170.205(u) (89 FR 51260), reflecting an aligned approach with the Part D Program to adoption of standards that support electronic prescribing. In the same rulemaking, CMS finalized to cross-reference NCPDP Formulary and Benefit standard version 60 in the requirements for transmitting formulary and benefit information between prescribers Part D sponsors proposed at 42 CFR 423.160(b)(3) (89 FR 51250 and 51251). However, we did not make any updates to the Program to incorporate the proposed Formulary and Benefit standard as part of certification criteria.

In response to our request for comment in the HTI–1 Proposed Rule, some commenters supported incorporation of capabilities to access formulary and benefits information within the Program based on the NCPDP Formulary and Benefit standard. However, many stated that a certification criterion based on the standard is not necessary as this functionality is already widespread in the industry due to existing CMS regulatory requirements. Furthermore, these commenters stated that a criterion based on the NCPDP Formulary and Benefit standard may limit innovation around other approaches to obtaining formulary and benefit information currently being explored by the industry.

We have considered the comments received in response to the RFI and have determined not to propose new functionality related to formulary and benefits information within the Program at this time. We also note that we have proposed to adopt the HL7 FHIR Da Vinci—Payer Data Exchange (PDex) US Drug Formulary Implementation Guide, version 2.0.1—STU 2, in § 170.215(m)(i) in this proposed rule and have referenced this standard as part of the ''patient access API'' certification criterion proposed in § 170.315(g)(30)(iii).

Negotiated Price

Section 1860D–4(o)(2)(B)(ii) of the Social Security Act, as added by section 119(a) of the CAA, 2021, specifically requires real-time benefit tools capable of providing information on ''cost-sharing information and the negotiated price'' for drugs and alternatives. However, we note that we have not proposed to include negotiated price in the proposed § 170.315(b)(4) certification criterion. The NCPDP RTPB

[62] *See https://www.ncpdp.org/Access-to-Standards.aspx.*

[63] An RXCUI is a machine-readable code or identifier that points to the common meaning shared by the various source names grouped and assigned to a particular concept. More information can be found at *https://www.nlm.nih.gov/research/umls/rxnorm/overview.html.*

[64] *See* ''Medicare Prescription Drug Benefit Manual: Chapter 6—Part D Drugs and Formulary Requirements'' 30.2.7 at *https://www.cms.gov/medicare/prescription-drug-coverage/prescriptiondrugcovcontra/downloads/part-d-benefits-manual-chapter-6.pdf.*

[65] *See* USCDI v4: *https://www.healthit.gov/isa/taxonomy/term/821/uscdi-v4.*

standard version 13 does not include fields to support the exchange of negotiated price. We solicited comments regarding negotiated price in response to the RFI, and commenters expressed strong disapproval for the inclusion of negotiated price in RTBTs. Additionally, concerns were shared that plan negotiated prices may be confusing to providers and patients and are not likely to assist or improve the utility or usability of technology certified to a real-time prescription benefit certification criterion. We also note that CMS does not require the exchange of negotiated price by Part D sponsors when implementing an electronic real-time benefit tool. NCPDP RTPB standard version 13, which we have proposed to incorporate into the proposed ''real-time prescription benefit'' certification criterion, is the best available standard for use currently to provide patient specific cost-sharing information. Unfortunately, we have not identified a standard or any consistent approach to deliver reliable negotiated price information in real-time. ONC will continue to work with CMS and other interested parties to determine how negotiated price information may be made available and what technical approaches exist to support transparency in negotiated prices of drugs.

10. Electronic Health Information (EHI) Export—Single Patient EHI Export Exemption

a. Background

In the ONC Cures Act Final Rule (85 FR 25690 through 25700), we finalized a new certification criterion in § 170.315(b)(10) for Electronic Health Information (EHI) Export. The certification criterion's conformance requirements were intended to support two contexts in which we believe 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 finalized in § 170.315(b)(10)(i) that health IT certified to this criterion must support single patient EHI export upon a valid request by a patient or a user on the patient's behalf. Second, we finalized in § 170.315(b)(10)(ii) that the product would support the export of all EHI when a health care provider chooses to transition or migrate information to another health IT system. Furthermore, we established in § 170.402(a)(4), as part of the Assurances Condition of Certification requirement, that any 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).

For the single patient EHI export functionality, we also established in § 170.315(b)(10)(i)(B) that a user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate. Subsequently, ONC has heard from developers that some certified Health IT Modules act primarily as intermediaries between systems and, through integration, function without any direct human interaction. As an example, a Health IT Module may facilitate public health reporting by processing existing EHI into a required format for report submission without any user interactions. In such circumstances, a human user may not interact with the certified Health IT Module itself; and even though the Health IT Module stores EHI or causes EHI to be stored, this EHI may be a differently formatted copy of the EHI that already exists in a different, yet integrated, certified Health IT Module.

b. Proposal for EHI Export

ONC continues to believe that access to EHI export in such circumstances is critical. However, we recognize the potential burden in requiring the technology development and implementation of functionality to execute the capability of single patient EHI export at any time the user chooses and without subsequent developer assistance to operate, as established in § 170.315(b)(10)(i)(B), for those products that act primarily as intermediaries between systems and, through integration, function without any direct human interaction.

Therefore, we propose to exempt Health IT Modules that act primarily as intermediaries between systems and, through integration, function without any direct human interaction from the requirement in § 170.315(b)(10)(i)(B) to provide functionality without subsequent developer assistance to operate. We propose this new exemption in § 170.315(b)(10)(i)(F), and we caveat the availability of this exemption in two ways. First, in § 170.315(b)(10)(i)(F)(*1*) we propose to require that the EHI stored, or caused to be stored, by the Health IT Module certified to § 170.315(b)(10) must be a copy, whether in the same or another format, of EHI also stored by another Health IT Module with which the Health IT Module certified to § 170.315(b)(10) is integrated. Second, in order to ensure that such an exemption is appropriately limited to Health IT Modules that primarily function without user interaction and from which users would only rarely seek single patient EHI export consistent with § 170.315(b)(10)(i), we further propose in § 170.315(b)(10)(i)(F)(*2*) that any Health IT Module for which the developer receives more than 10 requests in the immediately preceding calendar year for a single patient EHI export would no longer qualify for this exemption and would need to provide functionality under § 170.315(b)(10)(i)(B) without subsequent developer assistance to operate. For purposes of this exemption, we clarify that requests for a single patient EHI export would be counted at the product-level rather than the individual instance-level. This means any request made across all deployed settings or deployed instances of the Health IT Module would count towards this proposed threshold. We note that the developer must still meet all other requirements in § 170.315(b)(10), but that such an exemption would allow them flexibility in how single patient EHI export is provided under § 170.315(b)(10)(i), including providing the export with developer assistance similar to how they provide patient population EHI export under § 170.315(b)(10)(ii).

We note that the limited circumstance defined here would not be applicable to health information exchanges or networks. ONC believes that patients and users assisting patients have a continued need for access to all single patient EHI, and products in which EHI is aggregated (such as health information exchanges and networks) should facilitate full and unfettered access to such information.

We welcome comments on this proposal, including on the threshold of 10 requests across all deployed settings (or deployed instances) of the Health IT Module per calendar year to qualify for the exemption.

c. Proposal for Associated Assurances Requirements for Single Patient EHI Export Exemption

To ensure that a developer of certified health IT with a Health IT Module certified to § 170.315(b)(10) does not inappropriately use the proposed exemption for single patient EHI export in § 170.315(b)(10)(i)(F) to block information or inhibit the appropriate access, exchange, and use of EHI, we propose a new Assurances Maintenance of Certification requirement. We propose in § 170.402(b)(2)(iii) that developers of certified health IT with Health IT Modules certified to § 170.315(b)(10) that claim the exemption proposed in

§ 170.315(b)(10)(i)(F) would need to report the number of requests for single patient EHI export on an annual basis to their ONC–ACB(s). Specifically, in § 170.402(b)(2)(iii)(A) we propose that on and after January 1, 2028, a health IT developer of a Health IT Module certified to the certification criterion in § 170.315(b)(10) and meets the requirements of paragraph (b)(10)(i)(F) must report to its ONC–ACB no later than March 1 of each calendar year how many requests it received during the immediately preceding calendar year. We welcome comments on this proposal.

11. Revised End-User Device Encryption Criterion

a. Background

In the final rule titled ''Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology'' (2014 Edition Final Rule) we included end-user device encryption requirements in § 170.315(d)(7) focused on designing EHR technology to secure EHI on end-user devices in accordance with the approach recommend by the Health IT Standards Committee (HITSC) at the time (77 FR 54236). Since finalizing this certification criterion in the 2014 Edition Final Rule, encryption technology has continued to advance significantly, and we have identified a gap in our current requirements, which only include end-user device encryption requirements and exclude server-side encryption requirements.

When finalizing our end-user device encryption requirements in § 170.315(d)(7) in the 2014 Edition Final Rule, we posited that end-user device encryption was ''more practical, effective and easier to implement'' than the general encryption requirement we had finalized originally in the ONC 2011 Edition certification criteria, which included server encryption requirements (77 FR 54236). Encryption technology and availability have significantly improved in the time since the 2014 Edition Final Rule. For example, developers using Microsoft Windows Server version 2016 and later versions have BitLocker disk encryption software readily available, and Linux-based server developers have free and open-source disk encryption utilities like Cryptsetup.[66] These tools, and others like them, make it easy for server developers to take advantage of the numerous benefits of server encryption.

Encryption of server-side data prevents unauthorized data access in many scenarios, including those involving a server breach, theft, or improper disposal. Mitigating these risks using encryption is a best practice for all server developers and, given the unique characteristics of EHI, is especially important for health IT server developers. EHI is considered one of the most valuable types of personal information for theft because of the breadth of information included in electronic health records and the long shelf life of this information. However, despite its high value, EHI often is not being properly protected, and the problem is getting worse according to data published on the Department of Health and Human Services Office for Civil Rights (OCR) website. Between 2010 and 2022, OCR received 5,144 reports of breaches affecting 500 or more individuals, impacting a total of 394,236,737 individuals.[67] The frequency of breaches affecting 500 individuals or more has increased significantly over the past few years, with almost two such breaches reported per day in 2022, nearly double the frequency in 2018.[68] These statistics indicate that vulnerabilities and risks exist in technology storing EHI in the United States. While no single solution can fully protect EHI, data breach risks can be mitigated by encryption of data maintained on servers.

b. Proposal

To better protect electronic health information stored in Health IT Modules certified under the Program, we propose to clarify the scope of information that needs to be protected in Health IT Modules certified to § 170.315(d)(7) and revise the order and sequence of existing requirements in § 170.315(d)(7) to include new requirements for server-side encryption.

First, to clarify the scope of electronic health information that needs to be protected in Health IT Modules certified to § 170.315(d)(7), we propose that on and after January 1, 2026 the information that must be protected within Health IT Modules certified to this revised criterion in § 170.315(d)(7) include all personally identifiable information (PII). This includes, but is not limited to, individually identifiable health information meeting the definition of electronic protected health information in 45 CFR 160.103, regardless of whether the information is held by or for a HIPAA covered entity or entity required to comply with the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

Second, we propose to revise existing requirements in § 170.315(d)(7) to include new requirements for server-side encryption and include the PII encryption requirements for servers in a way that maintains our existing end-user device encryption requirements and applies the existing encryption standard and the default settings requirements broadly in one criterion.

We propose to change the name of § 170.315(d)(7) to ''health IT encryption,'' to better describe the end-user and proposed server-side requirements together. We also propose moving our existing end-user device encryption requirements, in § 170.315(d)(7)(i) and (ii), into paragraph § 170.315(d)(7)(i) that expires on January 1, 2026 and is replaced by a new PII encryption requirement for end-user devices in § 170.315(d)(7)(ii) that must be met on and after January 1, 2026.

Additionally, we propose including the new server-side encryption requirement in § 170.315(d)(7)(iii) that must be met on and after January 1, 2026. We propose that this new server encryption requirement in § 170.315(d)(7)(iii) state that technology designed to store PII must encrypt the stored PII after use of the technology on those servers stops.

We also propose to move the encryption standard and default settings requirements that are currently in § 170.315(d)(7)(i)(A) and (B) respectively into their own higher-level sections in § 170.315(d)(7)(iv) and (v) respectively. Additionally, we propose that these encryption standard and default settings requirements apply to the new server encryption requirement. Pointing to an encryption standard and requiring that default settings be in place for encryption capabilities in § 170.315(d)(7) is consistent with our existing requirements for end-user device encryption, and we believe these

[66] Microsoft documentation explaining how to deploy BitLocker disk encryption on Windows Server 2016 and later: *https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server.* Homepage for the Cryptsetup utility that can be used for Linux hard disk encryption: *https://gitlab.com/cryptsetup/cryptsetup/.* Note that these tools would need to be configured to use Approved Security Functions for FIPS PUB 140–2 to meet ONC's proposed server encryption requirements outlined later in this section. Approved Security Functions for FIPS PUB 140–2 are here: *https://csrc.nist.gov/files/pubs/fips/140-2/upd2/final/docs/fips1402annexa.pdf.*

[67] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* These numbers are based on breach reports made to OCR as of May 17, 2024.

[68] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* These numbers are based on breach reports made to OCR as of May 17, 2024.

settings are necessary for our proposed new server encryption requirement as well.

While certain conformance requirements within the proposed § 170.315(d)(7) have been reorganized, as is outlined in the previous paragraphs, health IT developers with Health IT Modules certified to this criterion will continue to have traceability. If we were to finalize the updates to § 170.315(d)(7) as proposed, developers with Health IT Modules already certified to § 170.315(d)(7) would only need to consider updates to the applicable encryption standards, server-side encryption, and encryption of any non-encrypted PII for the purposes of maintaining Health IT Module certification in the future.

The permissible encryption algorithms for our proposed new server encryption requirement are listed in Annex A of The National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 140–2, October 12, 2021, which specifies the security requirements for cryptographic modules.[69] We believe Annex A of FIPS Publication 140–2 is appropriate for our proposed server-side encryption requirements for the same reasons it was considered appropriate for end-user device encryption requirements—it provides clear requirements and flexibility in demonstrating compliance (75 FR 44622). We note that the October 12, 2021, draft is the most recent version of Annex A: Approved Security Functions for FIPS Publication 140–2, and elsewhere in this Proposed Rule at III.B.4, we describe our proposal to revise the standard in § 170.210(a) to include this updated version of Annex A (Draft, October 12, 2021).

Together, we believe that end-user device and server encryption requirements help better protect PII. We clarify that in the context of this certification criterion, a server is a system designed to store PII. We also clarify that in the context of our proposed new server encryption requirement in § 170.315(d)(7)(iii), ''stops'' means that PII on a server is not actively in use and is not actively moving (*i.e.,* PII that is not being processed, updated, or otherwise acted upon). We welcome comments on these proposed changes and additions to § 170.315(d)(7).

[69] Annex A of FIPS PUB 140–2: *https://csrc.nist.gov/files/pubs/fips/140-2/upd2/final/docs/fips1402annexa.pdf.*

12. Revised Criterion for Encrypt Authentication Credentials

a. Background

In the ONC Cures Act Final Rule, we finalized an authentication credential encryption requirement in § 170.315(d)(12) (85 FR 25700). We established an approach that requires health IT developers with Health IT Modules certified to the criterion to be transparent about whether their certified Health IT Module encrypts stored authentication credentials according to industry standards by attesting ''yes'' or ''no.'' These ''yes'' or ''no'' attestations are made public on ONC's Certified Health IT Product List (CHPL), which is available at *https://chpl.healthit.gov/.*

We established this approach in acknowledgement that some Health IT Modules certifying to the certification criterion in § 170.315(d)(12) may not be designed to store authentication credentials. We included a provision in § 170.315(d)(12)(ii) that permits health IT developers attesting ''no'' to explain why their Health IT Module does not support encrypting authentication credentials. We noted in the ONC Cures Act Final Rule that the information regarding the security capabilities of certified health IT provided by the attestation increased transparency and aided 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 [70]) (85 FR 25701).

b. Proposal

We now propose to revise the requirements in the ''Encrypt authentication credentials'' certification criterion in § 170.315(d)(12). We propose to expire our current ''yes'' or ''no'' attestation requirements by moving them to § 170.315(d)(12)(i) and indicating they are applicable only for the time period up to and including December 31, 2025. We propose to replace the attestation requirements by revising § 170.315(d)(12) to include new requirements in § 170.315(d)(12)(ii) that become effective on and after January 1, 2026. Additionally, we propose that a health IT developer may meet the proposed revised certification criterion's requirements by satisfying the new conformance requirements proposed in § 170.315(d)(12)(ii) in lieu of § 170.315(d)(12)(i) prior to paragraph (i)'s December 31, 2025, expiration.

With these new requirements, we propose that Health IT Modules designed to store authentication credentials must protect the confidentiality and integrity of their stored authentication credentials. These revisions include requirements in § 170.315(d)(12)(ii)(A) and (B) for authentication credentials to be protected using either encryption and decryption according to the latest version of the Federal Information Processing Standards (FIPS) 140–2 (October 12, 2021) standard in § 170.210(a) or by hashing in accordance with the FIPS 180–4 standard specified in § 170.210(c)(2). As discussed more fully below, we believe that revising § 170.315(d)(12) to require Health IT Modules protect stored authentication credentials according to updated industry standards in § 170.210(a) is necessary and important to improve the security of certified health IT. We note in section III.B.4 in this preamble our proposal to adopt the latest available FIPS Publication 140–2 standard version in § 170.210(a)(3) and expire the old FIPS Publication 140–2 standard in § 170.210(a)(2) as of January 1, 2026.

Healthcare data breaches have trended significantly upward in recent years with around two breaches affecting 500 or more individuals reported per day in 2023, nearly double the frequency in 2018.[71] During this same period, we also found that public CHPL attestation data for Health IT Modules certified to § 170.315(d)(12) indicates that less than 73% of products meeting the Base EHR Definition in § 170.102 included a ''yes'' attestation to encrypting authentication credentials.[72] Given that protecting stored authentication credentials according to industry standards is a critical defensive step to help ensure that stolen or leaked authentication credentials are useless to an attacker, we believe it is important to require that a Health IT Module designed to store authentication credentials must protect the confidentiality and integrity of its stored authentication credentials according to § 170.315(d)(12)(ii).

We have chosen to reference the FIPS 140–2 (§ 170.210(a)) and FIPS 180–2 (§ 170.210(c)(2)) standards in § 170.315(d)(12)(ii) because they are the seminal, comprehensive, and most appropriate standards for protecting

[70] The HIPAA Security Rule is located at 45 CFR part 160 and subparts A and C of part 164.

[71] *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* These numbers are based on breach reports made to OCR as of February 12, 2024.

[72] Percentages are based on data retrieved in February 2023 from *https://chpl.healthit.gov/#/* search for ''Active,'' ''2015 CURES UPDATE'' listings certified to ''170.315 (D)(12): ENCRYPT AUTHENTICATION CREDENTIALS (CURES UPDATE) and ''170.315 (D)(13): MULTI–FACTOR AUTHENTICATION (CURES UPDATE)''

sensitive information within computer systems. Referencing these standards also remains consistent with our references to these standards in other certification criteria in our Program.

To reflect our proposed revisions to § 170.315(d)(12), we propose to rename the certification criterion from ''Encrypt authentication credentials'' to ''Protect stored authentication credentials.'' We believe ''protect'' is a broader term that more clearly includes methods like hashing that can be used to safeguard stored authentication credentials. In the ONC Cures Act Final Rule we clarified that ''encrypting authentication credentials could include password encryption or cryptographic hashing'' (85 FR 25700). Despite this clarification, we have received inquiries asking if we consider hashing an acceptable form of ''encryption'' in the context of this certification criterion. We propose updating the certification criterion title and regulation text to address such concerns. We invite comments on our proposal to revise § 170.315(d)(12) to require a Health IT Module designed to store authentication credentials to protect the confidentiality and integrity of its stored authentication credentials according to updated industry standards.

13. Health IT Modules Supporting Public Health Data Exchange

a. Background

Public health promotes and protects the health of all people and their communities. To accomplish this mission, public health authorities (PHAs) rely on public health data exchange to acquire the information they need to provide critical functions for society and to keep communities healthy.[73] However, the nation's public health infrastructure, the technology in place within PHAs, and the methods of data exchange are often siloed, dated, and incapable of quickly providing timely, actionable data needed by PHAs and their partners, resulting in delays in detecting and responding to public health threats.[74] As documented in numerous studies, and illustrated by the COVID–19 pandemic, there is an ongoing challenge for PHAs at all levels to obtain timely, accurate, representative, and actionable information from electronic health records and other related systems.[75] However, as noted in a 2022 Government Accountability Office (GAO) report, PHAs do not always have access to—or, often, the ability to share—data needed to address public health needs (emergent or otherwise). This is due, in part, to the lack of common standards utilized in the reported data, variable reporting requirements, limited interoperability of systems, and an inadequate public health data infrastructure.[76] Addressing these challenges can improve public health response readiness and the nation's healthcare system, enabling better-informed decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies.[77] [78]

Congress recognized the need to modernize our public health data infrastructure and in response to the COVID–19 pandemic passed legislation that included funding and directives related to such activities. Section 2301 of the American Rescue Plan of 2021 (ARP) (Pub. L. 117–2, enacted March 11, 2021) included funding for information technology, standards-based data, and public health reporting enhancements, including improvements to support standards-based exchange of data related to vaccine distribution and vaccinations.[79] The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) (Pub. L. 116–136, enacted March 27, 2020) provided funding to support enhancement of public health information system capabilities to address COVID–19 reporting needs.[80]

Several promising Federal efforts have been initiated to address the urgent need to improve public health infrastructure and health IT for public health to enable PHAs to get better and more timely access to the information they need to protect and improve the health of our nation. In this proposed rule, we use the phrase ''health IT for public health'' to mean hardware, software, integrated technologies or related licenses, IPs, upgrades, or packaged solutions sold as services that are designed to support public health use cases for the electronic creation, maintenance, access, or exchange of public health information, which is consistent with the ''health IT'' definition in section 13101(5) of the HITECH Act and 45 CFR 170.102. In 2020, CDC launched the Data Modernization Initiative (DMI) to modernize public health data and surveillance infrastructure.[81] More recently, CDC has released its Public Health Data Strategy (Ph.D.S), which outlines the data, technology, policy, and administrative actions essential to exchange critical core data efficiently and securely across healthcare and public health.[82] The strategy is designed to describe a path to address gaps in public health data and help the nation become response-ready, promote health equity, and improve health outcomes for all.

ONC actively works with CDC and other Federal partners on initiatives that complement, support, and extend CDC's efforts under the Ph.D.S, including USCDI+ Public Health and Helios, a Fast Healthcare Interoperability Resources® (FHIR®) accelerator through HL7®, to help address DMI priorities around data interoperability.[83] USCDI+ is intended to build upon the core dataset established in the United States Core Data for Interoperability (USCDI), a standardized set of health data classes and data elements for nationwide, interoperable health information exchange, discussed in more detail in section III.B.1 of this proposed rule. We launched USCDI+ Public Health in October 2021 to capture the data needs of public health that extend beyond USCDI to ultimately improve the availability and consistency of data necessary to support various aspects of public health.[84] In November 2021, HL7

[73] *https://www.healthit.gov/sites/default/files/page/2023-03/2023-02-08_HITAC_Annual_Report_for_FY22_supplemental_background_research_508_1.pdf.*

[74] Data Modernization Initiative Strategic Implementation Plan. December 22, 2021. Available at *https://www.cdc.gov/surveillance/pdfs/FINAL-DMI-Implementation-Strategic-Plan-12-22-21.pdf.*

[75] *See* Public Health Data Modernization: Listening Session on Real-World Testing of 21st Century Cures Act Requirements. Available at *https://www.cdc.gov/surveillance/pubs-resources/dmi-summary/index.html;* Alonzo Plough, Gail C Christopher, Equity-Centered Public Health Data Demands New Voices at the Table, Health Affairs (April, 20222) available at *https://www.healthaffairs.org/do/10.1377/forefront.20220427.865970/;* Robert Wood Johnson Foundation, Transforming Public Health Data Systems, available at *https://www.rwjf.org/en/insights/our-research/2021/09/transforming-public-health-data-systems.html,* and Bipartisan Policy Center, Call to Action for State, Territorial, and Local Policymakers to Move Public Health Forward, December, 2021, available at *https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2021/12/PHF-Call-to-Action-Policymakers-1.pdf.*

[76] *https://www.gao.gov/products/gao-22-106175.*

[77] *https://cdn.ymaws.com/www.csteorg/resource/resmgr/pdfs/pdfs2/Driving_PH_Print.pdf.*

[78] *https://www.cdc.gov/surveillance/pdfs/20_319521-D_DataMod-Initiative_901420.pdf.*

[79] *https://www.congress.gov/117/plaws/publ2/PLAW-117publ2.pdf.*

[80] *https://www.congress.gov/116/plaws/publ136/PLAW-116publ136.pdf.*

[81] *https://www.cdc.gov/surveillance/data-modernization/basics/index.html.*

[82] *https://www.cdc.gov/ophdst/public-health-data-strategy/index.html.*

[83] *https://www.cdc.gov/surveillance/policy-standards/interoperability.html.*

[84] *https://www.healthit.gov/buzz-blog/health-it/thinking-outside-the-box-the-uscdi-initiative; see also https://www.healthit.gov/topic/interoperability/uscdi-plus.*

launched Helios in collaboration with CDC and ONC.[85]

The Health Information Technology Advisory Committee (HITAC) was established by the Cures Act and is governed by the provisions of the Federal Advisory Committee Act (FACA)[86] which sets forth standards for the formation and use of Federal advisory committees. Section 3002 of the PHSA, as amended by section 4003(e) of the Cures Act, established that the FACA applies to the HITAC and that the HITAC would advise and make recommendations 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. The HITAC created a Public Health Data Systems Task Force in 2021 (2021 Task Force) to develop recommendations in response to President Biden's Executive Order on Ensuring a Data-Driven Response to COVID–19 and Future High Consequence Public Health Threats,[87] which tasked HHS with reviewing the ability of the public health infrastructure to address such threats.[88] The 2021 Task Force recommended the inclusion of ''certification of information systems for both senders and receivers'' for public health data.[89] In 2022, the HITAC convened a second Public Health Data Systems Task Force (2022 Task Force) and directed it to build on the recommendations from the 2021 Task Force to more specifically examine the existing ''(f) criteria'' within our Program, which certifies health IT for its ability to support various transmissions to PHAs.[90] The 2022 Task Force found that improvements were needed with respect to the flow of data for public health across the healthcare ecosystem and for robust support of public health in the Program. In particular, the 2022 Task Force highlighted that while the Program has certification criteria related to transmitting data to PHAs, it has not included sufficient real-world testing requirements or the ability of technology used by PHAs to receive and utilize data transmitted according to standards required for certified health IT.[91] The 2022 Task Force had several recommendations approved by HITAC, including that we establish certification criteria for Health IT Modules supporting public health use cases focused on interoperability functions such as access, exchange, and use of data, and to provide a common floor for addressing public health interoperability needs.[92] The 2022 Task Force emphasized that the intent of certification criteria related to health IT for public health would be to create a base level of interoperability inclusive of all providers and PHAs and the methods by which data is primarily electronically exchanged—not to restrict public authorities from requesting and receiving data in the manner needed to fulfill their mission.

In response to these HITAC recommendations in 2021 and 2022 and consistent with the PHSA sections 3001 and 3004 previously described (see section II.A), we are proposing several changes to existing certification criteria as well as the creation of new certification criteria related to health IT for public health. These proposals are responsive to the HITAC recommendations to ONC of increasing the adoption and use of health IT standards for electronic lab reporting, electronic case reporting, and syndromic surveillance, among others. These updates and additions to the certification criteria related to health IT for public health additionally address the HITAC's recommendations to ONC to position CDC, and other Federal partners, to be nimble, responsive, and resilient during the next public health emergency.

Additionally, CDC's Advisory Committee to the Director (ACD) recommended that a certification program for health IT for public health would help address core problems with data infrastructure and exchange.[93] The ACD recommendations include that CDC and ONC should work together to develop and implement a coordinated and phased approach for certifying health IT for public health, grounded in the use of shared data standards. Both the ACD and the HITAC recommendations highlight the shared consensus regarding the need to develop a standards-based certification program to improve the availability and interoperability of important health information between healthcare providers and PHAs.

We have also addressed public health data exchange as part of efforts related to the Trusted Exchange Framework and Common Agreement™ (TEFCA™),[94] which includes public health as a specific ''exchange purpose,'' and work is underway with the Recognized Coordinating Entity® (RCE™) to develop a Standard Operating Procedure (SOP) for the public health exchange purpose under TEFCA to support the ability of providers and PHAs to exchange information, as well as standardized, secure interoperability for PHAs to exchange information with each other.[95] Additionally, we funded the Association of State and Territorial Health Officials (ASTHO) to launch a Health Information Exchange (HIE) and Immunization Information System (IIS) COVID–19 Data Management: Immunization Data Exchange, Advancement and Sharing (IDEAS) program focused on expanding partnerships between state, regional, and local HIEs and IISs.[96] As a program deliverable, ASTHO conducted an environmental scan focusing on data sharing between HIEs and IISs.[97] Findings included the need for data exchange partners to use the same vocabularies and coding systems and for the use of a standard messaging format and transmission method for data exchange.[98]

b. Regulatory History

In addition to the efforts described above, we have adopted several standards, implementation specifications, and certification criteria related to public health as part of the Program. While the Program itself is voluntary for health IT developers, compliance with Program standards, implementation specifications, and

[85] *https://confluence.hl7.org/display/PH/Helios+FHIR+Accelerator+for+Public+Health+Home.*

[86] Federal Advisory Committee Act (FACA), Pub. L. 92–463 (1972), codified as amended at, 5 U.S.C. Chapter 10 (formerly 5 U.S.C. App. 2).

[87] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-ensuring-a-data-driven-response-to-covid-19-and-future-high-consequence-public-health-threats/#:~:text=It%20is%20the%20policy%20of,a%20better%20public%20health%20infrastructure.*

[88] *https://www.healthit.gov/sites/default/files/page/2021-08/2021-07-14_PHDS_TF_2021_HITAC%20Recommendations%20Report_Signed_508_0.pdf.*

[89] *https://www.healthit.gov/sites/default/files/page/2022-11/2022-11-10_PHDS_TF_Recommendations_Report_Transmittal_Letter_508.pdf.*

[90] *Id.*

[91] *https://www.healthit.gov/sites/default/files/facas/2022-11-10_HITAC_Meeting_Notes_508_1.pdf.*

[92] *Id.*

[93] *https://www.cdc.gov/about/pdf/advisory/dsw-recommendations-report.pdf.*

[94] *https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca#:~:text=The%20overall%20goal%20of%20the,for%20interoperability%20across%20the%20country.*

[95] *https://rce.sequoiaproject.org/tefca-and-rce-resources/.*

[96] *https://www.healthit.gov/topic/onc-funding-opportunities/funding-announcements.*

[97] *https://www.astho.org/globalassets/report/immunization-information-systems-and-health-information-exchanges.pdf.*

[98] *https://www.astho.org/globalassets/report/immunization-information-systems-and-health-information-exchanges.pdf.*

certification criteria is encouraged through CMS incentive programs. The American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5, enacted February 17, 2009) authorized incentive payments to eligible professionals, eligible hospitals, and critical access hospitals (CAHs) to promote the adoption and meaningful use of CEHRT. In 2011, CMS established the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs to encourage eligible professionals, eligible hospitals, and CAHs to adopt and make meaningful use of CEHRT. CMS changed the name of the EHR Incentive Programs to the Medicare and Medicaid Promoting Interoperability Programs in April 2018.[99] The Medicaid Promoting Interoperability Program ended in 2022, and the program is currently known as the Medicare Promoting Interoperability Program for eligible hospitals and CAHs.[100] The Medicare Promoting Interoperability Program is also a performance category component of CMS' Merit-Based Incentive Payment System (MIPS), a program that determines Medicare payment adjustments.

As we have described in prior rulemakings, Congress tied the standards, implementation specifications, and certification criteria adopted as part of the Program to the incentives available under CMS Programs by requiring the meaningful use of CEHRT (75 FR 44591). Generally, we support the use of certified health IT under CMS incentive programs by establishing standards, implementation specifications, and certification criteria for health IT as part of the Program that are then incorporated into the CMS definition of CEHRT relied upon by health care providers and other users of health IT to receive incentives from CMS programs. For example, for calendar year 2023, to be considered a meaningful user and avoid a downward payment adjustment, eligible hospitals and CAHs attesting to the Medicare Promoting Interoperability Program are required to use CEHRT that has been updated to meet the 2015 Edition Cures Update certification criteria.[101]

In the 2010 interim final rule with comment period entitled ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology'' (75 FR 2014), we first established standards and certification criteria related to public health. These included standards and certification criteria for the electronic submission of laboratory results to PHAs, electronic submission to PHAs for surveillance or reporting, and electronic submission to immunization registries. These standards and certification criteria were updated in the 2010 final rule entitled ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology'' (75 FR 44590).

In the 2012 final rule entitled ''Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology'' (77 FR 54163), we expanded the public health related standards and certification criteria and codified the 2014 Edition EHR certification criteria in § 170.314, with the public health certification criteria organized in § 170.314(f). The public health certification criteria in the 2012 final rule included:

- § 170.314(f)(1) ''Immunization information'';
- § 170.314(f)(2) ''Transmission to immunization registries'';
- § 170.314(f)(3) ''Transmission to public health agencies—syndromic surveillance'';
- § 170.314(f)(4) ''Inpatient setting only—transmission of reportable laboratory tests and values/results''; and,
- two ''optional'' certification criteria:
  - § 170.314(f)(5) ''Optional—ambulatory setting only—cancer case information''; and,
  - § 170.314(f)(6) ''Optional—ambulatory setting only—transmission to cancer registries.''

Then, in the 2014 final rule entitled ''2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange'' (79 FR 54430), we added an optional, ambulatory-setting only certification criterion for syndromic surveillance in § 170.314(f)(7).

In the 2015 final rule entitled ''2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications'' (2015 Edition Final Rule) (80 FR 62601), we revised the public health certification criteria to include the following:

- § 170.315(f)(1) ''Transmission to immunization registries,'' revised as compared to the 2014 Edition;
- § 170.315(f)(2) ''Transmission to public health agencies—syndromic surveillance,'' revised as compared to the 2014 Edition;
- § 170.315(f)(3) ''Transmission to public health agencies—reportable laboratory tests and values/results,'' revised as compared to the 2014 Edition;
- § 170.315(f)(4) ''Transmission to cancer registries,'' revised as compared to the 2014 Edition;
- a new certification criterion § 170.315(f)(5) ''Transmission to public health agencies—electronic case reporting;''
- a new certification criterion § 170.315(f)(6) ''Transmission to public health agencies—antimicrobial use and resistance reporting,'' and,
- a new certification criterion § 170.315(f)(7) ''Transmission to public health agencies—health care surveys.''

In the in the 2020 final rule entitled ''21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program'' (85 FR 25642), we revised the public health certification criterion § 170.315(f)(5) ''Transmission to public health agencies—electronic case reporting'' to incorporate the USCDI v1 standard and C–CDA companion guide (85 FR 25671). However, in the subsequent Interim Final Rule with comment period entitled ''Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency'' (85 FR 70064), we further revised that requirement so that health IT developers certifying to § 170.315(f)(5) were required to conform to data classes expressed in the USCDI standard in § 170.213 or the Common Clinical Data Set for the period before December 31, 2022 (85 FR 70076). Additionally, in a final rule titled, ''Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing'' (HTI–1 Final Rule) (89 FR 1192), we revised the ''Transmission to public health agencies—electronic case reporting'' certification criterion in § 170.315(f)(5) to replace the functional requirements

[99] *https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs.*

[100] *https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms#:~:text=About%20the%20Promoting%20Interoperability%20Program&text=Beginning%20in%20calendar%20year%20*(CY,for%20eligible%20hospitals%20and%20CAHs.

[101] *https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification#:~:text=In%20order%20to%20efficiently%20capture,data%20in%20a%20structured%20format.*

with standards and implementation guides (IGs) and updated vocabulary standards in § 170.207(a), (c), and (e) that are referenced in several public health certification criteria.

Currently, the Program includes seven certification criteria related to public health (see § 170.315(f)). We are referring to these seven certification criteria as the ''(f) criteria'' in this proposed rule and may refer to them in that way in future rulemaking. These (f) criteria are:

- § 170.315(f)(1) Transmission to immunization registries
- § 170.315(f)(2) Transmission to public health agencies—syndromic surveillance
- § 170.315(f)(3) Transmission to public health agencies—reportable laboratory tests and values/results
- § 170.315(f)(4) Transmission to cancer registries
- § 170.315(f)(5) Transmission to public health agencies—electronic case reporting
- § 170.315(f)(6) Transmission to public health agencies—antimicrobial use and resistance reporting
- § 170.315(f)(7) Transmission to public health agencies—healthcare surveys

Generally, the certification criteria listed above include report generation and transmission functionalities, require Health IT Modules to adhere to specific standards and implementation guides, and provide assurances that the certified Health IT Module performs as intended. However, we note that the certification criteria do not include all functionalities that may be of interest to public health, nor does the Program certify data quality or the technology that receives incoming submissions. Additionally, most of these certification criteria have not been substantially updated since 2015, as described above.

c. Proposal Overview

As indicated in the regulatory history, we have not updated the Program's certification criteria related to public health since 2015, with the exception of standards and IGs being added to the requirements for the ''Transmission to public health agencies—electronic case reporting'' certification criterion in § 170.315(f)(5) and updates to several vocabulary standards in the HTI–1 Final Rule. Standards referenced in § 170.315(f)(5), § 170.315(f)(6), and § 170.315(f)(7) have advanced through the Standards Version Advancement Process (SVAP), which allows health IT developers to voluntarily use more recent versions than those adopted in regulation as part of certification under the Program.[102]

Considering the urgent need for greater public health data exchange and access to more actionable data by PHAs, we propose a multi-pronged approach that takes advantage of and builds upon the various efforts described above, including advancements in FHIR-based solutions and evolving standards related to public health interoperability. For example, a CDC report on public health data modernization found that enabling greater flow of health information from electronic health records to PHAs using HL7 FHIR-based standards could allow public health to take advantage of advanced data science capabilities such as predictive analysis, enhanced surveillance, personalized communications, and streamlining of data sharing while protecting patient privacy.[103]

We propose to revise the Program's current certification criteria related to public health in § 170.315(f); add several new functional requirements and adopt newer versions of standards within the current (f) criteria; add two additional certification criteria in the current (f) criteria for birth reporting and bi-directional exchange with a prescription drug monitoring program (PDMP); adopt new certification criteria for health IT for public health in § 170.315(f)(21) through (29); adopt enhancements to the standardized API for patient and population services in § 170.315(g)(10) (see section III.B.19); and adopt a new certification criterion for a standardized FHIR-based API for public health data exchange in § 170.315(g)(20), which we also propose to adopt as part of the Base EHR definition. Additionally, we propose to revise the naming of the (f) criteria to reflect first the public health use case, followed by the functionality the certification criterion supports. We believe this will help support clarity for both the use case and the specific capabilities as we continue to expand health IT supports for public health data exchange. While the proposed (f) criteria updates and additions focus primarily on health IT for public health, we believe it is likely that these certification criteria may be used in other use cases and settings.

In general, we seek to frame health IT certification criteria so that the certified health IT can be used by a wide range of entities in a different setting—including by health care providers, researchers, PHAs, or third-party entities supporting public health use cases defined in § 170.315(f), such as health information networks or other types of registries. For these public health use cases, we propose to group functions within use cases based on the implementation guides and the transactions within a bi- or multi-directional information exchange workflow. These functions may be part of a wide range of technologies, employed by a wide range of users, and we remain agnostic to the specific entity that may purchase any health IT product certified to the functionality. As such, we use the term ''health IT for public health'' to support the functions and transactions in the public health use cases in § 170.315(f)(21) through (29). Accordingly, we propose to revise the naming of the current (f) criteria as follows:

- § 170.315(f)(1) Immunization registries—Bi-directional exchange
- § 170.315(f)(2) Syndromic surveillance—Transmission to public health agencies
- § 170.315(f)(3) Reportable laboratory results—Transmission to public health agencies—and Laboratory Orders—Receive and validate
- § 170.315(f)(4) Cancer registry reporting—Transmission to public health agencies
- § 170.315(f)(5) Electronic case reporting—Transmission to public health agencies
- § 170.315(f)(6) Antimicrobial use and resistance reporting—Transmission to public health agencies
- § 170.315(f)(7) Health care surveys—Transmission to public health agencies

The new (f) criteria for public health data exchange and for health IT for public health that we propose to adopt are:

- § 170.315(f)(8) Birth reporting—Transmission to public health agencies
- § 170.315(f)(9) Prescription Drug Monitoring Program (PDMP) Databases—Query, receive, validate, parse, and filter
- § 170.315(f)(21) Immunization information—Receive, validate, parse, filter, and exchange—response.
- § 170.315(f)(22) Syndromic surveillance—Receive, validate, parse, and filter
- § 170.315(f)(23) Reportable laboratory test values/results—Receive, validate, parse, and filter
- § 170.315(f)(24) Cancer pathology reporting—Receive, validate, parse, and filter
- § 170.315(f)(25) Electronic case reporting—Receive, validate, parse, filter, electronic initial case reports and

[102] *https://www.healthit.gov/topic/standards-version-advancement-process-svap.*

[103] *https://www.cdc.gov/surveillance/data-modernization/index.html.*

reportability response; and create and transmit reportability response

- § 170.315(f)(28) Birth reporting—Receive, validate, parse, and filter
- § 170.315(f)(29) Prescription Drug Monitoring Program (PDMP) Data—Receive, validate, parse, filter prescription data, support query and exchange

We also propose revisions to the ''Computerized provider order entry—laboratory'' certification criterion in § 170.315(a)(2) that relate to the proposed updates to the public health certification criteria listed above. Please see section III.B.18 for detail on those proposed updates to § 170.315(a)(2).

We propose this multi-pronged approach—updating existing requirements, adding new requirements for receipt, updating standards, and including a glidepath for transitioning to FHIR-based exchange in the future—to harmonize data exchange across the industry and further advance public health infrastructure to be response-ready, scalable, and flexible. We intend for this approach to allow for systems to mature and advance in an aligned fashion, reduce the need for manual workarounds and intervention, and lead to wider adoption of modern standards-based capabilities.

We understand that some health IT certification terms used in ONC's regulations for specific technical actions or capabilities may not be the same uses of the terms by the public health or healthcare sector when discussing programmatic activities. For example, in the Program we use the term ''validate'' in reference to the technical capability to correctly identify if a structured document or message received is conformant to a standard and if formats or vocabulary standards are valid or invalid. This is a necessary technical step to map data received in an interoperable manner. Public health or quality reporting related organizations may use the term ''validate'' to refer to an organizational or programmatic process to support program integrity, data accuracy, and data quality. In order to maintain consistency within the Program and to provide clarity for health IT developers, we use terms that describe health IT software functions that—while they may enable such activities by users—are specific to technical requirements. In addition, we use terms that are consistent across certification criteria—such as receive, validate, parse, and filter—to clearly and consistently define health IT functions in a manner that supports health IT developers participating in the Program. The capabilities we propose in this manner are intended to advance tools which can be used in a variety of ways to support greater efficacy across multiple programmatic and organizational use cases and processes for the public health and healthcare community.

Prior experiences with the Program demonstrated an imperative to test both the sending and receiving of information, particularly in HL7 messages and documents. The initial requirement of Continuity of Care Documents (CCDs) in early iterations of the Program only included the functionality to create and send, resulting in multiple deviations and variations of the same document type and creating challenges with receiving the same standard from different vendors. Such variability included different formatting, such as line and page breaks or representation of date, as well as including or excluding specific data elements, such as onset time of problem.[104] These variations, while allowed under the Program at the time, made receiving, integrating, and interpreting CCDs challenging. However, when certification requirements and associated testing expectations were updated to include the receipt of CCDs as well, there was a noticeable improvement in consistency. Over time, implementation guides developed through standards development organizations became more constrained, with fewer areas of optionality, and companion guides supplemented these IGs, reducing the variations discussed above, and improving interoperability.

These lessons in the early implementation of the Program were considered when developing the current proposals. For public health reporting, only sending systems—namely health IT used by health care providers—have been held to requirements for transmission. Similar divergence in minimum system capabilities and variable adoption and use of established national standards between certified health IT developers and health IT for public health have created challenges for PHAs, which have struggled to make use of data that is not consistent, even when it conforms to a healthcare standard. At best, these differences result in significant inefficiencies, as PHAs must develop manual workarounds and custom tools that standardize and format incoming data to reduce processing time and improve receipt, data mapping, and parsing processes. At worst, these differences impede public health's ability to quickly translate data it receives from healthcare into actions that protect and support the health of all people and their communities.

By establishing minimum functional capabilities and exchange standards for health IT and health IT for public health to send and receive public health data, we expect to enhance interoperability across healthcare and public health and provide a long-term mechanism for alignment as data exchange matures over time. Modernization efforts across health IT and health IT for public health will progress and upgrade on the same timeline, using the same standards in their entirety.

d. Revised Certification Criteria for Health IT Modules Supporting Public Health Data Exchange

We propose to revise the current certification criteria located in § 170.315(f) as described below.

i. § 170.315(f)(1)—Immunization Registries—Bi-directional Exchange

While immunization reporting is one of the most advanced components of the public health data exchange ecosystem, challenges remain. Throughout the COVID–19 pandemic, certain issues rose in prominence, such as individuals needing access to their personal immunization histories from health IT systems and providers being unable to consistently query or view vaccines given at different places of care. Further, there were challenges with Health IT Modules being unable to consistently provide bulk access on vaccinated populations to immunization systems (*e.g.,* to understand if students were up to date on vaccines for vaccine-preventable diseases).

The current certification criterion in § 170.315(f)(1) has been widely implemented in Health IT Modules but has not been updated since 2015, with the exception of the vocabulary standards in § 170.207(e) that are referenced in the certification criterion and updated in the HTI–1 Final Rule (89 FR 1226). We propose to update the Immunization Messaging Implementation Guide (IG) standard in § 170.205(e) to the HL7 v2.5.1 IG for Immunization Messaging, Release 1.5, Published October 2018, which is a compilation of the Release 1.5 version and the Addendum from 2015 referenced in the current Program, and incorporate it by reference in § 170.299. We are aware that the HL7 Public Health Workgroup will work on further updates to the IG, based in part on

[104] D'Amore JD, Sittig DF, Wright A, Iyengar MS, Ness RB. The promise of the CCD: challenges and opportunity for quality improvement and population health. AMIA Annu Symp Proc. 2011; 2011:285–94. Epub 2011 Oct 22. PMID: 22195080; PMCID: PMC3243208.

lessons learned from the pandemic, but that this new version will likely not be published until mid-to-late 2024. We welcome comments on advances beyond the current 1.5 version of the IG and encourage participation in the HL7 Public Health Workgroup. We also propose that adoption of the standard in § 170.205(e)(4) expires on January 1, 2028. Additionally, as described in the ''Minimum Standards Code Sets Updates'' section (III.B.5), we propose to update the vocabulary standards in § 170.207(e) that are referenced in § 170.315(f)(1) and thus are proposing to update § 170.315(f)(1)(i)(B) to reference the new proposed § 170.207(e)(5) and to update § 170.315(f)(1)(i)(C) to reference the new proposed § 170.207(e)(6).

We propose to add a functional requirement in § 170.315(f)(1)(iii) to receive incoming patient-level immunization-specific query or request from external systems and respond. We propose to revise the name of the certification criterion in § 170.315(f)(1) to ''Immunization registries—Bi-directional exchange'' to more accurately represent the capabilities included in the certification criterion. We note that we additionally propose a requirement in support of requests for multiple patients' data as a group using an application programming interface in § 170.315(g)(20)(ii) and direct readers to section III.B.13.f for further information on that related proposal, in addition to our proposed revisions to § 170.315(g)(10) which includes capabilities to support multiple patients' data as a group using an application programming interface (section III.B.19). We expect these changes to enable more approaches for bi-directional exchange of immunization information. Further, we propose patient access to their immunization information stored in Health IT Modules using SMART Health Cards ''verifiable health records'' in proposed § 170.315(g)(10) and direct readers to section III.B.19 for further information on that proposal.

We expect these proposed changes would improve patient access to more complete and standardized immunization information stored in Health IT Modules, and request feedback on this approach. Specifically, we request feedback on the standard referenced in § 170.205(e) and whether we should consider adopting that soon-to-be most current version in a final rule, as we are aware that an updated version of the standard is due to be published in mid-2024. We request feedback on the functional requirement to respond to patient-level, immunization-specific queries from external systems and request comment on if the standard referenced in § 170.205(e) is sufficient for the proposed functional requirement to respond to incoming patient-level and immunization-specific queries, or if that is better handled through the IG currently going through HL7 processes for updates.

We propose to revise the certification criterion in § 170.315(f)(1) to include revised minimum standard code set requirements, updated implementation specifications, and new functionality. We propose that, for the time period up to and including December 31, 2026, a Health IT Module may continue to be certified to the existing version of the certification criterion as described in § 170.315(f)(1)(i), with proposed modifications for clarity and with a proposed revision to include the minimum standard code set updates for representation of historic and administered vaccines proposed for adoption in § 170.207(e), or it may be certified to the newly proposed certification criteria in § 170.315(f)(1)(ii) and (iii). We propose the new and revised certification criteria in § 170.315(f)(1)(ii) and (iii) to replace the existing certification criterion in § 170.315(f)(1)(i) beginning on January 1, 2027. Specifically, the proposed revisions to the certification criterion in § 170.315(f)(1)(ii) include updates to the minimum standards specified in § 170.207(e), use of newer versions of implementation specifications proposed for adoption in § 170.205(e), and new functionality to enable a user to receive and respond to incoming patient-level immunization-specific query or request from external systems. We propose that a Health IT Module certified to § 170.315(f)(1) must be updated to meet the requirements of the revised certification criterion in § 170.315(f)(1)(ii) and the requirements in § 170.315(f)(1)(iii), and that a health IT developer must provide such updated technology to their customers by no later than December 31, 2026. We propose that any Health IT Module seeking certification to the certification criterion in § 170.315(f)(1) on and after January 1, 2027, must meet the revised requirements in § 170.315(f)(1)(ii) and the requirements in § 170.315(f)(1)(iii).

ii. § 170.315(f)(2)—Syndromic Surveillance—Transmission to Public Health Agencies

Syndromic surveillance has proven to be a vital component of public health data exchange and surveillance. Such data provide early indicators of public health threats, identify changes in occurrence of disease, illness, or injury patterns, and detect population-wide hazards. Today, the Program references an implementation guide last updated in 2015. Due to outdated cardinality within the standard and customization in the implementation of the standard, there are often missing or incomplete data elements.

The current certification criterion in § 170.315(f)(2) has not been updated since 2015 and references a 2015 ADT-based IG published through CDC's Public Health Information Network (PHIN). The current version of the IG, Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1—US Realm Standard for Trial Use, July 2019 published by HL7, more specifically defines the required data elements and message specifications for an ADT-based interface implemented specifically for syndromic surveillance. This standard includes new and updated data elements to aid in public health surveillance, including, but not limited to, patient discharge disposition, patient class, diagnosis code, reason for admission, and service location. Additionally, the observation component within the implementation guide now contains additional required elements relevant to public health, including, but not limited to, pregnancy status, travel history, and acuity. These new and updated data elements provide additional information for PHAs to inform assessment of emerging threats and the proceeding action.

We propose to revise the standard in § 170.205(d), which is referenced in § 170.315(f)(2), to reference the most recent IG, HL7 Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1—US Realm Standard for Trial Use, July 2019 in § 170.205(d)(1) and incorporate it by reference in § 170.299. We also propose to add an expiration date of January 1, 2027 for the standards previously adopted in § 170.205(d)(2) and (d)(4). However, we propose that the standard adopted in § 170.205(d)(2) shall include an indication that the expiration is for the purposes of the certification criteria in § 170.315(f). We propose that the adoption of the standard in § 170.205(d)(2) on behalf of HHS shall be otherwise maintained as it is currently referenced by HHS programs for other use cases. We propose that any health IT module certified to § 170.315(f)(2) would be required to meet at least one implementation specification that is (1) adopted in § 170.205(d) or approved for SVAP and (2) not expired at the time of use. We propose that a health IT developer must update any health IT module certified to § 170.315(f)(2) and provide such

updated module to its customers by the expiration date of the applicable standard in order to maintain certification of the health IT module. These revisions to the certification criterion in § 170.315(f)(2) would support additional data elements being shared with syndromic surveillance programs. We further propose to change the name of the criterion in § 170.315(f)(2) to Syndromic surveillance—Transmission to public health agencies.

iii. § 170.315(f)(3)—Reportable Laboratory Results—Transmission to Public Health Agencies—and Laboratory Orders—Receive and Validate

The COVID–19 pandemic brought issues with laboratory data interoperability and associated reporting challenges to light. However, many of these issues are not specific to the pandemic and are instead due to the existing infrastructure and low adoption of current standards. Health IT Modules currently exchange older versions of the electronic laboratory reporting standard that no longer fully meet the needs of public health. We recognize there are also issues facing laboratory reporting and interoperability related to local codes and the manual effort involved with mapping local codes to standard codes. We received feedback about the challenges and time it takes for the mapping needed for exchange, and the downstream issues that occur if the mapping is not completed. However, we do not believe this can be solved solely through updates to the Program, which can require that technology support standard codes but cannot mandate that users record data using such standard codes. We will continue to partner with industry and others on addressing these broader challenges. We propose that health IT presented for certification support use of at least one of the versions of Systemized Nomenclature of Medicine—Clinical Terms (SNOMED CT®),[105] Logical Observation Identifiers Names and Codes (LOINC®),[106] and the Unified Code for Units of Measure (UCUM) [107] code sets specified in § 170.207(a), (c), and (m) respectively to include updated code sets.

We propose to revise the certification criterion in § 170.315(f)(3) to include these revised minimum standard code set requirements, as well as updated implementation specifications, and new functionality. The proposed revisions to the certification criterion include the same minimum standards updates in § 170.207(a), (c), and (m), use of newer versions of implementation specifications proposed for adoption in § 170.205(g), and new functionality to enable a user to receive and validate reportable laboratory order consistent with the new standards proposed for adoption in § 170.205(g).

The certification criterion in § 170.315(f)(3) is specific to lab results being transmitted to PHAs and has been applied primarily to Health IT Modules reporting laboratory values/results to jurisdictional PHAs. The certification criterion currently only includes transmission of laboratory results and does not cover functions related to the laboratory order. We propose to update the certification criterion to also include functionality for Health IT Modules to receive, validate, parse, and filter laboratory orders, according to the standard proposed in § 170.205(g)(2). We also propose to update the certification criterion to reference the standard proposed in § 170.205(g)(3) for the transmission of laboratory results.

We propose to revise the content and exchange standards for electronic transmission of lab results to PHAs in § 170.205(g). In § 170.205(g) we propose to reorganize the paragraph to include the current standard HL7 2.5.1, HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm) (ELR) with Errata and Clarifications, and ELR 2.5.1 Clarification Document for EHR Technology Certification adopted in § 170.205(g) and incorporated by reference in § 170.299 into a new paragraph (1). We propose an expiration date of January 1, 2028 for the standard in § 170.205(g)(1). We propose to adopt the standard for HL7 Version 2.5.1 Implementation Guide: Laboratory Orders (LOI) from EHR, Release 1, STU Release 4—US Realm in § 170.205(g)(2) and incorporate it by reference in § 170.299. We propose to adopt in § 170.205(g)(3), and incorporate by reference in § 170.299, the standard for HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface, Release 1 STU Release 4—US Realm (LRI), and to specify the use of the Public Health Profile, in addition to the ELR IG.

We propose to revise § 170.315(f)(3)(ii) to reference LRI in addition to the HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm) (ELR). We propose to revise the standards in § 170.207(a), (c), and (m), which are referenced in § 170.315(f)(3)(i) and (ii), to reference the latest versions of SNOMED CT, LOINC, and UCUM respectively. We further propose to add a functional requirement in § 170.315(f)(3)(ii) requiring the ability to receive, validate, parse, and filter reportable laboratory orders according to the standards proposed in § 170.205(g)(2) and (g)(3). Additionally, we propose to rename the certification criterion in § 170.315(f)(3) to ''Reportable laboratory results—Transmission to public health agencies—and Laboratory Orders—Receive and validate.''

The proposed changes to the certification criterion in § 170.315(f)(3) would help increase the data shared between healthcare providers, laboratories, and PHAs and would increase interoperability among the different systems in place at each entity. Our proposed changes would also provide more complete patient-level information for contact tracing, patient outreach, direct care, and other clinical and public health activities.

The use of the LRI IG would provide more specificity than ELR, which can decrease the need for one-off mapping. Given the benefit of the LRI IG, we propose adding the LRI as an option for reporting to PHAs, in addition to the existing ELR IG. Additionally, the LRI and LOI IGs could have use beyond public health reporting, which can reduce implementation and maintenance burden for hospitals and providers, as both the LOI and LRI standards have multiple use cases defined in the IGs, allowing for more flexibility, reusability, and scalability. We are proposing to add the option of the public health profile in the LRI IG, given that it is an updated version of the ELR R1 IG, but request comment on whether there are additional profiles that should also be included within the LRI IG as part of the updated § 170.315(f)(3) certification criterion.

The LOI IG makes important patient demographic information required, including race, ethnicity, sex, and contact information, which may allow PHAs to get more complete data in circumstances when the laboratory has these data elements and can appropriately fill the fields. This demographic information can also be used to improve patient matching, which in turn improves patient care and the efficiency of care. In one study, electronic laboratory reports were missing data on race more than one-third of the time and data on ethnicity were present less than one-fifth of the time.[108] Missing data in laboratory

[105] *https://www.snomed.org/.*

[106] *https://loinc.org/.*

[107] *https://ucum.org/.*

[108] Electronic health information quality challenges and interventions to improve public health surveillance data and practice.—Abstract—

Continued

results to PHAs also remains a problem, which has not been solved through various attempts within industry. However, there is currently low uptake of the LOI and LRI standards, despite the increased specificity. We believe that including both standards in the Program will lead to more complete demographic information and higher rates of adoption.

We propose that for the time period up to and including December 31, 2027, a Health IT Module may continue to be certified to the existing version of the certification criterion as described in § 170.315(f)(3)(i), with proposed modifications for clarity and with a proposed revision to include the minimum standard code set updates in § 170.207(a), (c), and (m). We propose that a Health IT Module certified to § 170.315(f)(3) must be updated to meet the requirements of the revised certification criterion in § 170.315(f)(3)(ii) and that a health IT developer must provide such updated technology to their customers by no later than December 31, 2027. We propose that any Health IT Module seeking certification to the certification criterion in § 170.315(f)(3) on and after January 1, 2028, must meet the revised requirements in § 170.315(f)(3)(ii). We welcome comment on this proposal.

We recognize that there is a high volume of laboratory reporting interfaces in place today, for clinical and public health purposes, among others. As such, we request comment on whether the time period to phase out the ELR IG is sufficient, or if there needs to be a longer transitional period where both LRI and ELR are allowed for the purposes of transmitting laboratory results/values to PHAs. If January 1, 2028, is not feasible for the shift to only using LRI, we request comment on a feasible date for this transition.

We further request comment on whether we should specify the LOI IG standard, or whether we should instead include the functional requirements for the receipt, validation, parsing, and filtering of orders without referencing a specific standard. We also request comment on whether there are specific profiles within the LOI IG that should be referenced rather than the IG in its entirety.

iv. § 170.315(f)(4)—Cancer Registry Reporting—Transmission to Public Health Agencies

Cancer reporting is an important, mandatory component of cancer control efforts in the United States. State registries collect information on diagnosed cases of cancer, treatments, and demographic information. Such information informs interventions and helps allocate resources in communities and populations affected by high rates of cancer. For example, in areas where high rates of breast cancer are diagnosed, PHAs can work with healthcare organizations and providers on programs and efforts to increase early screening and other preventative interventions.

We propose to revise the certification criterion in § 170.315(f)(4) to include revised minimum standard code set requirements, updated implementation specifications, and new functionality. Since our last rulemaking cycle, there have been minor updates to the CDA Implementation Guide for Cancer Registry Reporting,[109] which is currently referenced in § 170.205(i)(2) and is required by the certification criterion. There is also a FHIR IG for cancer registry reporting that has been used in several pilots: Central Cancer Registry Reporting Content IG 1.0.0—STU 1.[110]

We propose to modify the certification criterion to specify that a Health IT Module would need to support the creation and submission of cancer registry reports using either (at least one) of these standards:

- The cancer FHIR reporting bundle and accompanying profiles according to the HL7 FHIR Central Cancer Registry Reporting Content IG 1.0.0—STU1 in § 170.205(i)(3), with the requirement that all data elements indicated as ''mandatory'' and ''must support'' in the IG must be supported, including support for the requirements described in the ''Central Cancer Registry Reporting HER Capability Statement,'' or
- The HL7 CDA® Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1—US Realm in § 170.205(i)(2).

Our intent would be that a certified Health IT Module supports at least one of these kinds of standards, but we do not preclude a Health IT Module from supporting both. However, we request comment on this approach and on whether we should instead require a Health IT Module certified to this certification criterion to support both the CDA IG and the FHIR reporting bundle and accompanying profiles within the Central Cancer Registry Reporting Content IG for the purpose of cancer registry reporting. We also note our proposal to create a standardized API for public health in § 170.315(g)(20) as described section III.B.13.f, which also addresses standards-based API information exchange for public health.

We also propose the inclusion of an additional requirement within the cancer registry reporting certification criterion, to include cancer pathology reporting. Cancer pathology reporting is an important component of diagnosing cancer and understanding how advanced cases are at the point of diagnosis. Pathology reporting for this certification criterion has not been part of our Program in the past, but we have heard feedback that pathology laboratory data is not being collected or exchanged in a standard way. Having standardized, electronic pathology reports would be an important foundation to more complete and accurate understanding of cancer diagnoses and assessing the stage at diagnosis. However, for cancer registries to receive all the information needed for accurate assessment, the data elements within the LRI IG are not enough for cancer pathology reporting. As such, CDC's National Program of Cancer Registries has been actively working with state PHAs and pathology partners, including the College of American Pathologists (CAP), to develop and pilot a FHIR Implementation Guide for cancer pathology reporting: Cancer Pathology Data Sharing 1.0.0—STU1. Early results of these pilots demonstrate that use of this implementation guide will reduce the need for manual intervention and data cleansing, aid in more timely reporting, and include data elements that are important for public health action.

We propose to adopt the standard HL7 FHIR Cancer Pathology Data Sharing, 1.0.0—STU1 in § 170.205(i)(4) and incorporate it by reference in § 170.299. We also propose to revise § 170.315(f)(4)(ii) to add a requirement in § 170.315(f)(4)(ii)(C) to create and transmit cancer pathology laboratory values and results in accordance with the proposed standard referenced in § 170.205(i)(4), Cancer Pathology Data Sharing, 1.0.0—STU1, including support for all ''mandatory'' and ''must support'' data elements within the IG, including support for the requirements described in the ''Central Cancer Registry Reporting Pathology EHR Capability Statement.'' We also propose changes to the name of this certification criterion. Specifically, we propose to change the name from ''Transmission to cancer registries'' to ''Cancer registry

Europe PMC. *https://europepmc.org/article/PMC/3804098.*

[109] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=398.*

[110] *https://build.fhir.org/ig/HL7/fhir-central-cancer-registry-reporting-ig/usecases.html.*

reporting—Transmission to public health agencies''. We welcome comments on the above proposal.

Finally, we propose to add a timeline to allow certification of a Health IT Module to the current certification criterion in § 170.315(f)(4) for the period up to and including December 31, 2027, after which period only the revised certification criterion in § 170.315(f)(4)(ii) would be available for certification. We propose that, for the time period up to and including December 31, 2027, a Health IT Module may continue to be certified to the existing version of the certification criterion as described in § 170.315(f)(4)(i), with modifications for clarity and with a proposed revision to include the minimum standard code set updates. The proposed revisions to the certification criterion include updates to the same minimum standards updates, use of newer versions of implementation specifications, and new functionality as described above. We propose that a Health IT Module certified to § 170.315(f)(4) must be updated to meet the requirements of the revised certification criterion and that a health IT developer must provide such updated technology to their customers by no later than December 31, 2027. We propose that a Health IT Module seeking certification to § 170.315(f)(4) on and after January 1, 2028, must meet the requirements described in § 170.315(f)(4)(ii).

We welcome comments on the above proposal.

v. § 170.315(f)(5) Electronic Case Reporting—Transmission to Public Health Agencies

In the HTI–1 Final Rule, we finalized requirements in § 170.315(f)(5) for compliance with specific standards for electronic case reporting to PHAs (89 FR 1231). Based on commenters' response to the proposal, we finalized allowing either the CDA or FHIR standard for the transmission of electronic case reports and reportability responses (RRs), as well as the ability to consume and process electronic case reporting trigger codes based on a match from the Reportable Conditions Trigger Code (RCTC) value set as specified in the HL7 FHIR electronic case reporting (eCR) IG. As finalized in the HTI–1 Final Rule, after December 31, 2025, developers would only be able to certify to case reporting using the standards-based approach described § 170.315(f)(5)(ii), and previously certified products would need to update their certification to the standards-based approach described in § 170.315(f)(5)(ii) by December 31, 2025 (89 FR 1228).

We believe requiring Health IT Modules to conform to a single standard, specifically the HL7 FHIR standard, would coalesce industry, PHAs, and other interested parties to dedicate resources towards improved functionality and interoperability for electronic case reporting. The use of HL7 FHIR-based solutions encourages more flexibility and reduced burden for both initial development as well as maintenance for healthcare information technology developers and aligns with CDC's Public Health Data Strategy. The Public Health Data Strategy prioritizes electronic case reporting as an important automation that reduces burden and encourages more complete and timely data exchange.

We propose no changes to the capabilities specified within the certification criterion in § 170.315(f)(5), but we do propose to update the standard used for the certification criterion in § 170.205(t)(2). Given the potential benefits of adopting a single standard, and our overall progress toward shifting to HL7 FHIR-based standards and solutions when appropriate and feasible, we propose that adoption of the CDA-based standard in § 170.205(t)(2) expires on January 1, 2028. This proposal would have the effect of requiring all Health IT Modules certified to § 170.315(f)(5) to use the eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1). We propose that Health IT Modules be required to support the HL7 FHIR-based IGs beginning January 1, 2028 to allow developers, intermediaries, and PHAs to make the needed updates to the HL7 FHIR eCR IG and develop needed system upgrades and solutions to transmit electronic case reports and receive RRs that adhere to the HL7 FHIR eCR IG implementation specification adopted in § 170.205(t)(1).

We propose to maintain in § 170.315(f)(5)(ii) adherence to specific aspects of the HL7 FHIR eCR IG to allow for flexibility: the electronic initial case report (eICR) profiles and the RR profile of the HL7 FHIR eCR IG, and the ability to consume and process electronic case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set as specified in the HL7 FHIR eCR IG. We welcome comments on this proposal.

vi. § 170.315(f)(6)—Antimicrobial Use and Resistance Reporting—Transmission to Public Health Agencies

The monitoring of antimicrobial use and resistance is a vital component of public health reporting, particularly as antimicrobial resistance rates continue to rise across the United States.[111] In order to adequately address this issue, timely reporting to PHAs is important; such reporting can allow for prescribers to receive feedback regarding prescribing practices and improve the appropriate use of antimicrobials.

CDC's National Healthcare Safety Network (NHSN) collects information on antimicrobial use and resistance from inpatient facilities enrolled in and reporting to its Patient Safety Component, including (but not limited to) general hospitals, CAHs (critical access hospitals), children's hospitals, long term acute care hospitals, military and veterans' hospitals, psychiatric hospitals, and rehabilitation hospitals. CDC uses antimicrobial use and resistance data reported through NHSN to generate metrics that states, facilities, and other users, such as hospital associations, use to improve clinical care and guide public health action. These data also provide a national picture of the threat posed by antimicrobial overuse and resistance. Given the importance of these data for patient safety and national efforts to combat antibiotic resistance, in FY 2022, CMS finalized a requirement that eligible hospitals and CAHs participating in the Medicare Promoting Interoperability Program must begin reporting a new Antimicrobial Use and Resistance (AUR) Surveillance measure for Electronic Health Record (EHR) reporting periods in calendar year (CY) 2024 (87 FR 49335 through 49337).

We propose minimal changes to the certification criterion in § 170.315(f)(6), specifically, revising to reference the standard in § 170.205(r) instead of the current reference to § 170.205(r)(1). We then propose several revisions to the standard adopted in § 170.205(r). Specifically, we propose the adoption of the standard in § 170.205(r)(1) would expire on January 1, 2027. We also propose that the standard in § 170.205(r)(1) only requires conformance to § 170.205(r)(1)(i) and (ii) for the time period up to and including December 31, 2025. We propose to add an updated version of the standard in § 170.205(r)(2) to include HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release 3—US Realm, December 2020 and to incorporate it by reference in § 170.299. The updated IG can lead to more specific and complete information being shared with PHAs, allowing for follow-up activities and research to address rising rates of antimicrobial resistance. The updated version

[111] *https://www.cdc.gov/nhsn/pdfs/pscmanual/11pscaurcurrent.pdf.*

includes new and updated templates and value sets that enable more advanced reports. This proposal would mean that the updated templates in the new IG would replace the two specific components of the prior IG in § 170.205(r)(1) identified for expiration on January 1, 2026, and then upon the expiration of the prior standard in its entirety on January 1, 2027, the updated template in the new IG in § 170.205(r)(2) would become the only applicable version of the specifications for certification to the certification criterion.

This updated version of the standard was previously advanced for voluntary adoption under our SVAP process for two of the three sections required within the current certification criteria: HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 and Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1. We propose advancing to the updated version by expiring the adoption of the prior standard components on January 1, 2026, for two of the required sections of the implementation guide referenced within current certification criteria given benefits listed above and advancement of system capabilities to support the standard since previous SVAP cycles. The third required component, ''Antimicrobial Use (AUP) Summary Report (numerator and denominator)'' should continue to use the standard HL7 Implementation Guide for CDA Release 2—Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm, until the expiration date of the entire standard on January 1, 2027. The two required components that are in the updated IG are HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator); Antimicrobial Resistance Option (ARO) Summary Report (Denominator).

We also propose minimal changes to the name of the certification criterion in § 170.315(f)(6) to be ''Antimicrobial use and resistance reporting—Transmission to public health agencies.'' We welcome comments on the above proposal.

vii. § 170.315(f)(7)—Health Care Surveys—Transmission to Public Health Agencies

Data from the National Health Care Surveys, sent to CDC's National Center for Health Statistics, provides information on healthcare utilization, and includes information related to symptoms, diagnoses, and procedures. These surveys are nationally representative, provider-based, and cover a broad spectrum of healthcare settings. Within each setting, data are collected from a sample of organizations that provide care and from samples of patient (or discharge) encounters within the sampled organizations. Data are collected not only from traditional healthcare settings such as hospitals and physicians' offices, but also from long-term care providers and community health centers. These surveys help provide insight to inform policy, research, and quality; sending them electronically allows for wider representation from hospitals and healthcare organizations, as well as reduces manual burden on the reporters.[112] Improving the process for electronic collection of survey data, including the use of standards, could make these important surveys easier to administer.

We propose minimal changes to the certification criterion in § 170.315(f)(7), specifically, revising to reference the standard in § 170.205(s) instead of the current reference to § 170.205(s)(1). We then propose to add an expiration date of January 1, 2027, to the standard for healthcare survey information for electronic transmission specified in § 170.205(s)(1). We also propose to revise § 170.205(s)(2), which is currently reserved, to reference HL7 CDA R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1—US Realm and incorporate it by reference in § 170.299. To advance the electronic transmission of healthcare surveys and include the relevant and needed information to achieve its intent, we propose this version of the standard, as it includes new and updated templates with important context. These revisions include, but are not limited to, changes to sections for emergency department encounters, patient information sections, gender identity observation, and number of visits over the past 12 months. Such information will provide additional insight on trends in hospitalization, surveillance of symptomology and diagnoses, and demographics that can highlight disparities and better inform interventions.

We are aware that the HL7 FHIR Health Care Surveys Content Implementation Guide has gone through the HL7 approval process and was published in 2023. We are further aware that a FHIR pilot project for using FHIR standards to send survey information was initiated in fall of 2023. We have not proposed to include this newer, FHIR-based standard for healthcare survey information at this time, but request feedback on whether it should be an option for health care surveys. Specifically, we request comment on whether we should consider modifying the certification criterion to require a Health IT Module certified to this criterion to support creation and submission using at least one of these standards:

- The HL7 FHIR Health Care Surveys Content IG; or,
- The HL7 CDA R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1—US Realm.

Under this alternative, a Health IT Module certified to this criterion would be required to support at least one of these kinds of standards but would not be precluded from supporting both. We welcome comment on this proposal—in particular, on current usability and maturity of the FHIR IG and readiness among certified health IT vendors to implement it.

We also propose minimal changes to the name of this certification criterion in § 170.315(f)(7) to be ''health care surveys—transmission to public health agencies.'' We welcome comment on this proposal, including on FHIR-based approaches.

e. New Certification Criteria for Health IT Modules Supporting Public Health Data Exchange

We propose to establish new certification criteria as described below for Health IT Modules supporting public health data exchange. These certification criteria would certify the ability of Health IT Modules to receive HL7 v2, CDA-based, and/or FHIR reports for birth reporting and Prescription Drug Monitoring Programs (PDMPs). Additionally, certification criteria proposed in this section would certify receive, validate, parse, and filter capabilities related to immunization information, syndromic surveillance, cancer pathology reports, electronic case reporting, birth reporting, and PDMP data.

i. § 170.315(f)(8)—Birth Reporting—Transmission to Public Health Agencies

Providers currently rely on manual and duplicative data entry processes to report information on live births to state vital records offices. With most U.S. births occurring in hospitals or free-standing birthing facilities, birth reporting typically entails clinicians supplying the medical and health information for the birth certificate to a

[112] *https://www.cdc.gov/nchs/dhcs/index.htm?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fnchs%2Fdhcs.htm.*

state web-based Electronic Birth Registration System (EBRS) or nonclinical hospital staff reviewing the hospital medical records for the information and entering it into the state EBRS. The legal and demographic information is typically collected directly from the mother using a standardized worksheet, and the information is then entered into the State EBRS by nonclinical hospital staff. This information is then sent to the state and a birth certificate is then issued by the state vital records authority. Much of the medical and health information collected for the birth certificate necessary to report a live birth is also dually entered into EHRs by health care providers. As a result, birth reporting processes are duplicative and burdensome for providers and hospital systems.

Low adoption of standards to exchange data between EHRs and EBRSs have resulted in an overall lack of interoperability between all systems involved in birth reporting processes. CDC has provided significant funding and resources to support the adoption of EBRSs by PHAs and providers. Recent funding has also been provided to PHAs to develop and advance the use of the FHIR standard to report information. Despite investments made by CDC towards standards-based exchange with EBRSs, there has been very little uptake of these standards and associated functionalities by health IT developers.

We propose to adopt a new certification criterion, ''Birth reporting—Transmission to public health agencies.'' As a part of this new certification criterion, we propose to adopt the HL7 FHIR Vital Records Birth and Fetal Death Reporting–1.1.0—STU 1.1 in § 170.205(v) for electronically submitting medical and health information from birth certificate reports to PHAs.[113] However, if an updated version of this IG is published prior to the publication of a final rule, and made available to the public, it would be our intent to consider adopting the updated IG if it best aligns with and supports effective implementation of this proposed certification criterion. Based on public comments on HTI–1 and prior rulemakings, we believe that the health IT industry, healthcare standards developers, and health care providers expect and support ONC making such determinations so that the adopted version of standards are the most up-to-date available and are feasible for real-world implementation (see 89 FR 1215). We encourage commenters to comment on the preferred version associated with this proposal.

Additionally, we request comment specifically on whether the content specified in the IG can be exchanged using transport mechanisms defined in § 170.315(g)(10) and in the proposed § 170.315(g)(20) certification criteria. The selected information included in the standard in § 170.205(v) was piloted by the Michigan Health and Human Services Division for Vital Records and Health Statistics with four Michigan hospitals and their EHRs. In Michigan, the pilot has found increased data completion and accuracy for many data items when births are reported using the FHIR standard and a SMART-on-FHIR app when compared to reports completed manually by hospital staff.[114] We believe the standard, when adopted broadly, could aid in timely, more complete, and accurate reporting from hospitals with reduced burden on the reporting facilities. We seek comment from those who have implemented and used the IG on its readiness for nationwide adoption.

As an alternative to the IG proposed above, we propose, and seek comment on, adoption of an interim standards-agnostic functional criterion for electronically transmitting medical and health information from birth certificate reports to PHAs based on the data elements outlined in CDC National Vital Statistics System's ''Guide to Completing the Facility Worksheets for the Certificate of a Live Birth and Report of Fetal Death.'' [115] We further seek comment on the potential benefits and risks of adopting a functional approach, particularly as CDC's NCHS has retired and will not be actively updating the HL7 Version 2.6 Implementation Guide: Vital Records Birth and Fetal Death Reporting, Release 1 STU Release 2 and the HL7 CDA R2 Implementation Guide: Birth and Fetal Death Reporting, Release 1, STU Release 2—U.S. Realm standards. Finally, we request comment on whether a functional approach—if adopted—should be time-limited and require a transition to a standards-based approach as of a specific timeline. For example, a functional approach could be permitted for certification up to and including December 31, 2026, and then the standards-based approach for conformance would be required thereafter.

ii. § 170.315(f)(9)—Prescription Drug Monitoring Program (PDMP) Databases—Query, Receive, Validate, Parse, and Filter

We propose to adopt a new certification criterion to enable the bi-directional interaction and electronic data exchange between Health IT Modules and PDMP databases (referred to hereafter as PDMPs). Specifically, we propose a certification criterion to enable the query of prescription drug monitoring systems and the receipt, validation, parsing, and filtering of medication information from PDMPs. This aligns with a current requirement in CMS' Medicare Promoting Interoperability Program where Query of PDMP is a required measure.

PDMP Background

ONC has engaged in collaborative work to understand health IT's role in addressing the opioid crisis, including the opportunities created by state-run health IT systems known as PDMPs.[116] PDMPs are state-run electronic databases that provide critical health information to physicians and other health care providers about an individual's history of controlled substance prescriptions (and, in some states, more complete histories of all prescriptions). Evaluations of PDMPs suggest their use supports changes in prescribing behaviors, reduces use of multiple providers by patients, and decreases treatment admissions associated with substance misuse.[117]

Beginning in 2012, ONC, in collaboration with the Substance Abuse and Mental Health Services Administration (SAMHSA), sought to identify ways to use health IT to improve access to PDMPs. The collaborative project resulted in the development of the ''Enhancing Access to Prescription Drug Monitoring Programs Using Health Information Technology: Work Group Recommendations Report,'' [118] and 13 pilot studies to test the feasibility of connecting PDMPs with health IT systems.[119]

Bipartisan legislation aimed to address the opioid crisis—the 21st Century Cures Act (Cures Act) of 2016

[113] Please *see https://hl7.org/fhir/us/bfdr/2024Jan/.*

[114] Final Report submitted to Centers for Disease Control and Prevention In response to Request for Task Order Proposal No. (MI 2020–Q–45799), June 16, 2023.

[115] *https://www.cdc.gov/nchs/nvss/facility-worksheets-guide.htm.*

[116] *See* for reference: *https://www.healthit.gov/sites/default/files/page/2023-03/LPASO_Landscape_Assessment_508.pdf.*

[117] *See* for reference: *https://www.cdc.gov/drugoverdose/pdmp/index.html.*

[118] Enhancing Access to Prescription Drug Monitoring Programs Using Health Information Technology. (2012). *https://www.healthit.gov/sites/default/files/work_group_document_integrated_paper_final_0.pdf; see also https://www.cdc.gov/drugoverdose/pdf/pehriie_report-a.pdf.*

[119] *https://www.healthit.gov/topic/health-it-health-care-settings/enhancing-access-pilot-reports.*

(Pub. L. 114–255),[120] and the Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (SUPPORT Act) of 2018 (Pub. L. 115–271).[121] Additionally, the Commission on Combating Drug Addiction and the Opioid Crisis (Commission) was established in 2017 [122] to develop recommendations to address the opioid epidemic. In November 2017, the Commission released a final report with recommendations focused on reducing barriers and supporting programs and innovations aimed at strengthening Federal, state, and local responses to the opioid overdose epidemic.[123] Several of the report's recommendations include the use of state-run programs and health IT to address substance use disorder (SUD) and opioid use disorder (OUD).

These laws included important provisions related to PDMPs, health IT supports for OUD, and the integration of health IT supports into clinical workflows for OUD prevention and treatment. Section 1944(b) of the Social Security Act, as added by Section 5042(a) of the SUPPORT Act, also requires that states implement a qualified PDMP and defines the requirements for a qualified PDMP including that the PDMP administered by the state, at a minimum: [124]

- Facilitates access by a covered provider with respect to a covered individual—in as close to real time as possible—of patient-specific information for prescription drug history with regard to controlled substances, the number and type of controlled substances prescribed and filled in at least the most recent 12-month period, and information relating to each covered provider of such medications; and
- Facilitates the integration of the information into the workflow of a covered provider, which may include the electronic system the covered provider uses to prescribe controlled substances.

In addition, Section 1944(a) of the Social Security Act, as added by Section 5042(a) of the SUPPORT Act, directs states to implement requirements that certain covered Medicaid Providers check the qualified PDMP for Medicaid beneficiaries' prescription information prior to prescribing applicable controlled substances.[125]

The establishment and operation of PDMPs vary given that each PDMP is subject to existing policies and management of their own respective state. While PDMPs may operate differently, there are system components guidance that CDC promotes to improve PDMP functionality as a public health tool.[126] Those include:

- Universal use among clinicians and/or their delegates (for example, nurse practitioners or physician assistants) within a state;
- More timely or real-time data contained within a PDMP;
- Actively managing the PDMP in part by sending proactive reports to clinicians to inform prescribing; and
- Ensuring that PDMPs are easy to use and accessible by clinicians.

As of the publication of this proposed rule, 50 states, the District of Columbia, and three territories have established PDMPs, each with various requirements for querying and reporting from pharmacy information systems. Of these 54 PDMPs, 51 have additionally implemented regulations mandating the use of the state PDMP when prescribing controlled substances, sometimes for new patients or other scenarios.[127] However, despite the increase in PDMP utilization and promising, though mixed, evidence of their effectiveness, PDMPs are only able to truly impact care if prescribers and pharmacists use them, and when PDMP data are easily accessible in clinical workflows and accessible across state lines. While requirements are in place for providers to access PDMPs at the state level, states generally do not have specific requirements for PDMPs to support direct queries—in practice this leads to indirect query workflows and multiple translation points, creating gaps in interoperability. Additionally, there are no widespread established practices for integrating query information into clinical workflows within health IT systems—despite recommendations from CDC that, when prescribing initial opioid therapy for acute, subacute, or chronic pain, clinicians should review a patient's history of controlled substance prescriptions as well as non-opioid therapies using state PDMP data.[128] In addition, health IT systems may lack sufficient capabilities to reconcile query data from PDMP systems as discrete data element(s). At the same time, PDMPs also need to be able to respond to a query from a certified Health IT Module with discrete data.

Today, authorized users may have to access PDMP data that is not integrated into their workflow, as it is accessed through a separate portal, which may add to clinical burden and decrease the likelihood of checking and utilizing the PDMP data.[129] These pieces—integrating query information into health IT systems and informing workflow integration practices based on established guidelines, along with reconciling query data as discrete data elements for both the PDMP and certified Health IT Module—are supported by the functions we propose below.

From 2018 to 2022, ONC and CDC collaborated on the Advancing PDMP and EHR Integration project. The purpose of this project was to advance and scale vendor agnostic PDMP integrations with health IT systems in a variety of hospital, primary care, and outpatient settings. This effort produced an Integration Framework and Integration Toolkit to serve as technical resources for organizations interested in integrating PDMP with a variety of health IT systems.[130] The Integration Framework includes how best to implement advanced technologies such as electronic CDS systems that clinicians are increasingly using to combat the opioid crisis as well as information to help improve integration of state PDMPs within clinicians' workflows. The Integration Framework

[120] 21st Century Cures Act. (2016). *https://www.gov info.gov/content/pkg/PLAW-114publ255/pdf/PLAW-114publ255.pdf.*

[121] Substance Use–Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act. (2018). *https://www.congress.gov/bill/115th-congress/house-bill/6/text.*

[122] The White House. (2017). *https://trumpwhitehouse.archives.gov/presidential-actions/president-donald-j-trump-signs-executive-order-establishing-presidents-commission-combating-drug-addiction-opioid-crisis/.*

[123] The Commission on Combating Drug Addiction and the Opioid Crisis. (2017). *https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Final_Report_Draft_11-15-2017.pdf.*

[124] Section 1944(b) of the Social Security Act [42 U.S.C. 1396w–3a] as added by section 5042(a) of the Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (SUPPORT Act) of 2018 (Pub. L. 115–271).

[125] Section 1944(a) of the Social Security Act [42 U.S.C. 1396w–3a] as added by section 5042(a) of the SUPPORT Act of 2018 (Pub. L. 115–271). *See also https://www.medicaid.gov/federal-policy-guidance/downloads/faq051519.pdf.*

[126] CDC Clinical Practice Guidelines for Prescribing Opioids (Dowell D, Ragan KR, Jones CM, Baldwin GT, Chou R. CDC Clinical Practice Guideline for Prescribing Opioids for Pain—United States, 2022. MMWR Recomm Rep 2022;71(No. RR–3):1–95. DOI:*http://dx.doi.org/10.15585/mmwr.rr7103a1*).

[127] *https://www.medicaid.gov/medicaid/data-and-systems/downloads/rtc-5042-state-challenges.pdf.*

[128] CDC Clinical Practice Guideline for Prescribing Opioids for Pain—United States, 2022 | MMWR.

[129] *https://www.healthit.gov/sites/default/files/page/2023-03/LPASO_Landscape_Assessment_508.pdf.*

[130] HHS ONC/CDC Health Information Technology: Integration Framework for PDMP–EHR Integration: June, 2021: *https://www.cdc.gov/opioids/pdf/Integration-Framework.pdf.*

also includes helpful resources, such as MOU, auditing, and testing guidance, which can help advance and scale PDMP integration with health IT systems (*e.g.,* EHR systems, health information exchanges, and pharmacy systems) in a variety of hospital, primary care, and outpatient settings.[131]

In 2018, CMS issued frequently asked questions outlining how a state could ensure that its qualified PDMP aligns with and incorporates industry standards, consistent with 42 CFR 433.112(b)(12), and encouraged states to refer to the information on standards in the Interoperability Standards Advisory (ISA) published by the ONC, specifically the section of the ISA describing, ''A Prescriber's Ability to Obtain a Patient's Medication History from a Prescription Drug Monitoring Program,'' which outlined recommended industry standards for PDMP and EHR integration informed by the efforts of ONC and CDC to advance PDMP best practices.[132]

The 2022 CDC Clinical Practice Guideline for Prescribing Opioids for Pain [133] (2022 Clinical Practice Guideline) includes information that updates and replaces the 2016 CDC Guideline for Prescribing Opioids for Chronic Pain. The 2022 Clinical Practice Guideline provides evidence-based recommendations for prescribing opioid pain medication for acute, subacute, and chronic pain for outpatients aged 18 years or older, excluding pain management related to sickle cell disease, cancer-related pain treatment, palliative care, and end-of-life care. The 2022 Clinical Practice Guideline takes into account new science and data, along with lessons learned about the challenges faced by patients managing pain and pain care. The 2022 Clinical Practice Guideline also includes a key update that specifies which recommendations apply to patients who are being considered for *initial* treatment with prescription opioids versus those that have *already been receiving* opioids as part of ongoing care.

In March of 2023, ONC published a report from the *Leveraging PDMPs and Health IT for Addressing SUD/OUD (LPASO)* Project landscape assessment. The LPASO Project was originally established in 2018 to examine how jurisdictions utilize PDMPs and health IT to support SUD/OUD identification, prevention, and treatment. Specifically, ONC was interested in identifying and describing the policy and technical approaches to addressing the opioid overdose epidemic related to PDMPs for several key characteristics termed ''indicators'' (bolded for emphasis).[134] The PDMP indicators included in this analysis were:

- *PDMP data placement in health IT systems:* State statutes and policies that allow PDMP data to be stored in another system such as the EHR (*e.g.,* included in provider notes, medication history, etc.) as compared to a one-time view of the PDMP data.
- *Interpretation of PDMP data:* State statutes and policies related to the use of PDMP data for predictive analytics such as risk scores.
- *PDMP access roles:* Categories of professionals who are authorized by state statute or other policies to access PDMP data.
- *PDMP hospital integration:* Prevalence of PDMP integration within the clinical workflow. This indicator examined whether hospitals provided access to the PDMP within the hospital's EHR system or outside of the hospital's EHR system via a PDMP portal or secure website.
- *Data standards and hubs used for PDMP data capture, exchange, and reporting:* Health IT components and data standards in use for the transport, interpretation, and integration of PDMP data including those used for interstate data sharing.

The LPASO report presented the findings of the landscape analysis for each of these indicators, which is summarized below. The LPASO Project identified that where state law permitted the care team access to the PDMP data within a medical record and to incorporate the data as a discrete data element—as opposed to view only access—clinicians are better able to coordinate care, to assess prescribing practices across the organization, and to implement OUD prevention and treatment best practices.[135] Further, the LPASO Project found that clinical decision support tools can help clinicians across a wide range of specialties to better identify at-risk patients and facilitate best practices for OUD prevention and treatment. However, some clinicians have expressed concern at the potential risk of such analytics tools including variations in threshold values, lack of transparency for algorithms, and the potential for scores to over-simplify risk that could be identified with a more detailed review of PDMP data.[136] The LPASO report also found that the content received in response to a PDMP query varied in terms of clinical usefulness and, after querying, receiving a risk score based on a proprietary algorithm was of limited utility and inconsistently predictive of negative outcomes.[137] Additionally, state laws and regulations determine the categories of users who are authorized to access and use a state's PDMP data, and there is considerable variability in the number and types of access roles identified in each state. A 2018 analysis of the PDMP Training and Technical Assistance Center's (TTAC) data revealed that there are 63 unique access roles identified across all states and jurisdictions. This analysis indicated:

- In all states and jurisdictions, prescribers and pharmacists are allowed access to the PDMP.
- A majority of states and jurisdictions (more than 50) also allow access for law enforcement, physician assistants, nurse practitioners, and prescriber delegates.
- A majority of states and jurisdictions (more than 40) also include an access role for ''patient.'' [138]

The Prescription Monitoring Information Exchange (PMIX) Healthcare Roles document was developed by the PDMP Training and Technical Assistance Center (PDMP–TTAC) to provide states with a resource to assist in defining a harmonized set of healthcare access roles for PDMP data. The PDMP hospital integration indicator examined whether hospitals provided access to the PDMP within the hospital's EHR system or outside of the hospital's EHR system via a PDMP portal or secure website. In the assessment, less than half of hospitals reported integration of PDMP checks within their EHR workflows. In addition, the variability of tools used to exchange, store, and report PDMP data contributed to the complexity of PDMP

[131] ''Using Health IT Integration to Address the Drug Overdose Crisis'' August 2022: *https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/using-health-it-integration-to-address-the-drug-overdose-crisis.*

[132] *https://www.medicaid.gov/federal-policy-guidance/downloads/faq051519.pdf.*

[133] CDC Clinical Practice Guideline for Prescribing Opioids for Pain—United States, 2022 *https://www.cdc.gov/mmwr/volumes/71/rr/rr7103a1.htm.*

[134] Leveraging Prescription Drug Monitoring Programs and Health Information Technology for Addressing Substance Use Disorder and Opioid Use Disorder: A Landscape Assessment of Prescription Drug Monitoring Programs and Health Information Technology Indicators—March 2023: *https://www.healthit.gov/sites/default/files/page/2023-03/LPASO_Landscape_Assessment_508.pdf.*

[135] *Ibid.*

[136] Call for better validation of opioid overdose risk algorithms | Journal of the American Medical Informatics Association | Oxford Academic (*oup.com*).

[137] *https://pubmed.ncbi.nlm.nih.gov/31356498/.*

[138] Prescription Drug Monitoring Program Training and Technical Assistance Center. (2018). *http://www.pdmpassist.org/content/state-profiles.*

ecosystems.[139] Finally, the LPASO report analyzed several standards that today support PDMP data exchange workflows, including the American Society for Automation in Pharmacy (ASAP) and Prescription Monitoring Information Exchange (PMIX) standards.[140] These standards, and additional standards for electronic prescribing of controlled substances (EPCS) (such as those referenced for the certification criterion in § 170.315(b)(3)), support specific capabilities that are individually well suited to the task for which they were designed. However, they are not all directly harmonized, which creates challenges when data are moving from one system and one standard to another—for example from the standard transmitted by the clinician to the pharmacy and from the pharmacy to the PDMP. The request/response messages have the same information regardless of the standards in use, but the standards have different naming conventions for the message data, making it necessary to translate requests and responses to enable seamless communication across systems.

The applicable standards for the different parts of PDMP workflows are widely adopted to support pharmacy dispense reporting and interstate exchange, but further work in industry is necessary to align current standards with open, consensus-based standards, and specifically with HL7 FHIR.[141] The HL7 US Meds PDMP FHIR Implementation Guide is intended to define how an EHR or an app or other clinical system can access a patient's controlled substance prescription history from the State PDMP systems. This IG holds promise to advance health IT supports for PDMPs in a more interoperable manner including through new API-enabled transactions, which may also reduce the current translation challenges. However, the IG is based on the HL7 FHIR Release 3, and significant work is needed to advance, ballot, and test a version of the IG that is consistent with API standards adopted in 45 CFR 170.215.

While HL7 FHIR-based standards for PDMP exchange are developing and maturing, we propose to adopt functional requirements for exchanging data with PDMPs to make certain that applicable health IT can support capabilities required to engage with a PDMP meeting the requirements under Section 1944(b) of the Social Security Act, as added by Section 5042(a) of the SUPPORT Act.[142] These capabilities include enabling health IT systems to support integration of query into clinical workflows and to support requirements for the capability to reconcile queried data as discrete data elements (not just as read only). These requirements are also intended to enable the PDMP to respond to a query from a certified Health IT Module with discrete data. As described previously, Section 1944(b) of the Social Security Act defines specific capabilities for a PDMP to be considered a ''Qualified PDMP'' [143] and there are capabilities that Health IT Modules could support, agnostic to a specific standard, that would be of value to enable engagement with a Qualified PDMP:

- Enabling a user to query controlled substance prescription history from their state PDMP for a specific patient.
- Enabling a user to receive a response to their PDMP queries containing patient-specific controlled substance prescribed and dispensed prescription data.
- Supporting that all transactions can be sent and received from within electronic prescribing or EPCS workflows.

In order to support clinical and public health programs targeting the prevention and treatment of SUD/OUD, there are additional capabilities that Health IT Modules could support, agnostic to a specific standard, that would be of value. These include considerations of what should be a part of the PDMP (*e.g.,* interstate query) as well as related to the PDMP indicators data placement, interpretation, access roles, and integration into clinical workflows. Based on the findings of the LPASO report for each PDMP indicator, public forums with clinical and behavioral health care providers, and the 2022 Clinical Practice Guideline recommendations, these capabilities include:

- Enabling a user to query controlled substance prescription history from another state's PDMP for a specific patient.
- Enabling a user to receive a response to their interstate PDMP queries containing patient-specific controlled substance prescribed and dispensed prescription data.
- Enabling a user to validate, parse, and filter the PDMP data included in the responses received as discrete data elements—including to reconcile the data into a patient's medication list.
- Enabling access roles for clinicians and pharmacists, and with additional capabilities to create and allow customized access roles for any delegate or surrogate under applicable law such as physician assistants, nurse practitioners, and clinician delegates.
- Enabling an audit log of PDMP access.
- Enabling the use of clinical decision support tools that support clinical prescribing guideline recommendations such as those described in the 2022 Clinical Practice Guideline.
- Enabling automated or passive queries for specific common workflows consistent with state requirements and best practice guidelines
- Enabling implementation of the capabilities within other applicable workflows—such as administrative or transition of care workflows—consistent with SUD/OUD prevention and treatment best practice guidelines.

Given the current state of PDMP data exchange, we believe it is not yet feasible to adopt certification criteria leveraging the individual standards that currently support PDMP data exchange workflows. While standards developing organizations (SDOs) continue to work toward open API-enabled solutions for PDMPs, continued commitment and development effort is needed to advance FHIR-based implementation specifications to achieve readiness for widespread adoption and use.

In the interim, we believe inclusion of a functional criterion within the Program may help to advance systems to support the capabilities described in the SUPPORT Act [144] and implement recommendations and best practices per the 2022 Clinical Practice Guideline (*i.e.,* Recommendation 9 to check PDMPs) as well as addressing the impact factors identified in the LPASO report. Therefore, we propose to adopt a new certification criterion to improve interoperability between health IT and PDMPs. Specifically, we propose a new certification criterion in § 170.315(f)(9) entitled ''Prescription Drug Monitoring Program (PDMP) Databases—Query, receive, validate, parse, and filter.'' We propose that this criterion would be a functional criterion agnostic to a specific PDMP standard, but would include transport, content, and vocabulary standards where appropriate. We additionally propose to include functional requirements for

[139] LPASO—fix citation.

[140] *https://www.healthit.gov/isa/allows-exchange-state-prescription-drug-monitoring-program-pdmp-data.*

[141] HL7 ''US Meds Prescription Drug Monitoring Program (PDMP) FHIR Implementation Guide'': *http://hl7.org/fhir/us/meds/pdmp.html.*

[142] Section 1944(b) of the Social Security Act [42 U.S.C. 1396w–3a] as added by section 5042(a) of the Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (SUPPORT Act) of 2018 (Pub. L. 115–271).

[143] *Ibid.*

[144] *Ibid.*

access controls including access roles and audit logs within this new criterion.

We propose requirements in § 170.315(f)(9) to enable a user to query a PDMP, including bi-directional interstate exchange, to receive PDMP data in an interoperable manner, to establish access roles in accordance with applicable law, and to maintain records of access and auditable events.

We propose requirements in § 170.315(f)(9)(i) to enable both passive and active bi-directional query of a PDMP, including an interstate exchange query, and send an acknowledgement message in response to receipt of data after a query is performed. We propose requirements in § 170.315(f)(9)(i)(A) to initiate a passive or automated query upon the recording, change, or access of a medication order; upon the creation and transmission of an electronic prescription for a controlled substance; and upon entry of controlled substance medication data into a medication list or reconciliation of a medication list including controlled substance medication data. We also propose requirements in § 170.315(f)(9)(i)(B) to enable an active or user-initiated query of a PDMP including an interstate exchange query. In § 170.315(f)(9)(i)(C), we propose to send an acknowledgement message in response to receipt of data after a query is performed.

We propose requirements in § 170.315(f)(9)(ii) to enable a user to receive, validate, parse, and filter electronic PDMP information. We propose requirements in § 170.315(f)(9)(ii)(A) to enable a user to receive electronic controlled substance medication prescription transmitted through a method that conforms to the standard in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2); through a method that conforms to the standard in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol; and via an application programming interface in accordance with the standard specified in § 170.215(a)(1). We propose an optional capability to enable a user to receive electronic PDMP information governed by Trusted Exchange Framework and Common Agreement (TEFCA). In other words, that the Health IT Module is connected via the network enabled by TEFCA and can demonstrate that it can exchange data using it.

We propose requirements in § 170.315(f)(9)(ii)(B) to demonstrate the ability to detect valid and invalid electronic controlled substance medication prescription received. We propose requirements that a Health IT Module certified to this certification criterion include the capability to identify valid electronic controlled substance medication prescription received and process the data elements including any necessary data mapping to at least one of the versions of the USCDI standard in § 170.213 to enable use as discrete data elements, aggregation with other data, incorporation into a patient medication list, and parsing and filtering in accordance with the requirement proposed in § 170.315(f)(9)(ii)(C) described below. We also propose requirements that a Health IT Module certified to this certification criterion include the capability to: correctly interpret empty sections and null combinations; detect errors in electronic controlled substance medication prescription received, including invalid vocabulary standards and data not represented using a vocabulary standard; and record errors encountered and allow a user through at least one method to be notified of the errors produced, review the errors produced, and store or maintain error records for audit or other follow up action.

We propose requirements in § 170.315(f)(9)(ii)(C) to enable a user to parse and filter electronic PDMP information received and validated in accordance with paragraph § 170.315(f)(9)(ii)(B) at a minimum for any data element identified in at least one of the versions of the USCDI standard in § 170.213.

We propose requirements in § 170.315(f)(9)(iii) to enable access controls. This includes enabling access roles and recording access, including actions for auditable events and tamper-resistance. We propose requirements in § 170.315(f)(9)(iii)(A) to enable access roles for clinicians and pharmacists and to enable a user to customize additional roles for any delegate or surrogate under applicable law. Additionally, we propose requirements in § 170.315(f)(9)(iii)(B) to record access actions and maintain an audit log of actions.

We note that in our proposed certification criterion, we describe a passive or automated query as well as an active query. A passive or automated query is a query initiated by the system when another related action occurs—for example, a system automatically initiates a query on behalf of the clinician when the clinician uses an electronic prescribing module to send a prescription for a controlled substance. In such a case, the system may be configured to pair with a certified or non-certified Health IT Module that enables the EPCS in order to initiate the query without additional action by the clinician. An active query refers to a query of the PDMP initiated by the user to specifically query the PDMP based on their own clinical considerations. An active query might also be in conjunction with other clinical actions, but it should also enable the user to elect to initiate a query as part of other workflows such as administrative or care coordination actions. We welcome public comment on the inclusion of these query types, as well as the specific functions for which a passive query is required.

In addition, we note the inclusion of audit requirements and reference to auditable events. We propose that auditable events would include the same functions previously adopted for § 170.315(d)(2), (3), and (10). We note these include referenced standards in § 170.210(e) and (h). However, we have not proposed to specifically adopt auditable event or audit and disclosure log standards for the proposed certification criterion in § 170.315(f)(9) because the specific audit requirements vary across states, access roles, and use cases. However, we seek comment on the potential applicability of such standards for the proposed PDMP data certification criterion.

We welcome public comment on this proposal. In addition, we seek public comment specifically on the following areas:

- Should ONC consider additional functional requirements, or additional constraints on functional requirements, relating to the passive or automated query of a PDMP within EPCS or CPOE workflows?
- Should ONC consider either additional or reduced specificity within the minimum functions supporting receipt of the PDMP information as discrete data elements?
- Should ONC further specify or further constrain access roles? For example, should ONC consider adding a ''patient'' access role to the requirements? What access roles would be most beneficial to define more clearly in any final rule or supportive sub-regulatory guidelines? [145]
- Are there additional functional capabilities that would support effective SUD/OUD prevention and treatment that should be considered for a future version of the proposed certification criterion?

We additionally refer readers to section III.B.13.e.ix describing a new

[145] *See,* for example, access roles described in the LPASO report, March 2023 at: *https://www.healthit.gov/sites/default/files/page/2023-03/LPASO_Landscape_Assessment_508.pdf.*

proposed certification criterion in § 170.315(f)(29) that relates to this proposed certification criterion in § 170.315(f)(9).

iii. § 170.315(f)(21) Immunization Information—Receive, Validate, Parse, Filter, and Exchange—Response

Immunization reporting is a vital component of public health data, and is used by all 50 states, Washington DC, Puerto Rico, and many large local jurisdictions. States that have immunization information systems (IIS) consolidate immunization histories and exchange information with vaccination providers, with the goals of improving vaccination rates and reducing vaccine-preventable diseases. In order to achieve the stated goals of immunization information exchange, PHAs must have the technology in place to perform corresponding functions to certified health IT and receive the same standard included in § 170.315(f)(1).

We propose to adopt a new certification criterion for health IT for public health that would focus on immunization information—receipt, validation, parsing, and filtering—adhering to the same standard as required in § 170.315(f)(1). We further propose a requirement for responding to queries from external systems, as well as seek comment on patient access as a complement to the proposed updated requirements in § 170.315(f)(1). Such updates will provide clinicians with querying access to IISs in order to better determine the vaccination status of their patients, among other benefits. By including functions performed by health IT for public health within a certification criterion, the Program advances its focus on bi-directional interoperability between healthcare and PHAs. Such functionality for receipt, validation, query/response, and patient access should enable more users, including those using a variety of health IT systems, to have the most complete and accurate vaccine history for individuals. This functionality can help advance EHRs, IISs, and intermediaries in alignment, with the same foundational functionalities, and keep data moving with the speed of care. If an individual receives a vaccine from a pharmacy, from a community health clinic, away from their home state, or at their provider's office, any approved user regardless of their health IT should be able to have access to their complete, accurate vaccine history. We believe these proposed requirements, coupled with the proposed § 170.315(g)(20) and updates to § 170.315(f)(1), can move the nation closer to this ideal state.

These new capabilities include: receive, validate, parse, and filter incoming data in accordance with at least one of the versions of the standard and applicable implementation specification specified in § 170.205(e); transmission of immunization information electronically in accordance with at least one of the versions of the standard and applicable implementation specification in § 170.205(e); and technical capability to respond to incoming patient-level and/or immunization-specific queries from external systems. We request feedback on the functional requirement to respond to patient-level, immunization-specific queries from external systems and request comment on if the standard referenced in § 170.205(e) is sufficient for the proposed functional requirement to respond to incoming patient-level and immunization-specific queries. We seek comment on if we should also require health IT for public health to share immunization information on a population of patients using the standard specified in § 170.315(g)(20)(ii) in our proposals in section III.B.16, and whether health IT for public health should also be able to support patient access using SMART Health Cards for Immunization Criteria according to § 170.315(j)(22). We specifically request comment on readiness and feasible timelines for these capabilities.

Additionally, we recognize that due to the work and collaboration of state immunization programs, IIS vendors, CDC's National Center for Immunization and Respiratory Diseases (NCIRD), and the American Immunization Registry Association (AIRA), immunization systems can do much of what is described above already. Through these NCIRD sponsored and established programmatic requirements and optional testing programs conducted by AIRA, many IISs already meet most of, if not all, of the requirements in the proposed certification criterion. We applaud the work done already, and the intent of our proposal is to ground the certification requirements in what already exists without additional burden or cost for IISs that already participate in the NCIRD requirements. However, we know it is important to codify these functional requirements in the Program to demonstrate the success of modern approaches to data exchange and clinician access to data, and to create a shared floor of functionality for all health IT contributing to immunization information sharing.

We propose requirements in § 170.315(f)(21) to enable health IT for public health to receive, validate, parse, and filter electronic immunization information. We also propose requirements in § 170.315(f)(21) to enable health IT for public health to exchange immunization information. These proposed requirements are described below.

We propose requirements in § 170.315(f)(21)(i) to enable health IT for public health to receive electronic immunization information transmitted through a method that conforms to Simple Object Access Protocol (SOAP)-based transport. Optionally, to meet the received requirements, a developer (serving as a Participant or Subparticipant of a Qualified Health Information Network™ (QHIN™), or who is a QHIN) may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement, receipt through a method that conforms to the standard specified in § 170.205(p)(1) when the technology is also using an Simple Mail Transfer Protocol (SMTP)-based edge protocol, or receipt via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

We propose requirements in § 170.315(f)(21)(ii) to demonstrate the ability to detect valid and invalid electronic immunization information received and formatted in accordance with the standards specified in § 170.207(e)(5) and § 170.207(e)(6). In order to meet the validate requirements, the health IT for public health must include the capability to identify valid electronic immunization information received and process the data elements required for the standards specified in § 170.207(e)(5) and § 170.207(e)(6). Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with the parse and filter requirements in the proposed § 170.315(f)(21)(iii). Additionally, in order to meet the validate requirements, the health IT for public health must correctly interpret empty sections and null combinations; detect errors in immunization information received, including invalid vocabulary standards and codes not specified in the standards specified in § 170.207(e)(5) and § 170.207(e)(6); and record errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose that Health IT Modules certified to § 170.315(f)(21)(iii) support users to parse and filter immunization

information received and validated in accordance with validate requirements in the proposed § 170.315(f)(21)(ii) according to the standard specified in § 170.207(e)(5) or § 170.207(e)(6).

We propose functional requirements in § 170.315(f)(21)(iv) to respond to both incoming patient-level and immunization-specific queries from external systems.

We welcome comment on these proposals.

iv. § 170.315(f)(22) Syndromic Surveillance—Receive, Validate, Parse, and Filter

We propose to adopt a new criterion for the functional requirement to receive, validate, parse, and filter incoming syndromic surveillance information in accordance with at least one of the versions of the standards adopted in § 170.205(d) and not expired for the purposes of certification to criteria in § 170.315(f) at the time of certification. As discussed in § 170.315(f)(2), syndromic surveillance information is vital to the monitoring and early detection of potential public health events. Syndromic surveillance data help provide PHAs the information they need to prevent a public health threat from becoming a public health emergency. Further, since these threats do not respect boundaries, the cross-jurisdictional exchange and national awareness of syndromic surveillance data is vital. The transmission of information electronically, according to the standard specified in § 170.205(d), must be accompanied by the ability to receive and validate information according to the same standard in order to facilitate use of the standardized data for analysis and decision-making. Such functions—receipt and validation—are needed to reduce the need for manual effort or manipulation related to data integration and processing, and to allow for the prompt intake and analysis of information. This process also includes the recipients of reported information in the testing of the workflow at data submission, confirming that what is sent is formatted accurately and allows for validation and processing.

Syndromic surveillance has proven to be a highly effective tool for detecting localized trends in outbreaks, and in larger scale monitoring for seasonal illnesses.[146] The National Syndromic Surveillance Program (NSSP) receives data from over 77% of non-Federal emergency departments nationwide as of July 2023, and does so via jurisdictional PHAs, using the standard specified in § 170.205(d). Many of the systems used today for such monitoring also assisted in predicting trends in the COVID–19 pandemic and estimating future spread.[147] The pandemic also raised the importance of certain data elements being included in the standard in order to better assess hot spots and inform response, including travel status, pregnancy status, acuity, and admission information—all of which are reflected in the updated version of the standard specified in § 170.205(d).

We propose to require at least one of the versions of the standards and implementation specifications specified in § 170.205(d) for the receipt, validation, parsing, and filtering of incoming syndromic surveillance information. We note that given the widespread implementation of syndromic surveillance, most jurisdictions have technology that can already fulfill many of the proposed requirements. However, we believe that adopting this certification criterion for health IT for public health will reinforce the importance of a foundational functionality requirement for all syndromic surveillance systems to be able to validate and assess incoming information quickly to identify emerging threats. While receipt is a function that most syndromic surveillance systems can accomplish today, our proposal to certify this functionality for health IT for public health would allow for several additional benefits. First, it would include both sending and receiving systems in testing the shared standard, finding issues, and aligning on how to constrain specifications to limit variability. Second, it would advance syndromic surveillance technology on the same path as the systems reporting data to them, to allow all involved systems to grow and align when it comes to data exchange—eliminating the need for manual workarounds or costly third parties to fill the gaps between functionalities. Third, the coordination between sending and receiving systems would compel nationwide upgrades and transitions as public health needs and use cases evolve and shift.

We propose that consistent with at least one of the versions of the standards and implementation specifications specified in § 170.205(d), Health IT Modules certified to § 170.315(f)(22) enable a user to receive, validate, parse and filter electronic syndrome-based public health surveillance information in accordance with the proposed § 170.315(f)(22)(i) through (iii).

Specifically, we propose to require Health IT Modules certified to § 170.315(f)(22)(i) to receive electronic syndrome-based public health surveillance information transmitted through a method that conforms to a Secure File Transfer Protocol (SFTP) connection. SFTP is designed for securely moving large volumes of data, and syndromic surveillance reporting involves moving thousands of HL7 messages in a single batch. Even though this protocol does not function in real-time, unlike modern application programming interface (API)-based exchanges, and introduces the possibility of human error, this is the preferred protocol in use by NSSP for transport today and is also a key protocol supported by the current CDC architecture. Optionally, to meet the receive requirements, a developer (serving as a Participant or Subparticipant of a QHIN, or who is a QHIN) may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement or receipt via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

We propose in § 170.315(f)(22)(ii) that Health IT Modules certified to that criterion would demonstrate the ability to detect valid and invalid electronic syndrome-based public health surveillance information received and formatted in accordance with at least one of the versions of the standards specified in § 170.205(d). To meet the validate requirements, a Health IT Module certified to this criterion must include the capability to identify valid syndrome-based public health surveillance information received and process the data elements required for at least one of the versions of the standards specified in § 170.205(d). Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with parse and filter requirements in the proposed § 170.315(f)(22)(iii). A Health IT Module certified to § 170.315(f)(22) must also include the capability to correctly interpret empty sections and null combinations; detect errors in syndrome-based public health surveillance information received, including invalid vocabulary standards and codes not specified in at least one of the versions of the standards specified in § 170.205(d); and, record

[146] Buehler, J.W., Sonricker, A., Paladini, M., Soper, P., & Mostashari, F. (2008). Syndromic surveillance practice in the United States: findings from a survey of state, territorial, and selected local health departments. *Advances in Disease Surveillance, 6*(3), 1–20.

[147] *Ibid.*

errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose that Health IT Modules certified to § 170.315(f)(22)(iii) would need to enable a user to parse and filter electronic syndrome-based public health surveillance information received and validated in accordance with the validate requirements in the proposed § 170.315(f)(22)(ii).

We welcome comment on these proposals.

v. § 170.315(f)(23) Reportable Laboratory Test Values/Results—Receive, Validate, Parse, and Filter

Laboratory-based test results workflow is initiated when a clinician orders a diagnostic test for a patient who presents with symptoms related to a notifiable disease. Laboratory orders are often, but not always, initiated in EHR systems. After the order is placed, the laboratory conducts the test(s) and returns the result(s) to the clinician. The performing laboratory provides the results in various ways, but many laboratories provide the results of the test, ideally electronically, using a Laboratory Information Management Systems (LIMS) or Laboratory Information Systems (LIS). PHAs must also be able to receive the electronically transmitted reportable laboratory test values/results in their system(s) in order to conduct contact tracing, understand disease spread, and have early indications of potential outbreaks.

As described in section III.B.18, we propose a requirement in § 170.315(a)(2) that would require a user of a certified Health IT Module to be able to create and transmit laboratory orders electronically according to the standard specified in § 170.205(g)(2). We additionally propose in section III.B.13.d.iii a requirement in § 170.315(f)(3) to create laboratory tests and values/results for electronic transmission, according to specified standards.

In order to align all of the technical aspects related to reportable lab data across the different public health and health care entities involved, we propose to adopt a certification criterion in § 170.315(f)(23) to require the functionality for Health IT Modules certified to the criterion to be able to receive, validate, parse, and filter incoming reportable laboratory test values/results. By adopting a certification criterion for health IT for public health to receive results and values back electronically (according to national standards), such systems would be able to support delivering more complete patient information to clinicians throughout the laboratory workflow and to PHAs for public health action.

For reportable conditions with associated laboratory results, the laboratory is responsible for sending an electronic laboratory report to the relevant jurisdictional PHAs. We have required the ELR IG as the standard for reporting to PHAs in § 170.315(f)(3) throughout the Program. We understand that most laboratory systems already have the capability of transmitting results to PHAs according to the ELR IG, as demonstrated by the high level of connectedness of laboratories and PHAs. The PHA receiving the related laboratory result or value often, however, does not receive all of the information needed for action, such as patient demographics, creating gaps in understanding and issues with contact tracing and patient outreach to slow the spread of infectious disease. We propose the transition to the LRI IG—the public health profile—to send results to PHAs. This should enable increased completeness of data for public health action.

Accordingly, and consistent with at least one of the standards in § 170.205(g)(1) and (3), we propose requirements in § 170.315(f)(23) to enable Health IT Modules certified to the criterion to receive, validate, parse, and filter electronic reportable laboratory test values/results according to either the ELR IG or the LRI IG as described below. We propose that either standard will meet this requirement until the ELR IG expires on January 1, 2028, and we propose a transition to the LRI IG after that date. We note that because § 170.205(g) includes the expiration dates for the applicable standards, they are not duplicated within this certification criterion. We request comment on if this timeline is feasible for this transition.

We propose requirements in § 170.315(f)(23)(i) to receive electronic reportable laboratory test values/results transmitted at a minimum through a method that conforms to the standards specified in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2); and, through a method that conforms to the standard in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol. Optionally, to meet the receive requirements, a developer (serving as a Participant or Subparticipant of a QHIN, or who is a QHIN) may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement, or receipt via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the standards specified in § 170.215(d).

We propose requirements in § 170.315(f)(23)(ii) to demonstrate the ability to detect valid and invalid electronic reportable laboratory test values/results received and formatted consistent with the standard in § 170.205(g)(1) or the Public Health Profile within the implementation specification in § 170.205(g)(3). To meet the validate requirements, health IT for public health must include the capability to identify valid electronic reportable laboratory test values/results received and process the data elements as required by the standard in § 170.205(g)(1) or the standard in § 170.205(g)(3). Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with parse and filter requirements in the proposed § 170.315(f)(23)(iii). Health IT for public health must also include the capability to correctly interpret empty sections and null combinations; detect errors in electronic reportable laboratory test values/results received including invalid vocabulary standards and codes not specified in the § 170.205(g)(1) or (3) standards; and record errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose requirements in § 170.315(f)(23)(iii) to enable Health IT Modules certified to the criterion to parse and filter electronic reportable laboratory values/results received and validated in accordance with validate requirements in the proposed § 170.315(f)(23)(ii). We welcome comment on these proposals.

vi. § 170.315(f)(24) Cancer Pathology Reporting—Receive, Validate, Parse, and Filter

We propose to adopt a new certification criterion that is focused specifically on health IT for public health's ability to receive and validate incoming cancer pathology reports according to the proposed standard in § 170.205(i)(4), Cancer Pathology Data Sharing 1.0.0—STU1 and require conformance with its requirements across the certification criterion. As stated in the discussion above regarding proposed revisions to § 170.315(f)(4), cancer reporting informs cancer control efforts, including programs for preventative interventions. An

important component of diagnosing cancer, and particularly in understanding how advanced cases are at the point of diagnosis, is pathology reporting. In section III.B.13.d.iv.4 above, we propose to include cancer pathology reporting as a component of the transmission to cancer registry certification criteria in § 170.315(f)(4). For cancer registries to receive, validate, parse, and filter these reports according to the required standard, we propose to include an accompanying requirement for the receipt, validation, parsing, and filtering of cancer pathology reports in § 170.315(f)(24). Our proposal not only would support cancer registries in having the functionality to accept information in the same standard as sending systems, but it would help sending and receiving health IT progress at the same rate, with aligned functionality.

CDC's National Program of Cancer Registries has been actively working with state PHAs and pathology partners, including the College of American Pathologists (CAP), to develop and pilot a FHIR Implementation Guide for cancer pathology reporting. Early results of these pilots demonstrate that use of FHIR by all involved systems will reduce the need for manual intervention and data cleansing, aid in more timely reporting, and include more complete information, including the demographic information needed to confirm reporting is happening within the patient's state of residence, rather than the state of treatment, as well as for patient matching.[148] [149]

The inclusion of receipt, validation, parsing, and filtering of electronic cancer pathology reporting in the Program would result in more complete, accurate diagnostic information being received by state cancer registries, and contribute to data analysis and early preventative intervention.

We propose that consistent with the standard(s) and implementation specification(s) specified in § 170.205(i)(4), Health IT Modules certified to § 170.315(f)(24) enable a user to receive, validate, parse and filter cancer pathology reports in accordance with the proposed § 170.315(f)(24)(i) through (iii).

We propose requirements in § 170.315(f)(24)(i) to receive electronic cancer pathology reports transmitted via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d). Optionally, to meet the receive requirements, a developer (serving as a Participant or Subparticipant of a QHIN, or who is a QHIN) may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement.

We propose requirements in § 170.315(f)(24)(ii) to demonstrate the ability to detect valid and invalid electronic cancer pathology reports received and formatted in accordance with the standards specified in § 170.205(i)(4). To meet the validate requirements, Health IT Modules certified to the criterion must include the capability to identify valid electronic cancer pathology reports and process the data elements required for the standards specified in § 170.205(i)(4). Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with parse and filter requirements in the proposed § 170.315(f)(24)(iii). Health IT Modules certified to the criterion must also include the capability to correctly interpret empty sections and null combinations; detect errors in electronic cancer pathology reports received, including invalid vocabulary standards and codes not specified in the standards specified in § 170.205(i)(4); and, record errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose requirements in § 170.315(f)(24)(iii) to enable Health IT Modules certified to the criterion to parse and filter electronic reportable cancer pathology reports received and validated in accordance with the validate requirements proposed in § 170.315(f)(24)(ii).

We welcome feedback on these proposals.

vii. § 170.315(f)(25) Electronic Case Reporting—Receive, Validate, Parse, Filter Electronic Initial Case Reports and Reportability Response; and Create and Transmit Reportability Response

Case reporting is a vital component of public health surveillance and case management. Case reports act as early notification of emerging infectious disease outbreaks, as well as early indicators of other threats. For example, case reports demonstrating a rise in human rabies cases could help public health officials understand if there are problems in the local animal population. Case reporting goes beyond COVID–19 and public health emergencies and serves as a key activity to assess, monitor, investigate, and address disease in the community. Therefore, case reporting requires solutions be in place to support these foundational public health services. These activities are achieved by getting data reliably and consistently into health IT for public health for action.

In the HTI–1 Final Rule, we finalized requirements in § 170.315(f)(5) for compliance with either the CDA or the FHIR IGs for electronic case reporting to PHAs (89 FR 1226 through1231). However, in section III.B.13.d.v of this proposed rule, we propose updating the § 170.315(f)(5) certification criterion and its standards conformance requirements specified in § 170.205(t) to require adherence only to the HL7 eCR FHIR IG to be updated and provided by December 31, 2027, as part of a predictable multi-year strategy to facilitate the transition from CDA or FHIR to just FHIR. We believe adherence to a single standard, particularly the FHIR IG, will encourage consistent implementation and lead to greater interoperability compared to referencing multiple standards. Upgrading health IT for public health to support APIs and FHIR payload, as included in the HL7 FHIR eCR IG, creates greater flexibility to respond to emergency issues. Improvements in consistent implementation and interoperability would enable PHAs to have an improved picture of where and when disease outbreaks occur.

Based on feedback we have heard from PHAs and other public health partners that there are current challenges with technology in place at PHAs to receive, validate, parse, and filter incoming electronic case reports, we recognize that the eCR paradigm's newness for PHAs will mean that it will likely take time to fully utilize the data in public health surveillance systems and registries. Because of the variations and inconsistencies in electronic case reports received from Health IT Modules, PHAs often take manual steps and use additional tools in order to be able to parse case reports. Incoming information frequently needs to be re-formatted and filtered, among other steps, for it to be usable to conduct case investigations. Such steps reduce

[148] Blumenthal W, Alimi TO, Jones SF, Jones DE, Rogers JD, Benard VB, Richardson LC. Using informatics to improve cancer surveillance. J Am Med Inform Assoc. 2020 Jul 1;27(9):1488–1495. doi: 10.1093/jamia/ocaa149. PMID: 32941600; PMCID: PMC7647312.

[149] Ayaz M, Pasha MF, Alzahrani MY, Budiarto R, Stiawan D. The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities. JMIR Med Inform. 2021 Jul 30;9(7):e21929. doi: 10.2196/21929. Erratum in: JMIR Med Inform. 2021 Aug 17;9(8):e32869. PMID: 34328424; PMCID: PMC8367140.

efficiency and have the potential to delay time-sensitive public health action.

We propose to adopt a certification criterion for health IT for public health that focuses on the receipt, validation, parsing, and filtering of electronic case reports and reportability response and creation and transmission of the RR according to at least one of the standards referenced in § 170.205(t). Technology in place at PHAs for case reporting and surveillance must be able to receive, validate, parse, and filter electronic case reports, as well as create and electronically transmit RRs. This requirement should reduce burden on PHAs associated with processing reported data and reduce the need for manual intervention. Further, it advances the health IT for public health that receives reported data to align with the technology that transmits the reports, adhering to the same foundational functions and standards. Supporting this alignment allows the industry to advance in harmony and creates a more scalable infrastructure in daily activities as well as in times of emergency.

We note that some PHAs use intermediaries or shared service tools to implement components of the proposed certification criterion. As noted in relied upon software guidance, developers can demonstrate conformance with certification criteria requirements by developing the necessary functionality themselves or by relying on the functionality provided by a different software developer.[150] While we do not have the ability to require, or provide incentives for, PHAs to adopt certified Health IT Modules, other entities (*e.g.,* another Federal or state agency) could choose to do so.

We propose that consistent with at least one of the standards and implementation specifications specified in § 170.205(t), Health IT Modules certified to § 170.315(f)(25) enable a user to receive, validate, parse, and filter electronic case reporting information in accordance with the proposed § 170.315(f)(25)(i) through (iii), and to create and transmit a reportability response in accordance with the proposed § 170.315(f)(25)(iv).

We propose requirements in § 170.315(f)(25)(i) to receive electronic case reports and reportability responses transmitted via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d). Optionally, to meet the receive requirements a developer (serving as a Participant or Subparticipant of a QHIN, or who is a QHIN) may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement; or through a method that conforms to the standard specified in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol.

We propose requirements in § 170.315(f)(25)(ii) to demonstrate the ability to detect valid and invalid electronic case reporting information received and formatted in accordance with at least one of the § 170.205(t) standards. To meet the validate requirements, Health IT Modules certified to the certification criterion must include the capability to identify valid electronic case reporting information received and process the data elements for, at a minimum, the data classes expressed in at least one of the versions of the USCDI standard specified in § 170.213. Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with parse and filter requirements in proposed § 170.315(f)(25)(iii). Health IT Modules certified to the criterion must also include the capability to correctly interpret empty sections and null combinations; detect errors in electronic case reporting information received including invalid vocabulary standards and codes not specified in the § 170.205(t) standards; and record errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose requirements in § 170.315(f)(25)(iii) to enable Health IT Modules certified to the criterion to parse and filter electronic case reporting information received and validated in accordance with validate requirements in the proposed § 170.315(f)(25)(ii) of this section, at a minimum, for any data element identified in at least one of versions of the USCDI standard specified in § 170.213.

We propose requirements in § 170.315(f)(25)(iv) to enable a user to create and transmit a response in accordance with the RR profile in the HL7 eCR FHIR IG in § 170.205(t)(1).

We welcome comments on these proposals.

viii. § 170.315(f)(28)—Birth Reporting—Receive, Validate, Parse, and Filter

As discussed earlier in the section regarding proposed revisions to § 170.315(f)(8), the process of birth reporting has traditionally relied on a provider manually entering data into a web portal, which is used by the jurisdiction's office of vital statistics to produce a birth certificate and report selected data items to CDC's National Center for Health Statistics. Birth reporting helps inform public health programs on important health indicators, including birth rates and infant mortality rates, is used for research, and is used to produce the birth certificates needed for proof of identification, accessing benefits, and other administrative purposes. Our proposal for § 170.315(f)(8) would provide an electronic birth reporting option—that could greatly reduce manual effort if adopted—using the new proposed standard in § 170.205(v).

In order to create alignment between sending and receiving systems, we propose a technical capability for health IT for public health to demonstrate the receipt, validation, parsing, and filtering of incoming birth reports according to the standard referenced in § 170.205(v). Adopting a certification criterion to demonstrate receiving birth reports, and that such technology can do so according to the specified standard, could reduce implementation and maintenance burden and lead to greater consistency and completeness in the reported information.

While most states have adopted an electronic birth registry system (EBRS), these systems today are primarily portal-based, requiring birth information to be entered manually into electronic forms.[151] As described earlier in this proposal, current workflows involve dual-entry based processes. Despite investments made by CDC towards standards-based exchange with EBRS, there remains a gap in jurisdictional office of vital statistics' ability to receive and integrate data within applicable health IT for public health, particularly for data received using FHIR-based standards.

In consultation with CDC and its programmatic experience, we understand that there has been low implementation of the CDA-based IG as documented by CDC programs, and significant progress has been made on

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

[151] National Research Council (US) Committee on National Statistics. Vital Statistics: Summary of a Workshop. Washington (DC): National Academies Press (US); 2009. B, The U.S. Vital Statistics System: A National Perspective. Available from: *https://www.ncbi.nlm.nih.gov/books/NBK219884/.*

testing and piloting of the FHIR IG for birth reporting. As a result, we propose to adopt the FHIR-based approach (as referenced in the proposed § 170.205(v)) for receipt of birth reporting. Adoption of the FHIR-based approach would align the health IT used by public health receiving birth reports with those sending birth reports. Inclusion of the ability to receive and validate FHIR-specific birth reporting within applicable health IT for public health will also provide a baseline set of capabilities that vendors of health IT for public health can build on as additional FHIR-based approaches emerge for public health, including bulk import of data and FHIR Questionnaires. The receipt of FHIR formatted birth records also supports investments being made by CDC to receive FHIR messages downstream through the Data Modernization Initiative.[152]

However, as discussed in section III.B.13.e.i, due to the minimal adoption of the FHIR IG, we propose and seek comment on if we should adopt an interim standards-agnostic functional criterion for electronically transmitting selected medical and health information from birth certificate reports to PHAs based on the data elements outlined in CDC's National Vital Statistics System's ''Guide to Completing the Facility Worksheets for the Certificate of a Live Birth and Report of Fetal Death.'' [153] We seek comment from those who have implemented and used the FHIR IG on its readiness for nationwide adoption. We further seek comment on—if we were to adopt a functional criterion—whether such a criterion should be time-limited to transition to a standards-based criterion as of a specific timeline, for example at 24 months after the timeline for implementation of any such functional criterion.

We propose that consistent with the standard(s) and implementation specification(s) specified in § 170.205(v), Health IT Modules certified to § 170.315(f)(28) enable a user to receive, validate, parse, and filter birth reporting information in accordance with the proposed § 170.315(f)(28)(i) through (iii).

We propose requirements in § 170.315(f)(28)(i) to receive electronic birth reports transmitted via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d). Optionally, to meet the receive requirements a developer (serving as a Participant or Subparticipant of a QHIN, or who is a QHIN) may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement; receipt through a method that conforms to the standard specified in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2); or, receipt through a method that conforms to the standard in § 170.205(p) when the technology is also using an SMTP-based edge protocol.

We propose requirements in § 170.315(f)(28)(ii) to demonstrate the ability to detect valid and invalid electronic birth reports received and formatted in accordance with the standards specified in § 170.205(v). To meet the validate requirements, Health IT Modules certified to the criterion must include the capability to identify valid electronic birth reports received and process the data elements required for the standards specified in § 170.205(v). Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with parse and filter requirements proposed in § 170.315(f)(28)(iii). Health IT Modules certified to the criterion must also include the capability to correctly interpret empty sections and null combinations; detect errors in electronic birth reports received including invalid vocabulary standards and codes not specified in the standards specified in § 170.205(v); and record errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose requirements in § 170.315(f)(28)(iii) to enable Health IT Modules certified to the criterion to parse and filter electronic birth reports received and validated in accordance with validate requirements in the proposed § 170.315(f)(28)(ii).

We welcome comment on these proposals.

ix. § 170.315(f)(29)—Prescription Drug Monitoring Program (PDMP) Data—Receive, Validate, Parse, Filter Prescription Data, Support Query and Exchange

We propose to introduce a functional certification criterion focused on the ability of health IT for public health to receive and validate reported PDMP information, to respond to queries from providers or other PDMP databases and hubs, and to initiate queries to those other PDMP databases and hubs. As mentioned in the earlier discussion regarding a new proposed certification criterion in § 170.315(f)(9), a provider's ability to query information from a PDMP ''can help identify patients who may be at risk for overdose.'' [154] PDMP data can also ''be helpful when patient medication history is unavailable and when care transitions to a new clinician.'' [155] To complement our proposal to support certification of health IT used by providers to be capable of requesting data from PDMP databases, we also believe it is important to certify the capability of health IT for public health, in this case PDMPs, to respond to queries submitted. While it is expected that most PDMPs support this requirement today, inclusion of the functionality in the Program will support PDMPs capabilities in alignment with requirements for health IT systems to request and validate PDMP information. Our proposal will also require that functionality is based on open, consensus-based practices where possible, allowing PDMPs to have the ability to exchange information without undue burden. Additionally, PDMPs should have the capability to support interstate data sharing (or queries) to better inform prescribing practices, improve patient care and safety, monitor patient behaviors that contribute to the opioid epidemic, and facilitate a nimble and targeted response.

Concerns have been raised within the health IT industry regarding the lack of interoperability between different systems and data hubs involved in interstate queries, and these concerns have hindered policy objectives described in several statutes to address the opioid crisis. A lack of consistent interoperability requirements between PDMPs, systems, and data hubs involved in interstate exchange makes such queries burdensome on both the querying and responding systems. Inclusion of a functional certification criterion in the Program in § 170.315(f)(29) would help states conform to functionalities specified in section 1944(b) of the Social Security Act, as added by section 5042(a) of the SUPPORT Act,[156] to support interjurisdictional query and response, and to receive and validate data into health IT. Further, this approach is

[152] *https://www.cdc.gov/surveillance/data-modernization/technologies/cdc-front-door.html.*

[153] *https://www.cdc.gov/nchs/nvss/facility-worksheets-guide.htm.*

[154] *https://www.cdc.gov/opioids/healthcare-professionals/pdmps.html.*

[155] *Id.*

[156] Section 1944(b) of the Social Security Act [42 U.S.C. 1396w–3a] as added by section 5042(a) of the Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (SUPPORT Act) of 2018 (Pub. L. 115–271).

aligned with CMS requirements on funding state systems in 42 CFR 433.112(b)(10), which specify the conditions that a system must meet, including the ''Use [of] a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces . . .''

We also propose that Health IT Modules certified to this criterion be able to receive and validate data reported in a manner consistent with the PDMP technology transmitting, reporting, or querying that data. As expressed elsewhere within this proposal, while PDMP technology currently is capable of receiving and validating data, we believe it is necessary to include functionality for PDMP technology to support the receipt of information in accordance with section 1944(b) of the Social Security Act, as added by section 5042(a) of the SUPPORT Act,[157] and that PDMP technology can accept data according to the same functionality required for transmission under § 170.315(f)(9).

As stated in section III.B.13.e.ii, we believe that further work in the health IT industry is necessary to align current consensus-based standards, specifically FHIR. We also believe that previously described projects to map current standards to FHIR will greatly benefit functionality proposed here, specifically regarding the exchange of information between PDMPs. While HL7 FHIR-based standards are developing and maturing, we propose a set of functional criteria for receiving and validating reported data and initiating and responding to queries from applicable health IT, including other state PDMPs, to support applicable health IT capabilities that may be utilized to meet requirements under section 1944(b) of the Social Security Act, as added by section 5042(a) of the SUPPORT Act.

As described above in section III.B.13.e.ii, section 1944(b) of the Social Security Act, as added by section 5042(a) of the SUPPORT Act, describes a Qualified PDMP, with respect to a State, as a program which, at a minimum, satisfies the following two criteria. First, the program facilitates access by a covered provider to, at a minimum, the following information with respect to a covered individual, in as close to real-time as possible: information regarding the prescription drug history of a covered individual with respect to controlled substances; the number and type of controlled substances prescribed to and filled for the covered individual during at least the most recent 12-month period; and the name, location, and contact information (or other identifying number selected by the State, such as a national provider identifier issued by the National Plan and Provider Enumeration System of the Centers for Medicare & Medicaid Services) of each covered provider who prescribed a controlled substance to the covered individual during at least the most recent 12-month period. Second, the program facilitates the integration of information described in the first criteria above into the workflow of a covered provider, which may include the electronic system the covered provider uses to prescribe controlled substances.

Section 1944(f) of the Social Security Act, as added by section 5042(a) of the SUPPORT Act, includes an increase to Federal Medical Assistance Percentage (FMAP) and Federal Matching Rates for Certain Expenditures Relating to Qualified Prescription Drug Monitoring Programs under Section 1903(a).[158] The requirements proposed in § 170.315(f)(29) are, therefore, written to be consistent with the Section 1903(a) funding requirements in 42 CFR 433.112. Specifically, §§ 433.112(b)(10) and (12) include requirements for the use of open interfaces and exposed application programming interfaces, and alignment with, and incorporation of, standards and implementation specifications for health information technology adopted by the Office of the National Coordinator for Health IT in 45 CFR part 170, subpart B. Section 433.112(b)(16) also requires interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services as applicable.

We propose requirements in § 170.315(f)(29) to enable technology to receive, validate, parse, and filter electronic prescription information for controlled substance medications and support query and exchange of PDMP data as described below.

We propose requirements in § 170.315(f)(29)(i) to receive electronic controlled substance medication prescription information transmitted through a method that conforms to the standard in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2); through a method that conforms to the standard in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol; and, via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least of the versions of the standard specified in § 170.215(d). Optionally, to meet the receive requirements, a developer may demonstrate receipt through a connection governed by the Trusted Exchange Framework and Common Agreement.

We propose requirements in § 170.315(f)(29)(ii) to demonstrate the ability to detect valid and invalid electronic controlled substance medication prescription information received. To meet the validate requirements, the Health IT Module certified to this criterion must include the capability to identify valid electronic controlled substance medication prescription information received and process the data elements including any necessary data mapping or translation between standards. The Health IT Module certified to this criterion must also include the capability to correctly interpret empty sections and null combinations; detect errors in electronic controlled substance medication prescription information received, including invalid vocabulary standards and codes; and record errors encountered allowing a user to be notified of the errors produced, to review the errors produced, and to store or maintain error records for audit or other follow up action.

We propose requirements in § 170.315(f)(29)(iii) to enable a user to parse and filter electronic controlled substance medication prescription information received and validated in accordance with requirements in the proposed § 170.315(f)(29)(ii).

We propose requirements in § 170.315(f)(29)(iv) to enable patient-level query and exchange. The proposed requirement is to enable patient-level queries from external systems of electronic controlled substance medication prescription information of the PDMP including an interstate exchange query. This proposed requirement includes exchange—response requirements to respond to incoming patient-level queries from external systems and exchange—patient access requirements to enable patient access to view electronic controlled substance medication prescription information.

We welcome public comment on this proposed new certification criterion.

[157] *Ibid.*

[158] Section 1944(f) of the Social Security Act [42 U.S.C. 1396w–3a] as added by section 5042(a) of the Substance Use Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (SUPPORT Act) of 2018 (Pub. L. 115–271).

f. New Standardized API for Public Health Data Exchange

i. Background

Despite advances made over the last decade in public health data exchange and health IT interoperability, challenges and gaps remain in exchange capabilities and technical infrastructure. Current efforts have been hampered by a history of bespoke solutions and a multitude of projects, contracts, and implementations that struggled to scale or sustain adequate funding, limiting adoption of resulting standards or implementation guides. This limited adoption of standards and mechanisms for electronic public health data exchange, among other challenges, has resulted in poor interoperability that often relies on manual effort, such as phone calls, faxes, and data entry.

The COVID–19 pandemic stressed our public health system and surfaced flaws in the data that public health officials obtain from health care providers—both in the data itself, but also the ways in which data are reported. As a result, public health officials' access to critical health data during public health emergencies or disasters lags, and their experience varies with respect to the use of technology to glean insights to inform decisions on quarantines, hospital capacity, public health education campaigns, distribution of critical medical supplies, school closures, reopening after a pandemic, and many other essential public health decisions.

Without modern standards and consistent requirements to adopt standards-based IT systems, public health data exchange often relies on custom, siloed solutions, and manual workarounds. Currently, most public health data exchange relies on older versions of HL7 v2 or CDA standards. HL7 v2 and CDA standards support simple, single-patient, event-based submission of documents from healthcare to PHAs, but these standards do not adequately support more complex data exchange use cases, such as bulk exchange of patients who received a specific vaccine. However, now that the majority of hospitals and office-based clinicians nationwide have adopted FHIR-based APIs with Health IT Modules certified to § 170.315(g)(10) for patient and population level services, the technical landscape has evolved, and today's health IT infrastructure presents the public health ecosystem with vastly improved options to engage in more granular data exchange. The shift to HL7 FHIR is needed to support a wide-scale public health response, and we believe broad adoption of HL7 FHIR would reduce burden of implementation and maintenance for data exchange between and among healthcare organizations, providers, and PHAs.

The following describes our proposal to adopt a new certification criterion in § 170.315(g)(20) that would establish requirements for a standardized HL7 FHIR-based API for public health data exchange and extend the capabilities included in the standardized API for patient and population services in § 170.315(g)(10). This new certification criterion would support ongoing and future development of public health FHIR IGs leveraging a core set of existing, modular, and extensible capabilities and standards. Standards referenced in the proposed § 170.315(g)(20) support FHIR capabilities such as API-based event notifications (*i.e.,* HL7 FHIR Subscriptions), SMART App Launch, and Bulk Data Export. Our proposals in § 170.315(g)(20) would also include constrained, specific requirements for health IT for public health such as compliance with the United States Public Health Profiles Library Implementation Guide (USPHPL IG), referenced in the proposed § 170.215(b)(2).

We propose this approach for several reasons. First, we believe that establishing a standardized API for public health data exchange is a necessary first step towards furthering a FHIR-based ecosystem that would support a wide array of public health data exchange use cases, including those established in the Program currently, those being proposed as new certification criteria in the Program, and for future use cases. Importantly, we believe that a FHIR-based ecosystem will better streamline and reduce reporting burden for healthcare organizations and developers, while expanding PHA's access to critical data for action, such as identification of at-risk or infected individuals during an outbreak.

Second, we believe that a standard API for public health data exchange—with a consistent set of standards-based functionalities and capabilities for Health IT Modules certified to the § 170.315(g)(20) certification criterion—would support innovation and longer-term public health modernization and would establish baseline capabilities for public health use cases. The consistent functionalities established in the combination of § 170.315(g)(10) and § 170.315(g)(20) would support the creation or revision of health IT for public health IGs necessary to advance interoperability for specific use cases, such as cancer pathology reporting, which has a draft FHIR IG, or immunization reporting, which is currently only supported by a HL7 v2-based IG. Using HL7 FHIR-based APIs, PHAs and healthcare partners could create an ecosystem where health IT for public health can securely query data directly from the source, in real time, when needed, based on an initial push of relevant data. Helios tested this approach and participants were able to successfully query EHRs for additional patient-level information after an initial trigger, and we are working with CDC to pilot and scale this approach.[159]

Third, we believe that the proposed certification criterion in § 170.315(g)(20) would serve as a glidepath towards an eventual transition to broader HL7 FHIR-based reporting for public health data exchange. We propose that Health IT Modules certified to § 170.315(g)(20) would support modular and foundational capabilities and standards, such server support for subscriptions in § 170.315(j)(23), and support a public health specific set of HL7 FHIR profiles that extend the requirements in § 170.315(g)(10) to support a public health transition to HL7 FHIR.

Finally, we believe this approach will minimize development burden by relying heavily on the standards and capabilities already required of Health IT Modules certified to § 170.315(g)(10), while supporting near-term development and authoring of public health use case-specific HL7 FHIR IGs, where necessary, to transmit relevant data to PHAs. We emphasize for clarity that just because we propose to adopt a public health-focused API certification criterion in § 170.315(g)(20), developers of certified health IT are not required to build one API per criterion (if they are also certified to § 170.315(g)(10) for example). Developers of certified health IT would have flexibility to certify and deploy APIs scoped however they want, if and as they certify Health IT Modules to multiple API-based certification criteria, including those proposed to be included as part of the Base EHR definition in § 170.102, including certification criteria in § 170.315(g)(10), (g)(20), (g)(30) and (g)(34).

We believe that this rulemaking is necessary to set the stage for our long-term strategy to advance public health data modernization in partnership with CDC. We anticipate that requirements to support a standard API for public health exchange would lead to increased capacity for data exchange and spur additional pilots. As use case-specific HL7 FHIR IGs are authored for specific

[159] *https://confluence.hl7.org/display/FHIR/2024+-+01+Helios+Query+and+Response+Track.*

data exchange needs and are refined through successful pilots and approved for widespread adoption by relevant standards development organizations, we intend to consider referencing these HL7 FHIR IGs in future rulemaking. We will continue to work with partners, such as Helios—the public health FHIR accelerator made up of ONC, CDC, PHAs, health IT vendors, and HL7—to support PHAs in more easily receiving and accessing data to further their numerous objectives and missions.

ii. Adoption of Generalizable and Public Health-Specific Standards and Functionality in the Standardized API for Public Health Data Exchange

We propose to adopt some of the functional and standards-based requirements from our existing requirements in § 170.315(g)(10) as part of the certification criterion proposed in § 170.315(g)(20). For example, in § 170.315(g)(10), section III.B.19, we propose to rely on modular functionalities proposed and described in proposed § 170.315(j) to support both functional and dynamic registration, authentication and authorization for system access, and we propose to rely on HL7 FHIR-based IGs familiar to developers of certified health IT with Health IT Modules certified to § 170.315(g)(10), such as the SMART App Launch IG in § 170.215(c), and the FHIR Bulk Data Access IG in § 170.215(d). We also propose that Health IT Modules certified to § 170.315(g)(20) support new subscriptions capabilities proposed in § 170.315(j)(23), and we propose that Health IT Modules certified to § 170.315(g)(20) support HL7 FHIR Resources as profiled by the USPHPL IG proposed in § 170.215(b)(2).

Specifically, we propose that Health IT Modules certified to § 170.315(g)(20) support functional registration, according to the requirements proposed in § 170.315(j)(1) as well as dynamic registration according to the requirements proposed in § 170.315(j)(2) in § 170.315(g)(20)(i). The capability to support functional registration in § 170.315(g)(20)(i)(A) is the same as those currently in § 170.315(g)(10)(iii) for functional registration, which are required for Health IT Modules certified to § 170.315(g)(10). We additionally propose in § 170.315(g)(20)(i)(B) to require support for dynamic registration according to the certification criterion proposed in § 170.315(j)(2). Dynamic registration of apps is intended to reduce the burden of application registration through automated processes. Please see the section titled ''New Requirements to Support Dynamic Client Registration Protocol in the Program'' for more details about our dynamic registration proposal (see section III.B.15).

We also propose that Health IT Modules certified to § 170.315(g)(20) support authentication and authorization capabilities to support public health data access to provider systems. We propose to require such capabilities in § 170.315(g)(20)(ii). Specifically, we propose in § 170.315(g)(20)(ii)(A) to require support for SMART Backend Services system authentication and authorization according to the proposed certification criterion in § 170.315(j)(7) for system applications functionally registered according to the capabilities in § 170.315(g)(20)(i)(A). These capabilities are the same as those currently in § 170.315(g)(10)(v) and (vii) which are required for Health IT Modules certified to § 170.315(g)(10). Furthermore, we propose in § 170.315(g)(20)(ii)(B) to require support for asymmetric certificate-based system authentication and authorization according to the requirements proposed in § 170.315(j)(8) for system apps dynamically registered using the capabilities in § 170.315(g)(20)(i)(B). These requirements would support authentication and authorization for dynamically registered system apps. The proposed requirements to support system authentication and authorization for functionally and dynamically registered system apps will ensure that Health IT Modules certified to § 170.315(g)(20) criterion support authorization server capabilities to enable public health authorization to provider servers.

In § 170.315(g)(20)(iii), we propose a set of requirements necessary to facilitate PHA access to provider system data. These include identification of specific HL7 FHIR Resources often needed by PHAs, capabilities to read and search these data, and support for the subscription of event-based topics that PHAs can leverage in the development of IGs for various public health reporting use cases. We propose that Health IT Modules certified to § 170.315(g)(20) support read and search capabilities for each HL7 FHIR Resource identified in § 170.315(g)(20)(iii)(A) according to the standards and implementation specifications adopted in § 170.215(b)(2). This would enable an API User to read and search patient data that are profiled according to the USPHPL IG in § 170.215(b)(2), including the following HL7 FHIR Resources: Condition; Encounter; Location; Observation; Organization; Patient; and PractionerRole, identified in § 170.315(g)(20)(iii)(A)(*1*)–(*7*).

In referencing the USPHPL IG in § 170.215(b)(2), our intention is to leverage a public health-specific data set of common data elements necessary to support core public health exchange use cases. The USPHPL IG contains reusable content profiles that represent common data PHAs and public health officials receive and use. It was created as a complement to the US Core IG—the USPHPL IG re-uses US Core profiles whenever possible, and only adds new profiles when there is a need for specific profiles for public health data exchange, and no corresponding profile in US Core IG. We believe the USPHPL IG would enable the exchange of health data from healthcare organizations to PHAs with minimal implementation burden, due to its foundation in the US Core IG, and through the reuse of common profiles for public health data exchange purposes. We welcome comment on these proposed information access requirements described in 170.315(g)(20)(iii)(A).

In § 170.315(g)(20)(iii)(B) we propose that Health IT Modules support read and search API calls and bulk FHIR API calls. Specifically, in § 170.315(g)(20)(iii)(B)(*1*)(*i*) we propose that Health IT Modules support the ability for a system client to read HL7 FHIR Resources using the ''id'' data element for the data elements identified in § 170.315(g)(20)(iii)(A), and return the Resources profiled according to the USPHPL IG in § 170.215(b)(2). Similarly, we propose that Health IT Modules support the ability for a system client to search HL7 FHIR Resources according to the applicable search requirements in the ''US Core Server CapabilityStatement'' for the Resources included in § 170.315(g)(20)(iii)(A) and return the information profiled according to the implementation specification in § 170.215(b)(2). Together, these requirements would enable public health systems to extract data from provider systems, consistent with scopes and interactions identified in the SMART App Launch IGs in § 170.215(c). Once those data are read by the API call, the receiving system is then able to parse, process, and update receiving systems. Through this standards-based approach, Health IT Modules certified to § 170.315(g)(20) would enable consistent and predictable access to health data from which apps, systems, and other public health services can be informed and developed.

Additionally, in § 170.315(g)(20)(ii)(*2*), we propose that the Health IT Module certified to

§ 170.315(g)(20) must support Bulk FHIR queries by responding to requests for data according to the implementation specifications adopted in § 170.215(a) and at least one of the versions of the implementation specifications adopted in § 170.215(d) for the Resources listed in § 170.315(g)(20)(iii)(A) and return the information profiled according to the USPHL IG proposed in § 170.215(b)(2). We also propose in § 170.315(g)(20)(ii)(*2*) that for the time period up to and including December 31, 2027, the Health IT Module must support either the ''GroupLevelExport'' operation or the ''_type'' query parameter of at least one of the versions of the implementation specifications adopted in § 170.215(d), or a Health IT Module may support both the ''GroupLevelExport'' operation and the ''_type'' query parameter of at least one of the versions of the implementation specifications adopted in § 170.215(d). On and after January 1, 2028, a Health IT Module certified to § 170.315(g)(20) must meet both the ''GroupLevelExport'' operation and the ''_type'' query parameter for each of the data included in § 170.315(g)(20)(iii)(A) according to at least one of the versions of the implementation specifications adopted in § 170.215(d).

We welcome comment on our proposals for public health information access and our proposals to require support of HL7 FHIR Profiles as specified in the USPHPL IG as the foundation for Health IT Modules certified to § 170.315(g)(20). We recognize that the USPHPL IG does not support all data elements referenced in implementation specifications that support public health use cases represented by the current certification criteria in § 170.315(f). Nor does the USPHPL IG include all data elements necessary for proposed public health reporting in § 170.315(f). We understand this gap, and we intend to support updates to the USPHPL IG through current HL7 activities and processes, future edits, additions, and updates to the HL7 FHIR profiles contained within the USPHPL IG. For example, we anticipate that future versions of the USPHPL IG could include additional use case-specific data elements that are identified in USCDI+ Public Health.

iii. Incorporation and References to Criteria in § 170.315(j) as Part of the Standardized API for Public Health Data Exchange

As stated previously, we propose that Health IT Modules certified to § 170.315(g)(20) include modular capabilities and foundational standards to support a transition to HL7 FHIR-based public health data exchange. As described in section III.B.16 of this proposed rule, we describe a new category of ''modular API capabilities'' certification criteria in § 170.315(j). Specifically, in § 170.315(g)(20)(iii)(C) we propose that a Health IT Module certified to § 170.315(g)(20) support subscriptions according to the requirements in § 170.315(j)(23), including support for a client to subscribe to notifications and then send notifications for event-based interactions. In addition to the support for the framework, subscription topics, and filters in § 170.315(j)(23), we propose in § 170.315(g)(20)(iii)(C)(*1*) that a Health IT Module certified to § 170.315(g)(20) enable a client to subscribe to notifications filtered according to the conditions ''Encounter.reasonCode,'' and ''Encounter.subject'' when a patient encounter starts and the conditions ''Encounter.reasonCode,'' and ''Encounter.subject'' when a patient encounter ends. When an encounter starts or ends, we propose that Health IT Modules certified to § 170.315(g)(20) can send notifications for the event-based interactions identified in § 170.315(g)(20)(iii)(C)(*1*)(*i*) and (*ii*) according to the standard in § 170.215(a) and implementation specification in § 170.215(h)(1). Taken together, we believe that these capabilities would ensure that PHAs will have consistent access of discrete functionalities, defined capabilities, and standardized data from providers using certified health IT systems for a range of public health use cases. We welcome comment on these proposals.

We also invite comment on whether there is utility in requiring future support of other emerging HL7 FHIR standards, such as CDS Hooks proposed as ''workflow triggers for decision support interventions—services'' in § 170.315(j)(23) as part of the certification criterion in § 170.315(g)(20), to support public health data exchange use cases.

14. Bulk Data Enhancements

a. Background

In the ONC Cures Act Final Rule, we adopted the HL7® FHIR® Bulk Data Access (Flat FHIR) (v1.0.0: STU 1) implementation specification (referred to as the Bulk v1 IG), including mandatory support for the ''group-export'' ''OperationDefinition,'' in § 170.215(a)(4) to enable consistent implementation of API-enabled ''read'' services for multiple patients (85 FR 25742). In the HTI–1 Final Rule we moved this Bulk v1 IG standard to § 170.215(d)(1) (89 FR 1283). The Bulk v1 IG builds off the FHIR Asynchronous Pattern to define a standardized process for authenticated and authorized clients to ''request a Bulk Data Export from a server, receive status information regarding progress in the generation of the requested files, and retrieve these files.'' [160] The widespread adoption of Bulk Data APIs enables automated communication between health systems to support use cases like public health surveillance and reporting, clinical research, data analytics, electronic clinical quality measure reporting and more.

Support for the ''group-export'' ''OperationDefinition'' operation enables ''application developers interacting with § 170.315(g)(10)-certified Health IT Modules to export the complete set of FHIR resources . . . for a pre-defined cohort of patients'' (85 FR 25742). As we have stated previously, these cohorts are ''defined at the discretion of the user . . . including, for example, a group of patients that meet certain disease criteria or fall under a certain insurance plan'' (85 FR 25742, 25743). We have also noted previously that the Bulk v1 IG ''has optional parameters which can be used to filter results to a period of time, or one or several specified FHIR resources'' (85 FR 25744).

b. Proposal

We propose to adopt the HL7 FHIR Bulk Data Access (v2.0.0: STU 2) implementation specification (Bulk v2 IG) in § 170.215(d)(2) and incorporate it by reference as a subparagraph in § 170.299. Additionally, we propose that the adoption of the Bulk v1 IG in § 170.215(d)(1) would expire on January 1, 2028. We clarify that both the Bulk v1 IG and Bulk v2 IG would be available for purposes of certification where certification criteria reference the implementation specification in § 170.215(d) until the Bulk v1 IG adoption expiration date of January 1, 2028, after which time only the Bulk v2 IG would be available for certification, if we finalize our rule as proposed.

We believe that raising the floor for certification of bulk data export capabilities would help enable performant and consistent population service APIs. The Bulk v2 IG includes additional clarifications and expanded definitions based on industry feedback related to implementation of the Bulk v1 IG and HL7 workgroup consensus. We

[160] *https://hl7.org/fhir/uv/bulkdata/export.html#bulk-data-export-operation-request-flow.*

believe adopting the Bulk v2 IG would not add significant burden for Certified API Developers with Health IT Modules certified to certification criteria that reference the implementation specification in § 170.215(d) who have already implemented the Bulk v1 IG. The new requirements included in the Bulk v2 IG are generally incremental updates to Bulk v1 IG requirements, and only a handful of the updates are in scope for testing and certification.[161]

One of the pertinent new requirements in the Bulk v2 IG is required server support for the ''_since'' parameter, which allows for filtering by date and time on bulk exports. This parameter can be used to help improve API performance by reducing total resources exported and overall export time. This parameter is also defined in the Bulk v1 IG, but it is marked as ''optional'' for server support there. The Bulk v2 IG contains added clarifications and expanded definitions for the ''_since'' parameter, and the parameter is marked as ''required'' for server (*i.e.,* Health IT Module) support in the Bulk v2 IG.

The added requirement for the ''_since'' parameter, along with all the other clarifications and expanded definitions across the whole Bulk v2 IG, are aspects that we believe will help provide consistent implementation guidance and thus improve access, exchange, and use of EHI because developers will have more guidance to refer to when implementing their Bulk Data APIs. We welcome comment on our proposal to adopt the HL7 FHIR Bulk Data Access (v2.0.0: STU 2) implementation specification.

Our proposal to adopt the Bulk v2 IG in § 170.215(d)(2) implicates all certification criteria that reference the implementation specification in § 170.215(d), and in this proposed rule these certification criteria are: § 170.315(f)(23), (f)(25), (g)(10), (g)(20), (g)(31), (g)(32), and (g)(33). Note that § 170.315(f)(23), (f)(25), (g)(20), (g)(31), (g)(32), and (g)(33) are new Program certification criteria proposed in this rule, and the only currently finalized certification criterion in the Program that includes reference to § 170.215(d) is § 170.315(g)(10).

We propose to continue requiring mandatory support for the ''group-export'' ''OperationDefinition'' defined in the Bulk v2 IG for certification to § 170.315(g)(10); and we propose to require support for the ''group-export'' ''OperationDefinition'' in our proposed new certification criteria in § 170.315(g)(20), (31), (32), and (33). We refer readers to sections III.B.13.f and III.B.20.c for additional discussion on our proposed new certification criteria in § 170.315(g)(20), (31), (32), and (33) and proposed Bulk IG requirements.

We additionally propose to require support for the Bulk v2 IG ''optional'' query parameter known as ''_type'' for testing and certification to § 170.315(g)(10), (20), (31), (32), and (33) because we believe that implementation of the ''_type'' parameter will meaningfully improve API performance by reducing total resources exported and overall export time. The ''_type'' filter allows a requesting system to provide a list of FHIR resource types for the responding system to use, which limits the resources returned to a specific subset. Like the ''_since'' parameter, we believe that this requirement to use ''_type'' parameter is an incremental step that will encourage further industry adoption. As of Spring 2023, 73.7% of deployed Bulk FHIR certified Health IT Modules already support this optional parameter.[162] We welcome comment on our proposal to require support for the ''_type'' parameter for certification.

Finally, we welcome comment on the issues hindering the effective exchange of population data using Bulk FHIR APIs and additional steps ONC can take to help address those issues. Our research and findings to date, on the use of deployed ONC-certified Bulk FHIR APIs, indicate that there are significant challenges and barriers hindering interoperability. We have consistently heard about challenges creating the groups necessary for invoking the ''group-export'' operation, including that there is not a standard process for creating groups and that group sizes are being limited. We have also heard about significant performance issues, with Bulk FHIR exports in some cases taking days or even weeks to complete.[163]

For currently certified Bulk FHIR APIs, we expect that § 170.315(g)(10) certified Health IT Modules support complete patient cohorts (*i.e.,* groups) that enable automated communication between health systems without needing to parse data across multiple exports. For future rulemaking, we are interested in considering testable minimum expectations and/or thresholds for certified Bulk FHIR API performance. We acknowledge that there is variability in Bulk FHIR group exports and performance based on things like system architectures and the variability of resources per patient in a patient cohort. We seek input on Bulk FHIR API performance experiences from users in the field and seek comment on any potential performance bases, expectations, thresholds, industry standards, etc. that we could consider in the future for Certified Bulk FHIR APIs as a baseline. We also welcome comment on the latest developments in the Bulk FHIR space, like the early-stage proposals for Bulk FHIR import functionality that are intended to address data ''push'' use cases as opposed to the data ''pull'' flow modeled by Bulk FHIR export.[164]

We welcome comment on experiences using Bulk FHIR APIs deployed in Health IT Modules certified to § 170.315(g)(10)(i)(B) and (ii)(B) (note that elsewhere in this proposed rule we are proposing to restructure § 170.315(g)(10) and move the Bulk FHIR API requirements in § 170.315(g)(10) to § 170.315(g)(10)(iii)). We also welcome comment on performance experiences and minimum expectations for future iterations of our Bulk FHIR API requirements for different use cases, insofar as we should be thinking about performance differently for different use cases.

15. New Requirements To Support Dynamic Client Registration Protocol In the Program

a. Background to Dynamic Client Registration

In the ONC Cures Act Proposed Rule's preamble (84 FR 7483) we discussed that we considered proposing to require the OAuth 2.0 Dynamic Client Registration Protocol (DCRP) as per RFC 7591 [165] as the mechanism for application registration in the proposed § 170.315(g)(10)(iii). However, in the ONC Cures Act Final Rule (85 FR 25745), we noted that DCRP had low industry adoption at the time, and we subsequently finalized the application registration requirement in § 170.315(g)(10)(iii) without the DCRP

[161] We already include testing support for the Bulk v2 IG, since it was included as a 2022 Approved Standard via the Standards Version Advancement Process (SVAP), and in the Inferno testing tool we only needed three new tests for testing the Bulk v2 IG in comparison to the Bulk v1 IG.

[162] Market share numbers come from this briefing: *https://www.hhs.gov/sites/default/files/2022-02-17-1300-emr-in-healthcare-tlpwhite.pdf.* Support for this parameter was gathered by reviewing developer documentation.

[163] Jones, James R., et al. ''Real World Performance of the 21st Century Cures Act Population Level Application Programming Interface.'' *medRxiv* (2023): 2023–10. *https://www.medrxiv.org/content/10.1101/2023.10.05.23296560v2.*

[164] FHIR Bulk Data Import early stage proposals can be found here: *https://github.com/smart-on-fhir/bulk-import/blob/master/import.md.*

[165] *See* RFC 7591—OAuth 2.0 Dynamic Client Registration Protocol. Available at: *https://datatracker.ietf.org/doc/html/rfc7591.*

standard. We also encouraged health IT developers to coalesce around the development of a common industry standard for application registration.

In addition, we also finalized in the ONC Cures Act Final Rule the API Maintenance of Certification requirement of authenticity verification and registration for production use in § 170.404(b)(1) (85 FR 25763 through 25764). This requirement permits a Certified API Developer to implement an objective and uniform process to verify the authenticity of API Users, where ''API Users'' is defined at 45 CFR 170.404(c) and complete this process within ten business days. We also finalized in § 170.404(b)(1)(ii) that the 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.

In the years since finalization of requirements in § 170.315(g)(10)(iii) and § 170.404(b)(1) in the ONC Cures Act Final Rule, ONC has received feedback that the non-standard application registration process can be burdensome to API Users. The manual nature of some registration processes does not enable efficient registration across multiple certified Health IT Module deployments, and the absence of standardized requirements may cause varying, disparate registration processes across certified Health IT Modules, making widespread registration burdensome. To reduce the registration burden for API Users, we propose to adopt a standard for application registration in § 170.215(o)(1) and adopt a new certification criterion in § 170.315(j)(2) for dynamic registration as part of the suite of revised and new certification criteria proposed as modular API capabilities (See section III.B.16).

Consistent with our proposed new approach to leverage modular API capabilities in § 170.315(j) across various API-related certification criteria, we propose to revise the certification criterion in § 170.315(g)(10) by referencing § 170.315(j)(2) and requiring support for a dynamic registration pathway. We propose to revise the API Maintenance of Certification requirements in § 170.404(b) to require support for publication of information necessary to dynamically register apps. Additionally, we propose to adopt the standard for dynamic application registration as part of the certification criteria in § 170.315(g)(20), (30), (32)–(35). (Please see section III.B.13.d for details on the § 170.315(g)(20) Standardized API for public health data exchange certification criterion proposal and section III.B.20.c for details on our Patient, Provider, and Payer APIs § 170.315(g)(30), (32)–(35) proposals).

b. Adoption of HL7 UDAP Security IG v1

The OAuth 2.0 framework enables a third-party application to obtain limited access to a Hypertext Transfer Protocol (HTTP) service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. Given that the § 170.315(g)(10) certification criterion's authorization model is based on the OAuthAuthorization Framework, registration is required before an app can access information via an API conformant to the § 170.315(g)(10) certification criterion. A § 170.315(g)(10) certified Health IT Module's authorization server must support app registration, as required per the current requirements in § 170.315(g)(10)(iii).

To standardize the application registration approach in Program API criteria, we propose to adopt the HL7® Unified Data Access Profiles (UDAP™) Security for Scalable Registration, Authentication, and Authorization Implementation Guide Release 1.0.0 (UDAP Security IG v1) in § 170.215(o)(1). The UDAP Security IG v1 enables dynamic registration in alignment with the OAuth 2.0 security paradigm already in use in the Program. The SMART App Launch IG, which profiles the OAuthAuthorization Framework established in RFC 6749, is currently required in the Program in the § 170.315(g)(10) certification criterion to enable secure authorization of apps to receive a single patient's data via FHIR. Additionally, the SMART Backend Services specification, also profiling OAuth 2.0, already required in the Program in the § 170.315(g)(10) certification criterion for authorization to retrieve multiple patient's data. The UDAP Security IG v1 would augment the existing OAuth 2.0 found in the Program by enabling scalable and standardized application registration capabilities compatible with FHIR and the SMART App Launch IG to be referenced as requirements in Program API criteria. While the UDAP Security IG v1 defines additional capabilities beyond dynamic registration, Program API criteria requirements proposed in this rule focus on dynamic registration and subsequent authorization requests of dynamically registered apps. To achieve this focus, the Program API proposals referencing the UDAP Security IG v1 require only specific sections relevant to those capabilities.

Scalable dynamic registration in the UDAP Security IG v1 relies upon ''trust communities.'' Trust communities enable scalable trust by establishing common policies that all participants agree to abide by, thereby forgoing the need for individual agreements between organizations for establishing trusted relationships. Participation in a trust community can be represented in a secure and trustworthy manner in the form of cryptographically secure digital certificates. These certificates enable an application to prove to a server that it and its developer are trusted to meet the expectations of the trust community. With the certificate as proof of the trustworthiness of an API User and their application, registration can proceed in an automated manner without the need to perform manual or non-standardized trust verification.

We note that for the purposes of our proposals in § 170.315(g)(10), (20), (30), (32)–(35), and § 170.404(b)(1) an API User and the certified API technology that an API Information Source uses must be part of the same trust community for dynamic registration to occur according to the UDAP Security IG v1. Depending on the scenario, Certified API Developers as well as API Information Sources would be best positioned to determine which trust communities are supported for dynamic registration at a specific deployment. Under this proposal to adopt the UDAP Security IG v1, we have not proposed to require that all trust communities be supported by a Certified API Developer, nor have we specified a particular trust community. However, if an API User seeks to connect an application that is part of the same trust community as the deployed certified API technology, then dynamic registration must be made available to the API User's application.

We are aware that there is a planned update to UDAP Security IG v1, UDAP Security IG v1.0.1, that may publish after the publication of this proposed rule. We anticipate that UDAP Security IG v1.0.1 will fix errors within the UDAP Security IG v1 and not include substantial revisions. As an alternative proposal to adopting the UDAP Security IG v1 in § 170.215(o)(1), we propose to adopt UDAP Security IG v1.0.1 in § 170.215(o)(1) if it is published prior to publication of a final rule finalizing policies proposed in this proposed rule. Interested parties may review the current version of the UDAP Security IG v1.0.1 at *https://build.fhir.org/ig/HL7/fhir-udap-security-ig/.*

c. Revision of Standardized API for Patient and Population Services To Support Dynamic Client Registration

To reduce API User burden when registering their applications and facilitate accessibility of patient health data, we propose to revise the § 170.315(g)(10) certification criterion to require on and after January 1, 2028, dynamic registration of confidential apps, including patient-facing, user-facing, and system apps, and subsequent authorization and authentication support for such dynamically registered apps. We note for this proposal that ''user'' is as defined in 77 FR 54168. First, we propose to modify the existing registration requirements currently in § 170.315(g)(10)(iii) to require a standardized dynamic registration pathway supporting patient-facing, user-facing, and system confidential apps according to the UDAP Security IG v1. As proposed in section III.B.19 of this rule, the registration requirements for the § 170.315(g)(10) certification criterion are proposed to be organized under § 170.315(g)(10)(i). Therefore, we propose this new requirement for a dynamic registration pathway in § 170.315(g)(10)(i)(B). This new standardized dynamic registration pathway would exist alongside the functional registration pathway currently required in § 170.315(g)(10)(iii) and proposed in this rule to be included in § 170.315(g)(10)(i)(A). Second, we propose to require support for authentication and authorization for dynamically registered patient-facing, user-facing, and system confidential apps. Please see section III.B.19 for further details on the proposed re-structuring of the § 170.315(g)(10) certification criterion.

As described in the ''Revised Standardized API for Patient and Population Services Criterion to Align with Modular API Capabilities'' section of this rule, we propose to restructure and move to § 170.315(g)(10)(ii)(A) the existing requirements in § 170.315(g)(10)(v)(A) for authorization for functionally registered patient-facing apps and user-facing apps according to the SMART App Launch IG. In section III.B.19, we propose moving the authorization requirements for functionally registered patient-facing apps to the proposed § 170.315(g)(10)(ii)(A)(*1*)(*i*) and functionally registered user-facing apps to the proposed § 170.315(g)(10)(ii)(A)(*2*)(*i*). We refer readers to section III.B.19 of this proposed rule for additional details regarding this and other related proposals. As described in more detail in subsequent paragraphs, we propose to require support for authorization for dynamically registered patient-facing apps in accordance with the requirements at the proposed § 170.315(g)(10)(ii)(A)(*1*)(*i*) and for dynamically registered user-facing apps in accordance with the requirements at the proposed § 170.315(g)(10)(ii)(A)(*2*)(*i*).

On and after January 1, 2028, we propose to require support for authentication in accordance with the UDAP Security IG v1 of dynamically registered patient-facing apps in accordance with the requirements at the proposed § 170.315(g)(10)(ii)(A)(*1*)(*ii*) and for dynamically registered user-facing apps in accordance with the requirements proposed in § 170.315(g)(10)(ii)(A)(*2*)(*ii*). We describe the details of these proposed authentication requirements in subsequent paragraphs.

On and after January 1, 2028, we propose to require support for authentication and authorization in accordance with the UDAP Security IG v1 of dynamically registered system apps in accordance with the requirements at the proposed § 170.315(g)(10)(iii)(A)(*2*). We describe the details of these proposed authentication and authorization requirements in subsequent paragraphs. These proposed authorization requirements would establish a consistent, standardized method for authorizing dynamically registered patient-facing, user-facing, and system apps to retrieve patient data.

We propose in § 170.315(g)(10)(i)(B) to require on and after January 1, 2028, support for a dynamic registration pathway in the § 170.315(g)(10) certification criterion for confidential apps, including patient-facing, user-facing, and system apps, standardized according to the UDAP Security IG v1. Using this proposed pathway, patient-facing, user-facing, and system confidential apps capable of supporting the UDAP Security IG v1 would be able to dynamically register with the Health IT Module's authorization server in an automated manner. Apps incapable of dynamic registration according to UDAP Security IG v1 would still be able to be registered using the current functional, non-standardized registration pathway currently specified in § 170.315(g)(10)(iii), which is proposed to be moved to § 170.315(g)(10)(i)(A) according to the proposal in section III.B.19 of this rule. We propose in § 170.315(g)(10)(i)(B) to require Health IT Modules certified to § 170.315(g)(10) to support dynamic registration of confidential apps according to the requirements in § 170.315(j)(2), which requires support for dynamic registration of confidential apps according to the UDAP Security IG v1 proposed in § 170.215(o). This includes mandatory support for sections ''Home,'' ''Discovery,'' and ''Registration'' as well as the ''community'' query parameter as defined in section ''Multiple Trust Communities.'' We propose requiring mandatory support for the aforementioned sections as they are the sections from the UDAP Security IG v1 relevant to supporting dynamic registration. We note that trust communities are responsible for enforcing their own policies regarding security and trust, and we encourage such communities to address the topics mentioned in section ''Trust Community Checklist'' of the UDAP Security IG v1 in order to further support for dynamic registration processes.

We clarify in this proposal that Health IT Modules certified to § 170.315(g)(10), through reference to § 170.315(j)(2) in § 170.315(g)(10)(i)(B), must support the otherwise optional ''community'' query parameter as defined in section ''Multiple Trust Communities'' of the UDAP Security IG v1 to facilitate an app's ability to retrieve dynamic registration metadata particular to a specific trust community. The ''community'' query parameter enables an application to receive metadata integral to the dynamic registration process which may otherwise be obscured if the Health IT Module certified to § 170.315(g)(10) supports multiple trust communities.

Next, we propose to require on and after January 1, 2028, support for client authentication for dynamically registered patient-facing confidential apps according to section ''Consumer-Facing'' of the UDAP Security IG v1 in § 170.315(g)(10)(ii)(A)(*1*)(*ii*) by referencing the proposed certification criterion in § 170.315(j)(5). The proposed certification criterion in § 170.315(j)(5), in turn, requires support for authentication as detailed in section ''Consumer-Facing'' of the UDAP Security IG v1 proposed in § 170.215(o). It is through this series of cross-references that we propose, in § 170.315(g)(10)(ii)(A)(*1*)(*ii*), to require support for client authentication for dynamically registered patient-facing confidential apps according to section ''Consumer-Facing'' of the UDAP Security IG v1.

Further, we propose to require on and after January 1, 2028, support for client authentication for dynamically

registered user-facing confidential apps according to the ''Business-to-Business'' section of the UDAP Security IG v1 in § 170.315(g)(10)(ii)(A)(*2*)(*ii*) by referencing the proposed certification criterion in § 170.315(j)(11). The proposed certification criterion in § 170.315(j)(11), in turn, requires support for authentication for the ''authorization_code'' grant type as detailed in section ''Business-to-Business'' of the UDAP Security IG v1 proposed in § 170.215(o). It is through this series of cross-references that we propose, in § 170.315(g)(10)(ii)(A)(*2*)(*ii*), to require support for client authentication for dynamically registered user-facing confidential apps according to section ''Business-to-Business'' of the UDAP Security IG v1.

We propose requiring the ''Consumer Facing'' and ''Business-to-Business'' sections of the UDAP Security IG v1 as they provide authentication requirements for dynamically registered patient-facing apps and user-facing apps respectively during the authorization process. The conformance expectation for support for patient-facing apps for this proposal is that the SMART App Launch capabilities, required in § 170.315(g)(10)(ii)(A)(*1*)(*i*) by referencing the certification criterion proposed in § 170.315(j)(9), would be required to be supported for both functionally registered and dynamically registered patient-facing apps. We propose the exception that client authentication for dynamically registered apps would be required to be supported according to section ''Consumer-Facing'' of the UDAP Security IG v1 as proposed in § 170.315(g)(10)(ii)(A)(*1*)(*ii*) instead of client authentication according to the SMART App Launch implementation guide.

Similarly, the requirement for support for user-facing apps for this proposal is that both functionally and dynamically registered user-facing apps would be required to be supported according to the SMART App Launch capabilities required in § 170.315(g)(10)(ii)(A)(*2*)(*i*) by referencing § 170.315(j)(10)(i). However, client authentication for dynamically registered user-facing applications would be required to be supported according to the ''Business-to-Business'' section of the UDAP Security IG v1 as proposed in § 170.315(g)(10)(ii)(A)(*2*)(*ii*) instead of the SMART App Launch implementation guide.

This proposal does not propose to change the authentication and authorization requirements for patient-facing apps and user-facing apps registered using the functional registration pathway proposed in § 170.315(g)(10)(i)(A). Authentication and authorization for functionally registered patient-facing apps would be expected to occur according to the requirements proposed in § 170.315(g)(10)(ii)(A)(*1*)(*i*), which would by reference to the proposed § 170.315(j)(5) require SMART App Launch capabilities relevant to patient-facing app authentication and authorization. Similarly, authentication and authorization for functionally registered user-facing apps would be expected to occur according to the requirements proposed in § 170.315(g)(10)(ii)(A)(*2*)(*i*), which would by reference to § 170.315(j)(10)(i) require SMART App Launch capabilities relevant to user-facing app authentication and authorization. We refer readers to the ''Revised Standardized API for Patient and Population Services Criterion to Align with Modular API Capabilities'' section of this rule for additional information about the proposed requirements in § 170.315(g)(10)(ii)(A)(*1*)(*i*) and (*2*)(*i*) and how those proposed requirements relate to current § 170.315(g)(10) requirements for authentication and authorization for functionally registered patient-facing apps and user-facing apps.

We also propose in § 170.315(g)(10)(iii)(A)(*2*) that on and after January 1, 2028, authentication and authorization for dynamically registered system confidential apps must be supported according to the ''Business-to-Business'' section of the UDAP Security IG v1 by referencing the proposed § 170.315(j)(8). Proposed § 170.315(j)(8) would require authentication and authorization for the ''client_credentials'' grant type according to the ''Business-to-Business'' section of the UDAP Security IG v1 proposed in § 170.215(o). We propose the system authentication and authorization requirements in § 170.315(g)(10)(iii)(A)(*2*) to require support for a system authorization process which provides client authentication consistent with the proposed dynamic registration process for system confidential apps.

This proposal does not propose to change the authentication and authorization requirements for system apps registered using the functional registration pathway proposed in § 170.315(g)(10)(i)(A). Authentication and authorization for functionally registered system apps would be expected to occur according to the requirements proposed in § 170.315(g)(10)(iii)(A)(*1*), which would by reference to proposed § 170.315(j)(7) require the ''Backend Services'' section of at least one implementation specification adopted in § 170.215(c). We refer readers to the ''Revised Standardized API for Patient and Population Services Criterion to Align with Modular API Capabilities'' section of this rule for additional information about the proposed requirements in § 170.315(g)(10)(iii)(A)(*1*) and how those proposed requirements relate to current § 170.315(g)(10) requirements for authentication and authorization for functionally registered system apps.

We note that we propose in sections III.B.13.d and III.B.20.c to adopt dynamic registration according to the UDAP Security IG v1 for Health IT Modules certified to § 170.315(g)(20), (30), (32)–(35). We invite readers to review those sections for details related to those proposals.

d. Removal of Reference to OpenID Connect Core Specification

In the ONC Cures Act Final Rule, we adopted the OpenID Connect Core 1.0 specification in § 170.215(b) and clarified that only the components included in the SMART App Launch Framework 1.0.0 Implementation Guide adopted in § 170.215(a)(3) were in scope for testing and certification (85 FR 25742). Relatedly, we finalized requirements for the § 170.315(g)(10) certification criterion in (g)(10)(v)(A)(*1*)(*i*) that required for first time connections that authentication and authorization must occur during the process of granting access to patient data in accordance with SMART App Launch Framework 1.0.0 and OpenID Connect Core 1.0 (85 FR 25746). Subsequently in the HTI–1 Final Rule, we finalized moving the regulatory reference of the OpenID Connect Core 1.0 standard from § 170.215(b) to § 170.215(e)(1) (89 FR 1283).

We no longer believe it is necessary to reference the OpenID Connect Core 1.0 specification separately in the API criteria requirements in the Program since the relevant end-user authentication requirements are sufficiently described through the ''sso-openid-connect'' capability from the versions of the SMART App Launch implementation guide currently and as proposed to be adopted in § 170.215(c). We believe requiring the ''sso-openid-connect'' capability from the implementation specification in § 170.215(c) is sufficient to specify the intended end-user authentication requirements related to the § 170.315(g)(10), (30), and (34) certification criteria. The ''sso-openid-connect'' capability is proposed to be required in the § 170.315(g)(10), (30),

and (34) certification criteria by requiring the ''Single Sign-on'' section from the implementation specifications in § 170.215(c), which is required by referencing the proposed § 170.315(j)(9) certification criterion in (g)(10)(ii)(A)(*1*)(*i*) and (g)(30)(ii)(A) and by referencing the proposed § 170.315(j)(10) certification criterion in (g)(10)(ii)(A)(*2*)(*i*) and (g)(34)(ii)(A)(*3*)(*i*). Additional details regarding the proposed adoption of the ''sso-openid-connect'' capability in the § 170.315(g)(10) certification criterion is in section III.B.19, and section III.B.20 for the § 170.315(g)(30) and (34) certification criteria.

Since we are proposing to adopt the ''sso-openid-connect'' capability in the § 170.315(g)(10) certification criterion, we propose to remove reference to the § 170.215(e)(1) from the current requirements in § 170.315(g)(10)(v)(A)(*1*)(*i*) (as finalized in HTI–1 Final Rule), which are proposed to be moved to § 170.315(g)(10)(ii)(A)(*1*)(*i*) according to the proposal in section III.B.19 of this rule.

e. API Conditions and Maintenance Updates To Support Dynamic Client Registration

As discussed in the ONC Cures Act Proposed and Final Rules, Section 4002 of the Cures Act requires the Secretary of HHS to establish Conditions and Maintenance of Certification requirements for the Program (84 FR 7465, 85 FR 25647). To implement this, ONC established the Conditions and Maintenance of Certification requirements in the ONC Cures Act Final Rule, including API Conditions and Maintenance requirements in § 170.404, which establish baseline technical and behavioral requirements for Certified API Developers and their certified API technology. The API Conditions and Maintenance requirements established in the ONC Cures Act Final Rule implemented the Cures Act requirement that certified API technology 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'' (85 FR 25647). The API Condition of Certification includes three main conditions that focus on transparency, fees, and openness and pro-competitiveness. To complement these conditions, we also adopted in § 170.404(b) Maintenance of Certification requirements that address ongoing, and, at times, frequent experiences Certified API Developers would face, such as app registration with certified API technology.

We propose to revise the app registration-oriented maintenance requirements in § 170.404(b) to align with the proposed registration requirements as part of the certification criteria in § 170.315 (g)(10), (20), (30), and (32)–(35). First, we propose to revise the authenticity verification API Maintenance of Certification requirement in § 170.404(b)(1)(i) to not apply to API Users that are part of a trust community submitting registration requests via the proposed dynamic client registration pathways in the certification criteria in § 170.315 (g)(10), (20), (30), and (32)–(35). Specifically, if the API User is part of a trust community supported by the certified API technology used by an API Information Source and the API User's request to register is conformant to the UDAP Security IG v1, then this Maintenance of Certification requirement shall not apply. We propose to revise the requirement in this manner because API Users that are part of a supported trust community will have already undergone the authenticity verification processes required by the trust community to receive a trust community certificate, and their authenticity for registration can be rapidly proven via verification of their trust community certificate. Therefore, we believe that an additional verification process according to § 170.404(b)(1)(i) by a Certified API Developer for verification of API Users possessing a supported trust community certificate and dynamically registering an app is unnecessary and would hinder dynamic registration of apps at scale.

Second, we propose to revise the registration for production use API Maintenance of Certification requirement in § 170.404(b)(1)(ii) so that the registration timeframe for API Users submitting dynamic registration requests according to the UDAP Security IG v1 is one business day, rather than five business days as otherwise applies. Specifically, if the API User is part of a supported trust community and their request to register is valid and conformant to the UDAP Security IG v1, then the Certified API Developer must register and enable the application for production use within one business day. We propose to revise the requirement in this manner to reflect the reduced time necessary to process the automated dynamic registration request.

Third, we propose to add a new API Maintenance of Certification requirement by revising paragraph § 170.404(b)(2)(iv) to require a Certified API Developer to publish information regarding the trust communities supported at each service base URL published as part of the requirements in § 170.404(b)(2)(iii) that can be used by patients to access their EHI. This proposal includes publication of the trust community name, contact information, and web address, and identifying URL in a machine-readable format at no charge for each service base URL published in accordance with § 170.404(b)(2)(iii) on and after January 1, 2028. We propose that Health IT Modules certified to § 170.315(g)(10) may, but are not required, to support trust community discovery for dynamic registration in § 170.404(b)(2)(iv) for the period up to and including December 31, 2027. Additionally, we propose in § 170.404(b)(2)(i)(B) that these trust community details be reviewed quarterly, and, as necessary, updated by Certified API Developers. Finally, we propose to change the title of § 170.404(b)(2) to ''publication of API discovery details for patient access'' to better reflect the requirements we have proposed for this section.

We believe that these requirements would better facilitate individuals' access, exchange, and use of EHI, consistent with the Cures Act, and build upon the existing foundations established in the ONC Cures Act Final Rule by leveraging more advanced standards and enable individuals to access, exchange, and use health data without special effort via dynamic registration using applications of their choice. We welcome public comment on if the requirements for publication of API discovery details for § 170.315(g)(10) should include endpoints enabling provider, bulk, and system access to EHI.

Publication of information regarding supported trust communities enables API Users to know if a trust community they are participating in is also supported at a certified API technology's endpoint conformant to § 170.315(g)(10) or § 170.315(g)(30), and thus if dynamic client registration is supported at that endpoint for patient-facing apps. Without required publication of supported trust communities, API Users may have to query the metadata for each individual certified API technology's endpoint to confirm if their trust community is supported at that endpoint, which would hinder the registration of apps at scale. This requirement for Certified API Developers to publish trust community information would enable API access, exchange, and use of health data ''without special effort'' by ensuring API User access to information necessary for

scalable dynamic registration of patient-facing apps with certified API technology certified to § 170.315(g)(10) or § 170.315(g)(30). We refer readers to the ONC Cures Act Proposed Rule (84 FR 7477) for additional discussion regarding why we believe access to trust community, endpoint, and other API discovery details is a necessary attribute to enable API access, exchange, and use of health data ''without special effort.''

We clarify that Certified API Developers must publish the identifying URI as defined by the trust community, if such a UR is available. Otherwise, Certified API Developers are permitted to establish and publish a unique identifying URI for a trust community. For the purposes of this proposal, trust community URIs defined by the Certified API Developer must be used consistently to uniquely identify a trust community. We welcome comment on our proposal for publication of trust community details in § 170.404(b)(2)(iv).

As an alternative to requiring trust community details be published in any machine-readable format at no charge, we seek comment on standards-based publication strategies and formats for the trust community information we propose for § 170.404(b)(2)(iv). We note our proposal earlier in this preamble in section III.B.3 to require service base URLs and related organization details be published in aggregate vendor-consolidate Brand Bundle format according to the User-access Brands and Endpoints (Brands) specification. We seek comment from Certified API Developers on whether they would consider augmenting their Brand Bundle with trust community information. The Brands specification profiles do not specifically account for trust community information, but given the breadth and extensibility of FHIR, the trust community information could theoretically be included in a Brand Bundle in FHIR format (*e.g.,* using a FHIR extension). If this information is not included in the Brand Bundle, it would need to be published separately in some machine-readable format. We also seek comment from third party-app developers on how this information can best be published to support them in discovering and connecting to FHIR endpoints.

16. New Certification Criteria for Modular API Capabilities

a. Proposal Background

We propose to add a new paragraph (j) to § 170.315 titled ''modular API capabilities.'' This new certification criteria category would promote the Program's modular certification approach and, importantly, would enable different combinations of capabilities across Health IT Modules depending on future use case needs. In general, we expect the capabilities in § 170.315(j) would be standards-based and include a combination of new and existing standards, many of which are currently referenced in § 170.315(g)(10). Additionally, we anticipate that the proposed capabilities in § 170.315(j) would enable the Program to better support a growing number of clinical, public health, and administrative use cases over the long-term, as well as foster innovation and competition in these spaces by providing flexibility for modular development approaches among developers of certified health IT.

Section 4002 of the Cures Act requires health IT developers, as a condition of certification, 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.'' (emphasis added). 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.'' In the ONC Cures Act Final Rule (85 FR 25740), we described our approach to adopting a standardized API for patient and population services certification criterion in § 170.315(g)(10). The Standardized API for Patient and Population Services in § 170.315(g)(10) certification criterion includes conformance requirements for a combination of standards—including data content standards (such as the USCDI standard) and technical standards (such as the SMART App Launch implementation specification for authentication and authorization)—and functional criteria for other technical capabilities (such as application registration and token introspection). Since 2020, the standards development community has undertaken work to: (1) update existing standards and implementation specifications (*e.g.,* US Core IG from version 3.1.1 to 7.0.0) [166]; (2) formalize previously functional capabilities as part of implementation specifications (*e.g.,* token introspection is now part of SMART App Launch 2.0) [167]; and (3) support new and revised capabilities that are modular and use case agnostic (*e.g.,* HL7 CDS Hooks,[168] FHIR Subscriptions,[169] and UDAP Security FHIR IG).[170] These developments have changed the heath IT landscape and helped support a wider range of potential technical solutions for healthcare use cases that previously may not have been supported, or were ineffectively supported, by health IT.

Over time, we have made updates to previously adopted certification criteria based on the evolution of available standards to support more advanced use cases leveraging similar functionality and increasingly interconnected health IT systems. In addition, we have sought to continuously improve the extensibility of specific conformance requirements so that those conformance requirements can support functionality in different types of health IT, and so that complex systems can be certified in a modular fashion. By using the term ''modular'' we mean certification criteria in the Program that are scoped to limited capabilities to enable health IT developers to certify to the specific certification criteria that apply to Health IT Modules they wish to certify, rather than large, multi-functionality, and all-encompassing certification criteria that would give developers less flexibility for certifying in the Program. The work to support extensibility and modularity of certification criteria within the Program has included cross-referencing aligned standards or capabilities across other certification criteria, which support consistent standards and functionality for related actions both across and within certified capabilities. For example, the certification criterion in § 170.315(b)(2) clinical information reconciliation and incorporation references the same standards referenced throughout the transitions of care certification criterion in § 170.315(b)(1), including § 170.205(a)(3) through (5), and the privacy and security certification criteria in § 170.315(d) are conditionally required for certification according to Health IT Module certification requirements for ONC–ACBs described in the privacy and security certification framework in § 170.550(h). Establishing the privacy and security certification framework in § 170.550(h) for ONC–ACBs ensures that Health IT Modules are subject to more specific privacy safeguards and provides more flexibility for certified health IT developers than would be the case if we had a single,

[166] *https://hl7.org/fhir/us/core/history.html.*

[167] *https://hl7.org/fhir/smart-app-launch/STU2/token-introspection.html.*

[168] *https://cds-hooks.hl7.org/.*

[169] *https://hl7.org/fhir/uv/subscriptions-backport/STU1.1/.*

[170] *https://build.fhir.org/ig/HL7/fhir-udap-security-ig/branches/main/index.html.*

multi-functionality privacy and security criterion.

Throughout the Program's history, we have also adopted both certification criteria that include the full scope of a complex transaction (*e.g.,* § 170.315(b)(3) electronic prescribing) and certification criteria that include a discrete portion of a transaction (*e.g.,* § 170.315(c)(1)–(4) clinical quality measures). These different approaches are intended to align our Program requirements to real world implementation scenarios which necessitate both contained execution of complex transactions and the ability to implement related processes across a range of systems in a modular fashion. Our adoption of these varying types of certification criteria allows ONC to administer a more effective and efficient Program, gives developers of certified health IT more nuanced certification options to meet their customers' needs, and promotes a more dynamic marketplace of certified Health IT Modules than would be the case if we bundled different functionalities and standards under fewer certification criteria.

Based on our analysis of the continued evolution of standards and the real-world implementation scenarios for certified health IT to enable FHIR-based APIs, we are proposing to adopt new certification criteria supporting API capabilities for public health data exchange and patient, provider, and payer data exchange (see sections III.B.13 and III.B.20 respectively). As described in this section, we are proposing to revise § 170.315(g)(10) through references to modular API capabilities proposed as certification criteria in § 170.315(j). These certification criteria include standards, functionalities, and certification conformance requirements that align with or are the exact same as the standards, functionalities, and certification conformance requirements currently referenced in § 170.315(g)(10). In addition, we are proposing to update the § 170.315(g)(10) certification criterion to cross-reference newly proposed requirements. Specifically, we propose to adopt a suite of modular API capabilities as certification criteria in § 170.315(j) where each criterion focuses on one specific certification conformance requirement, and we propose to reference these certification criteria as applicable in the proposed revisions to the § 170.315(g)(10) certification criterion (see section III.B.19). For example, we propose to include in § 170.315((j)(1) functional registration, (j)(6) SMART App Launch user authorization, (j)(7) SMART Backend Services system authentication and authorization, (j)(9) SMART Patient Access for Standalone Apps, (j)(10) SMART Clinician Access for EHR Launch. However, we also propose to include in these proposed certification criteria in § 170.315(j) new certification conformance requirements that reflect more recent API standards advancements (*e.g.,* workflow triggers, verifiable health records, and subscriptions) further described below.

b. Modular API Capabilities Certification Criteria

We propose to adopt fourteen new modular API technology certification criteria in § 170.315(j) at (j)(1)–(2), (5)–(11), and (20)–(24). We propose to reserve (j)(3)–(4) and (12)–(19). These new certification criteria would be available for certification based on certain contexts or other programs requiring the use of the specified certified capabilities. Many of these certification criteria are substantially similar to capabilities currently referenced in § 170.315(g)(10)(iii) through (vii). We invite readers to review 85 FR 25739 through 25748 for discussion relevant to capabilities currently referenced in § 170.315(g)(10).

In § 170.315(j)(1), we propose the ''Functional registration'' certification criterion which would require that a Health IT Module demonstrate the ability for applications to register with its authorization server. The process of registration is necessary in many health IT workflows and enables an authorization server to establish a scope of information access for applications and share authentication credentials if applicable. This requirement would be similar to what currently exists in § 170.315(g)(10)(iii) ''Application registration,'' which has a functional requirement to ''enable an application to register with the Health IT Module's 'authorization server.' '' We clarify that for the proposed requirement in § 170.315(j)(1) 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). Additionally, this proposed certification criterion would require a health IT developer to demonstrate its registration process without requiring the use of an identified standard.

In § 170.315(j)(2), we propose the ''Dynamic registration'' certification criterion where a Health IT Module demonstrates the ability to dynamically register confidential apps according to the implementation specifications adopted in § 170.215(o), including mandatory support for sections ''Home,'' ''Discovery,'' and ''Registration'' as well as the ''community'' query parameter as defined in the ''Multiple Trust Communities'' section of the implementation specifications adopted in § 170.215(o). As described in more detail at section III.B.15 of this proposed rule, the UDAP Security IG v1 would provide a more uniform, standardized, and automated registration pathway for applications.

We propose to reserve § 170.315(j)(3) and (j)(4) for future potential registration capabilities.

In § 170.315(j)(5), we propose to adopt the ''Asymmetric certificate-based authentication for patient access'' certification criterion where a Health IT Module's authorization server must support authentication during the process of granting access to patient data to patients according to the implementation specifications adopted in § 170.215(o), including support for asymmetric certificate-based authentication as detailed in section ''Consumer-Facing'' of the implementation specifications adopted in § 170.215(o). Asymmetric certificate-based authentication is a process by which the client and server use public and private keys along with digital certificates for authentication. It is a similar process to asymmetric authentication with the modification that both the client and server verify each other's participation in a trust community. The client and server represent their participation in a trust community through a digital certificate issued by the trust community's certificate authorities. We note that asymmetric certificate-based authentication supports the dynamic client registration proposals included in this rule for adoption in § 170.215(o)(1) (see the section titled New Requirements to Support Dynamic Client Registration Protocol in the Program).

In § 170.315(j)(6) we propose to adopt the ''SMART App Launch user authorization'' certification criterion where a Health IT Module's authorization server must support user authorization during the process of granting access to patient data according to at least one implementation specification adopted in § 170.215(c). We note for this proposal that ''user'' refers to the end-user of an application, and may refer to either a patient, or a healthcare professional or his or her office staff. We clarify for the purposes of certification to this criterion that support for one type of user is sufficient (*e.g.,* support for a patient user, or

support for a healthcare professional or his or her office staff user). The specific requirements include requiring support for Health IT Modules to issue a refresh token valid for a period of no less than three months to confidential apps and native apps capable of securing a refresh token in § 170.315(j)(6)(i), receive and validate tokens issued by the Health IT Module in accordance with at least one implementation specification adopted in § 170.215(c) in § 170.315(j)(6)(ii), and enable for confidential apps persistent access to patient information without requiring user re-authentication or re-authorization until authorization revocation at the user's direction in § 170.315(j)(6)(iii). We further propose in § 170.315(j)(6)(iv) that a Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a user's direction within 1 hour of the request. This proposed certification criterion includes the same functions for refresh tokens from § 170.315(g)(10)(v)(A) ''Authentication and authorization for patient and user scopes'' as well as authorization revocation and token introspection functions from § 170.315(g)(10)(vi) and (vii), respectively. Regarding support for the issuance of refresh tokens for native apps for this certification criterion, we mirror the conformance expectations established in the Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency Interim Final Rule (85 FR 70076), namely that health IT developers can determine the method(s) they use to support interactions with native apps and that health IT developers are not required to support all methods that third-party application developers seek to use.

In § 170.315(j)(7), we propose to adopt the ''SMART Backend Services system authentication and authorization'' certification criterion where a Health IT Module would support system authentication and authorization during the process of granting a system access to patient data in accordance with the backend services profile of at least one implementation specification adopted in § 170.215(c). This certification criterion's conformance requirements are derived from what currently exists in § 170.315(g)(10)(v)(B) ''Authentication and authorization for system scopes,'' proposed in § 170.315(j)(7), as well as the token introspection requirements from § 170.315(g)(10)(vii), proposed in § 170.315(j)(7)(i). The proposed token introspection requirements in § 170.315(j)(7)(i) include requiring that a Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with at least one implementation specification adopted in § 170.215(c). The HL7 standards community re-organized their standards and moved the ''SMART Backend Services: Authorization Guide'' from the Bulk v1 IG (adopted in § 170.215(d)(1)) into the ''Backend Services'' section of the SMART Application Launch Implementation Guide Release 2.0.0 (adopted in § 170.215(c)(2)).

In § 170.315(j)(8), we propose to adopt the ''Asymmetric certificate-based system authentication and authorization'' certification criterion where a Health IT Module would support system authentication and authorization for the ''client_credentials'' grant type during the process of granting access to patient data according to the implementation specifications adopted in § 170.215(o), including support for the ''Business-to-Business'' section of the implementation specifications adopted in § 170.215(o). This certification criterion would support system authentication and authorization for business-to-business access use cases within supported trust communities. This certification criterion would be similar in function to the certification criterion proposed in § 170.315(j)(7) in that it would require system authentication and authorization capabilities but would additionally require support for contextual information and certificates as detailed in the UDAP Security IG v1 to enable authentication and authorization within a trust community. Additionally, we propose to include a section for ''Token introspection'' in § 170.315(j)(8)(i), where a Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with at least one implementation specification adopted in § 170.215(c). This requirement would be similar to what currently exists in § 170.315(g)(10)(vii) ''Token introspection'' and is aligned with similar token introspection requirements in § 170.315(j)(6)(ii) and (7)(i).

In § 170.315(j)(9), we propose to adopt the ''SMART Patient Access for Standalone Apps'' certification criterion where the Health IT Module would support patient authorization and authorization revocation at a patient's direction according to the requirements in § 170.315(j)(6). The capabilities described in the SMART Application Launch Framework Implementation Guide have matured and changed over time, and to support a health IT developer's ability to certify using any of the available implementation specifications in § 170.215(c) we propose allowing health IT developers to support one of the following sets of SMART capabilities listed in paragraph (j)(9)(i), (ii), and (iii). We also note that versions of the SMART Application Launch Framework Implementation Guide adopted in § 170.215(c) will expire on January 1, 2026 for § 170.215(c)(1), and January 1, 2028 for § 170.215(c)(2), and this proposed structure in § 170.315(j)(9) will support the transition to newer versions of the implementation specification. The first set of SMART capabilities requires up to and including December 31, 2025, support for the ''Patient Access for Standalone Apps'' Capability Set, as well as the capabilities of ''launch-standalone'' and ''context-standalone-patient,'' and the capabilities in subsections ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-user'' from § 170.215(c)(1). The second set of SMART capabilities requires up to and including December 31, 2027, support for ''Patient Access for Standalone Apps'' Capability Set as well as the capabilities of ''launch-standalone'' and ''context-standalone-patient,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' and ''permission-user'' capabilities from § 170.215(c)(2). The third set of SMART capabilities requires on and after January 1, 2028, support the ''Patient Access for Standalone Apps'' Capability Set as well as the capabilities of ''launch-standalone'' and ''context-standalone-patient,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' and ''permission-user'' capabilities from § 170.215(c)(3). In addition to requiring the foundational SMART App Launch capabilities for user authorization from proposed § 170.315(j)(6), this certification criterion adds requirements to support SMART App Launch capabilities to enable patients to authorize apps to access information using the SMART standalone launch process.

In § 170.315(j)(10), we propose the ''SMART Clinician Access for EHR Launch'' certification criterion where the Health IT Module would support user authorization and authorization revocation at a user's direction according to the requirements in

§ 170.315(j)(6)(i)–(iii), including mandatory support for one of three sets of SMART capabilities to facilitate user access using EHR launch, proposed in § 170.315(j)(10)(i)(A), (B), and (C). The proposal describes that for the time period up to and including December 31, 2025, a Health IT Module must meet either the requirements specified in paragraph § 170.315(j)(10)(i)(A), (B), or (C); for the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph § 170.315(j)(10)(i)(B) or (C); and finally on and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph § 170.315(j)(10)(i)(C).

The first set of SMART capabilities proposed in § 170.315(j)(10)(A) requires support for the ''Clinician Access for EHR Launch'' Capability Set as well as the capabilities of ''launch-ehr,'' ''context-banner,'' ''context-style,'' and ''context-ehr-patient'' as well as the capabilities in subsections ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' according to the implementation specification adopted in § 170.215(c)(1). The second set of SMART capabilities proposed in § 170.315(j)(10)(B) requires support for the ''Clinician Access for EHR Launch'' Capability Set as well as the capabilities of ''launch-ehr,'' ''context-banner,'' ''context-style,'' ''context-ehr-patient,'' and ''context-ehr-encounter,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' capability according to the implementation specification adopted in § 170.215(c)(2). The third set of SMART capabilities proposed in § 170.315(j)(10)(A) requires support for the ''Clinician Access for EHR Launch'' Capability Set as well as the capabilities of ''launch-ehr,'' ''context-banner,'' ''context-style,'' ''context-ehr-patient,'' and ''context-ehr-encounter,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' capability according to the implementation specification adopted in § 170.215(c)(3). In addition to requiring the foundational SMART App Launch capabilities for user authorization from proposed § 170.315(j)(6)(iv), this certification criterion adds requirements to support SMART App Launch capabilities to enable users to authorize apps to access information using the SMART EHR launch process.

As discussed in section ''SMART App Launch 2.2'' of this rule, we propose to no longer reference specific capabilities and sections of the SMART App Launch implementation guide under § 170.215(c). Instead, Program criteria would specify required capabilities of the SMART App Launch implementation guide. In alignment with that proposal, we propose the SMART capabilities as adopted in HTI–1 in § 170.215(c)(1) for SMART App Launch 1.0.0 and § 170.215(c)(2) for SMART App Launch 2.0.0 be moved to the proposed § 170.315(j)(6)–(10) certification criteria. We propose the SMART App Launch 1.0.0 capabilities relevant to patient access for standalone apps be specified at proposed § 170.315(j)(9)(i) and the capabilities relevant to clinician access for EHR launch be specified at proposed § 170.315(j)(10)(i)(A). Similarly, we propose the SMART App Launch 2.0.0 capabilities relevant to patient access for standalone apps be specified at proposed § 170.315(j)(9)(ii) and the capabilities relevant to clinician access for EHR launch be specified at proposed § 170.315(j)(10)(i)(B). Finally, we propose to include the SMART App Launch 2.2.0 capabilities in § 170.315(j)(9)(iii) for patient access and § 170.315(j)(10)(i)(C) for clinician access. We propose moving token introspection according to SMART App Launch 2.0.0 as adopted in § 170.215(c)(2) in HTI–1 Final Rule to requirements in the proposed certification criteria in § 170.315(j)(6)–(8), which includes (j)(6)(ii), (7)(i), and (8)(i). The proposed certification criteria in § 170.315(j)(9) and (10) would also include conformance dates for each set of required SMART App Launch capabilities that would enable developers as they present their products for certification to move to the newer requirements when they are ready and prior to when a particular conformance requirement may expire, and the other(s) become the new baseline.

In § 170.315(j)(11), we propose the ''Asymmetric certificate-based authentication for B2B user access'' certification criterion where the Health IT Module would support asymmetric certificate-based authentication for the ''authorization_code'' grant type during the process of granting access to patient data to users according to the implementation specifications adopted in § 170.215(o), including support for asymmetric certificate-based authentication as detailed in the ''Business-to-Business'' section of the implementation specifications adopted in § 170.215(o). This certification criterion would be similar to the certification criterion proposed in § 170.315(j)(5) in that it would require support for certificate-based authentication according to the UDAP Security IG v1. However, this certification criterion would be focused on business-to-business authentication requirements to enable users, not patients, access to information in a within a trust community.

We intend to reserve § 170.315(j)(12) through (j)(19) in anticipation of future standards-based capabilities that would be complementary to the certification criteria proposed for adoption in § 170.315(j)(1) through (j)(11).

Beginning in § 170.315(j)(20), we propose a set of new standards-based capabilities. These capabilities are *not* derived from the existing conformance requirements specified in § 170.315(g)(10). Rather, they reflect more advanced capabilities enabled by the HL7 FHIR standard and related implementation guides. We propose to adopt ''workflow triggers for decision support interventions—clients'' in § 170.315(j)(20) and Workflow triggers for decision support interventions—services at (j)(21); ''Verifiable health records'' in § 170.315(j)(22); and ''Subscriptions—server'' in § 170.315(j)(23) and ''Subscriptions—client'' at (j)(24). We propose these modular certification criteria to be broadly applicable to various clinical, public health, and administrative use cases. Below, we describe and provide our rationale for each of these advanced capabilities proposed for inclusion in § 170.315(j)(20) through (24).

i. § 170.315(j)(20) and (21) Workflow Triggers for Decision Support Interventions

We propose to adopt the CDS Hooks Release 2.0 implementation specification in § 170.215(f)(1) to support Program requirements for API-based workflow triggers for decision support interventions (as described in more detail in the next paragraph) in the proposed certification criteria in § 170.315(j)(20) and (j)(21). These certification criteria are proposed separately but are both related to the underlying specification in § 170.215(f)(1). The certification criterion proposed in § 170.315(j)(20) includes requirements for ''clients'' participating in API-based workflow triggers for decision support, and the certification criterion proposed in § 170.315(j)(21) includes requirements for ''services'' providing decision support services to clients.

CDS Hooks is a specification that describes a ''hook''-based pattern for invoking or triggering decision support from within a clinician's workflow (typically the ''client'' side of this pattern). This pattern facilitates a clinician's ability to either pull in results from decision support directly into a clinician's workflow or can be used to launch an interactive application.

We propose that a Health IT Module presented for certification to § 170.315(j)(20) support the requirements of the implementation specification in § 170.215(f)(1) as a ''CDS Client'' including support for the registration of ''CDS Services'' according to the implementation specification in § 170.215(f)(1) in § 170.315(j)(20)(i) and support for authentication and authorization [171] according to the implementation specification in § 170.215(f)(1) in § 170.315(j)(20)(ii). We also propose in § 170.315(j)(20)(iii) that Health IT Modules certified to § 170.315(j)(20) support the execution of decision support workflow triggers in accordance with the implementation specification in § 170.215(f)(1), as well as demonstrate the ability to send a decision support request to a CDS Service according to the implementation specification in § 170.215(f)(1), in § 170.315(j)(20)(iv). As part of the capability to send a decision support request to a CDS Service, we propose in § 170.315(j)(20)(iv)(A) that a Health IT Module support the ability to deliver a CDS Hook request with prefetched information according to the ''Prefetch Template'' section of the implementation specification in § 170.215(f)(1); support access to HL7 FHIR Resources via a RESTful API to support decision support intervention workflows according to the ''FHIR Resource Access'' section of the implementation specification in § 170.215(f)(1) in § 170.315(j)(20)(iv)(B); and support the receipt of a decision support response according to the implementation specification in § 170.215(f)(1) in § 170.315(j)(20)(iv)(C), including support the display of the contents of a decision support response to an end-user and support the ability to launch internal apps and SMART apps from decision support responses according to the implementation specification in § 170.215(f), including support for the ''Link'' field ''appContext,'' in § 170.315(j)(20)(iv)(C)(*1*) and § 170.315(j)(20)(iv)(C)(*2*), respectively.

We propose that a Health IT Module presented for certification to § 170.315(j)(21) support the complementary aspects of the workflow trigger implementation specification in § 170.215(f)(1). Specifically, we propose these Health IT Modules support the requirements of the implementation specification in § 170.215(f)(1) as a ''CDS Service'' including support for registration of CDS Clients in § 170.315(j)(21)(i) and authentication and authorization according to the implementation specification in § 170.215(f)(1) in § 170.315(j)(21)(ii). In § 170.315(j)(21)(iii), we propose a Health IT Module respond to requests for recommendations and guidance via a RESTful API according to the implementation specification in § 170.215(f)(1), including capabilities to receive and process decision support requests in § 170.315(j)(21)(iii)(A); the ability to receive pre-fetched information according to the ''Prefetch Template'' section of the implementation specification § 170.215(f)(1) in § 170.315(j)(21)(iii)(A)(*1*); and the ability to fetch HL7 FHIR Resources via an API according to the ''FHIR Resource Access'' section of the implementation specification § 170.215(f)(1) in § 170.315(j)(21)(iii)(A)(*2*). Finally, we propose in § 170.315(j)(21)(iii)(B) that Health IT Modules support returning a decision support response according to the implementation specification in § 170.215(f)(1), including support for the ''Link'' field ''appContext.''

We note that the proposed workflow triggers criteria in § 170.315(j)(20) and (j)(21) do not define or propose specific workflows associated with decision support, including how and when clinicians use decision support capabilities. Rather, we propose to include standards-based interfaces in § 170.315(j)(20) and (j)(21) to enable clinical systems to call other systems offering decision support services in a standardized manner to support the exchange and use of these services.[172] [173] [174] We request comment on these proposals.

ii. § 170.315(j)(22) Verifiable Health Records

We propose that a Health IT Module presented for certification to § 170.315(j)(22) support the issuance of verifiable health records according to the SMART Health Cards Framework version 1.4.0 standard (SMART Health Cards), which we propose to adopt in § 170.215(g)(1)(i). SMART Health Cards specifies a framework for issuing records represented using HL7 FHIR structured information to users that can be verified by another party.[175] SMART Health Cards is based on international open standards. In addition to HL7 FHIR, SMART Health Cards incorporate DEFLATE Compression, JSON Web Token (JWT), JSON Web Key (JWK), JSON Web Key (JWK) Thumbprint, and HMAC–SHA–256.[176] SMART Health Cards support a decentralized infrastructure and addresses common concerns around verifying portable data. Once a SMART Health Card is generated, the data becomes verifiable to a point in time, which can then be shared at the patient's discretion via Quick-Response Code (QR code). QR Codes are two dimensional barcodes that can encode up to about 3Kb of data.[177] The QR Codes can be easily scanned via smartphones to access the SMART Health Card. We also propose to adopt the SMART Health Cards: Vaccination and Testing Implementation Guide version 1.0.0-rc—STU 1 Release Candidate,'' in § 170.215(g)(2)(i), an HL7 FHIR implementation guide that leverages the SMART Health Cards Framework to describe standards-based methods for the issuance of verifiable health records for vaccination status and infectious disease-related laboratory testing.

The SMART Health Cards standard has seen rapid adoption in the past few years as a reliable and easy way for consumers to receive and share verifiable clinical information. Some notable use cases for verifiable records that have been implemented in clinical settings using the SMART Health Cards standard occurred during the COVID–19 public health emergency to support verifiable COVID–19 test results and

[171] CDS Hooks Release 2.0 includes authentication and authorization of endpoints and identity of the CDS Client. We direct readers to the implementation specification for more detail.

[172] Bradshaw, R.L., Kawamoto, K., Kaphingst, K.A., Kohlmann, W.K., Hess, R., Flynn, M. C., . . . Del Fiol, G. (2022). GARDE: a standards-based clinical decision support platform for identifying population health management cohorts. *Journal of the American Medical Informatics Association: JAMIA, 29*(5), 928–936. doi:10.1093/jamia/ocac028.

[173] Morgan, K.L., Kukhareva, P., Warner, P.B., Wilkof, J., Snyder, M., Horton, D., . . . Kawamoto, K. (2022). Using CDS Hooks to increase SMART on FHIR app utilization: a cluster-randomized trial. *Journal of the American Medical Informatics Association: JAMIA, 29*(9), 1461–1470. doi:10.1093/jamia/ocac085.

[174] Watkins, M., & Eilbeck, K. (2020). FHIR Lab Reports: using SMART on FHIR and CDS Hooks to increase the clinical utility of pharmacogenomic laboratory test results. *AMIA Summits on Translational Science proceedings, 2020,* 683–692.

[175] *https://smarthealth.cards/en/.*

[176] *https://spec.smarthealth.cards/#what-software-libraries-are-available-to-work-with-smart-health-cards.*

[177] *https://www.qrcode.com/en/about/.*

COVID–19 vaccination records.[178] [179] In support of these and related use cases, we propose in § 170.315(j)(22)(i) that Health IT Modules support the ''data minimization'' and ''allowable data'' profiles of the following according to the implementation specification adopted in § 170.215(g)(2)(i): ''Immunization Bundle,'' ''COVID–19 Labs Bundle,'' and ''Generic Labs Bundle,'' ''Patient—United States,'' ''Vaccination,'' ''Lab results COVID–19,'' and ''Lab results—Generic.'' We propose in § 170.315(j)(22)(ii) that Health IT Modules support the ''$health-cards-issue'' operation via a standardized API according to the implementation specification adopted in § 170.215(g)(1)(i). We are also aware that the SMART Health Cards standard is going through the ballot and publication process at HL7 over the next several months. ONC encourages the community to follow along and can access the current CI Build at *https://build.fhir.org/ig/HL7/smart-health-cards-and-links/cards-specification.html.* If there is a published version of the SMART Health Cards standard prior to the publication of the final rule, we will consider adopting that version. We welcome comment on our proposals.

We also note that while we have not proposed nor are we seeking comment on the SMART Health Links technical specification that we are closely following its advances as well as industry uses for future rulemakings.

iii. § 170.315(j)(23) and (24) Subscriptions

The HL7 FHIR Subscriptions Framework describes a standardized method for clients to subscribe to notifications from servers based on pre-negotiated criteria. Once the subscription is established, servers can proactively notify a client when new information has been added or existing information has been updated in its system. Once a notification has been received by a client, the client can take appropriate action, including querying the server for the desired information. The HL7 FHIR Subscriptions Framework also describes methods to transmit payloads with notifications, which may help simplify some interorganizational transactions by enabling real-time updates, selective data transmission, and interoperability, making data exchange between organizations more efficient and effective.

We anticipate that API-based subscriptions will support several use cases across clinical, public health, administrative and research domains. Specific to public health use cases, we envision that future implementation guides could leverage the HL7 FHIR Subscriptions Framework for case reporting processes, immunization reporting processes, syndromic surveillance, reportable laboratory tests and values, and transmitting cancer case information to state cancer registries, among others. We welcome comments on this approach, particularly with respect to the readiness of this standard to support public health reporting and any potential benefits or limitations to this approach that we should consider.

The HL7 FHIR Subscriptions Framework has undergone a significant redesign during the development of the HL7® FHIR® Release 5 (R5) standard, including the use of ''SubscriptionTopic'' HL7 FHIR Resources that define the criteria for standardized subscription notifications. We have structured our proposals in § 170.315(j)(23) and (24) to best accommodate health IT developers and the industry's maturity so that API-based subscriptions can be more easily implemented in the current health IT landscape. While the HL7 FHIR Subscriptions Framework in HL7® FHIR® R5 is well developed, the health IT industry is largely using HL7® FHIR® Release 4, Version 4.0.1 (HL7® FHIR® R4), for HL7 FHIR standards-based exchange. Updating all the criteria in the Program to HL7® FHIR® R5 to accommodate the updated HL7 FHIR Subscriptions Framework would not be practicable nor prudent given the full-scale industry redesign that would be necessary to do so and impacts on users. In order to enable health IT developers using HL7® FHIR® R4, to support the improvements made in the HL7 FHIR Subscriptions Framework in HL7® FHIR® R5, the HL7 standards community created the Subscriptions R5 Backport Implementation Guide version 1.1.0, which specifies some of the HL7® FHIR® R5 Subscriptions Framework enhancements in a way that is compatible with HL7® FHIR® R4.

We propose that a Health IT Module presented for certification to § 170.315(j)(23) or § 170.315(j)(24) support API-based subscriptions according to HL7 FHIR Subscriptions Framework included in the HL7 FHIR Subscriptions R5 Backport Implementation Guide version 1.1.0 (hereafter referred to as ''Subscriptions IG''), which we propose to adopt in § 170.215(h)(1). The proposals in § 170.315(j)(23) and (24) specify constraints on the implementation specification proposed in § 170.215(h)(1), which intend to ensure that Health IT Modules certified to § 170.315(j)(23) or (24) can conform to separate but related aspects and functions of the implementation specification in § 170.215(h). Similar to the proposals in § 170.315(j)(20) and (21), we propose that Health IT Modules certified to § 170.315(j)(23) support subscriptions as a ''server'' and Health IT Modules certified to § 170.315(j)(24) support subscriptions as a ''client'' according to the implementation specification proposed in § 170.215(h)(1).

Recognizing the importance of reducing burden on health IT developers while also striving to improve nationwide interoperability, we propose to adopt the Subscriptions IG in § 170.215(h)(1) support certification criteria for API-based subscriptions in § 170.315(j)(23) subscriptions—server and § 170.315(j)(24) subscriptions—client requirements. The Subscriptions IG includes API-based subscription functionality that goes beyond the scope of FHIR R4, but for the purposes of the Program, we propose in § 170.315(j)(23)(i) and (24)(i), for servers and clients respectively, that Health IT Modules support the requirements specified in section ''1.6 Topic-Based Subscriptions—FHIR R4'' of the implementation specification in § 170.215(h)(1).

Additionally, we propose in § 170.315(j)(23)(ii) and (24)(ii), for servers and clients respectively, that Health IT Modules support the ''R4/B Topic-Based Subscription'' profile as specified in the Subscriptions IG. We note that while this profile is compatible with both HL7® FHIR® R4, and HL7® FHIR® R4B, we propose it for use with HL7® FHIR® R4, at this time.

We also propose in § 170.315(j)(23)(iii) that Health IT Modules support the requirements described in the ''R4 Topic-Based Subscription Server Capability Statement'' of the implementation specification in § 170.215(h)(1), including support for ''create,'' ''update,'' and ''delete'' interactions for HL7 FHIR Subscription Resources according to the implementation specification in § 170.215(h)(1). We propose corresponding requirements for clients in § 170.315(j)(24)(iii), specifically that Health IT Modules support the accompanying client capabilities for the minimum requirements included in the ''R4

[178] Braunstein, M.L. (2022). SMART on FHIR. In: Health Informatics on FHIR: How HL7's API is Transforming Healthcare. Health Informatics. Springer, Cham. *https://doi-org.hhsnih.idm.oclc.org/10.1007/978-3-030-91563-6_10.*

[179] *https://www.thecommonsproject.org/shc.*

Topic-Based Subscription Server Capability Statement'' of the implementation specification in § 170.215(h)(1), including support for ''create,'' ''update,'' and ''delete'' interactions for HL7 FHIR Subscription Resources according to the implementation specification in § 170.215(h)(1). We propose to require servers support the ''create,'' ''update,'' and ''delete'' interactions so that a client will be enabled to create, modify, and delete subscriptions on a server using a standardized API.

Finally, we propose in § 170.315(j)(23)(iv) that Health IT Modules support the ability to send subscription notifications to subscribed clients, and in 170.315(j)(24)(iv) that Health IT Modules support the ability to receive subscription notifications, according to the ''1.6 Topic-Based Subscriptions—FHIR R4'' section of the implementation specification in § 170.215(h)(1). We propose to include in § 170.315(j)(23)(iv)(A) and (24)(iv)(A), for servers and clients respectively, that support for ''id-only'' Payload Types is required as specified in the ''Payload Types'' section of the implementation specifications in § 170.215(h)(1). There are three options available when specifying contents of a notification: empty, id-only, and full-resource. We believe that id-only provides a good balance between security and performance.

Additionally, we propose in § 170.315(j)(23)(v) that Health IT Modules support the ability for a client to subscribe to a subscription topics and parameters defined in notifications by the subscription topics as defined in § 170.315(j)(23)(v)(A) and § 170.315(j)(23)(v)(B)(*1*)–(*19*). We propose in § 170.315(j)(23)(A) to require Health IT Modules support USCDI change notifications which allows a client to subscribe to receive notifications filtered by a patient identifier and send notifications when any of the Resources specified in § 170.315(j)(23)(v)(B) are created or updated as applicable according to the standard in § 170.215(a) and implementation specification in § 170.215(h)(1). We further propose in § 170.315(j)(23)(v)(B) that Health IT Modules support resource notifications supporting the ability for a client to subscribe to notifications filtered according to the conditions below and send notifications for the following Resource interactions according to the standard in § 170.215(a) and implementation specification in § 170.215(h)(1):

- ''AllergyIntolerance'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''patient'' data elements.
- ''CarePlan'' Resource is created or updated, including support for filtering subscription notifications using ''category'' and ''subject'' data elements.
- ''CareTeam'' Resource is created, or updated, including support for filtering subscription notifications using ''category'' and ''subject'' data elements.
- ''Condition'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.
- ''Coverage'' Resource is created or updated, including support for filtering subscription notifications using ''beneficiary'' and ''type'' data elements.
- ''DiagnosticReport'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.
- ''DocumentReference'' Resource is created or updated, including support for filtering subscription notifications using ''subject'' and ''type'' data elements.
- ''Encounter'' Resource is created or updated, including support for filtering subscription notifications using ''reasonCode,'' ''subject,'' and ''type'' data elements.
- ''Goal'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''description,'' and ''subject'' data elements.
- ''Immunization'' Resource is created or updated, including support for filtering subscription notifications using ''patient,'' and ''vaccineCode'' data elements.
- ''MedicationDispense'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''medication[x],'' and ''subject'' data elements.
- ''MedicationRequest'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''medication[x],'' and ''subject'' data elements.
- ''Observation'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.
- ''Patient'' Resource is updated, including support for filtering subscription notifications using the ''identifier'' data element.
- ''Procedure'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.
- ''QuestionnaireResponse'' Resource is created or updated, including support for filtering subscription notifications using the ''subject'' data element.
- ''RelatedPerson'' Resource is created or updated, including support for filtering subscription notifications using the ''patient'' data element.
- ''ServiceRequest'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.
- ''Specimen'' Resource is created or updated, including support for filtering subscription notifications using ''patient'' and ''type'' data elements.

We believe our proposal in § 170.315(j)(23)(v) reflects the public feedback we received during the HTI–1 rulemaking process. Several commenters recommended that the subscription criterion focus on retrieving patient data associated with a specific patient ID as a starting point.

Proposals in § 170.315(j)(23) and § 170.315(j)(24) included in this section reflect public feedback we received in the HTI–1 Proposed Rule. For § 170.315(j)(23), in the HTI–1 Proposed Rule, we received feedback supporting subscription notification for patient data associated with a specific patient ID that allows for notifications based on new or updated data associated with the patient's resources. The proposed resources specified in § 170.315(j)(23)(v)(B) are a subset of USCDI/US Core IG Resources filtered to include those that are part of the HL7 FHIR ''Compartment Patient'' [180] and are widely supported across the healthcare industry. We believe that aligning subscription requirements with US Core resources that are required across several ONC certification Program criteria will contribute to better data exchange, improved patient care, and more effective health IT systems.

We seek public comment on the listed US Core resources in § 170.315(j)(23)(v)(B), and we alternately propose to require client servers to support the ability for a client to subscribe to notifications filtered by all, meaning any, USCDI/US Core resources for ''category,'' ''code,'' and ''subject'' data elements where applicable.

We additionally propose to include in § 170.315(j)(23)(iv)(B) that at a minimum, support for the ''REST-Hook'' channel is required for sending subscription notifications to clients as specified in the ''Channels'' section of the implementation specifications in § 170.215(h)(1). The REST-hook channel

[180] *https://hl7.org/fhir/R4/compartmentdefinition-patient.html.*

uses the RESTful model which is extensively used in FHIR standard and is considered to present the lowest bar for implementation. Finally, we propose to include in § 170.315(j)(24)(iv)(B) required support for consuming notifications via the ''REST-Hook'' channel as specified in the ''Channels'' section of the implementation specifications in § 170.215(h)(1).

We note that we have included references to the proposed certification criterion in § 170.315(j)(23) in two proposed certification criteria in § 170.315(g)(20) and § 170.315(g)(35) and refer readers to those sections for more information on the proposals. Additionally, we have included a reference to the proposed certification criterion in § 170.315(j)(24) in the proposed certification criterion in § 170.315(g)(34) and refer to that section for more information on the proposals.

We believe our proposal and alternative proposals in § 170.315(j)(23) and § 170.315(j)(24) reflect the public feedback we received during the HTI–1 rulemaking process. We acknowledge that the standards may have matured beyond the prior recommended feedback from the HTI–1 Proposed Rule and request comment on these proposals and whether interested individuals and organizations would prefer to implement other standards listed in the Subscriptions IG, including API-based subscriptions based on HL7 FHIR R5.

17. Multi-Factor Authentication Criterion

a. Background

In the ONC Cures Act Final Rule, we finalized a ''multi-factor authentication'' (MFA) certification criterion in § 170.315(d)(13) and applied it to all certification criteria across the privacy & security (P&S) certification framework (85 FR 25700). Through this certification criterion and the P&S Certification Framework, we established an approach that required health IT developers to be transparent about whether their certified Health IT Module supports MFA. As part of the certification process, developers' ''yes'' or ''no'' attestations are made public on ONC's Certified Health IT Product List (CHPL) which is accessible here: *https://chpl.healthit.gov/.*

We established this approach in acknowledgement that ''MFA may not be appropriate or applicable in all situations'' and that ''there is a wide variation in authentication needs and approaches throughout the industry'' (85 FR 25701). We also acknowledged some of the challenges with adopting MFA in healthcare, noting comments expressing concern that it could increase provider burden (85 FR 25701). We therefore finalized our current approach to allow for developers to attest ''no'' as a certification option, and to promote increased transparency into these ''no'' attestations, we included a provision that permitted health IT developers attesting ''no'' to explain why their Health IT Module does not support MFA. Any optional explanations provided were also made available to the public on the CHPL as part of the certification process.

b. Proposal

We propose to update the requirements in the ''Multi-factor authentication'' certification criterion in § 170.315(d)(13) to increase support for MFA in certified health IT without imposing additional requirements on health care providers. We believe these updates match industry information security best practice for important authentication use cases in health IT and that it is necessary to help better protect electronic health information. We propose to expire our current ''yes'' or ''no'' attestation requirements by moving them to § 170.315(d)(13)(i) and including an applicability date for the time period up to and including December 31, 2027 in § 170.315(d)(13). We propose to replace the attestation requirements by revising § 170.315(d)(13) to include the new requirements in § 170.315(d)(13)(ii) that become required for continued conformance on and after January 1, 2028. We propose with these new requirements to require, in § 170.315(d)(13)(ii)(A), Health IT Module support for authentication, through multiple elements of the user's identity, according to industry recognized standards. Additionally, we propose, in § 170.315(d)(13)(ii)(B), to require that Health IT Modules certified to the criterion provide functionality that allows users (*e.g.,* providers and patients) to configure, enable and disable these multi-factor authentication capabilities. Lastly, we propose that a health IT developer may meet the proposed revised certification criterion's requirements just by satisfying the new conformance requirements proposed in § 170.315(d)(13)(ii) in lieu of § 170.315(d)(13)(i) prior to paragraph (i)'s December 31, 2027, expiration.

We expect that Health IT Modules certifying to this MFA criterion must have the ability to authenticate users using multiple means to confirm that users are who they claim to be. Multiple means of authentication in this context 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 (85 FR 25701). Examples of industry recognized standards for MFA include NIST Special Publication 800–63B Digital Identity Guidelines, and ISO 27001.[181] As we stated in 2019, when we first proposed MFA requirements in the Program, a government led initiative and numerous organizations and groups recommend the use of MFA (84 FR 7451). More recently, the HHS Office for Civil Rights has identified weakened healthcare authentication measures as one of the biggest causes of data breaches in recent years.[182] We believe our proposal helps improve security by increasing access to MFA. This is because it is less likely that an unauthorized individual or entity will be able to succeed in proving one's identity when more than one authentication factor is used.

We also propose corresponding revisions in the principles of proper conduct for ONC–ACBs in § 170.523(m) and the privacy and security certification framework in § 170.550(h)(3). In § 170.523(m)(3) we propose to time-limit the applicability of § 170.315(d)(13) for the time period up to and including December 31, 2027. After this date, ONC–ACBs will no longer be required to obtain a record of updates from health IT developers to describe MFA use cases. Additionally, we propose to apply the updated MFA requirements to each of the certification criteria in § 170.315(b)(3), (e)(1), (g)(10), and (g)(30). Specifically, in §§ 170.315(b)(3)(ii)(G), 170.315(e)(1)(iii), 170.315(g)(10)(ii)(A)(*1*)(*iii*), and 170.315(g)(30)(ii)(C) we propose to include a requirement that on and after January 1, 2028, Health IT Modules certified to any of these criteria are also certified to § 170.315(d)(13)(ii). Given our proposal to embed § 170.315(d)(13) references into the certification criteria we propose requiring MFA support in, § 170.315(d)(13) does not need to also be referenced in § 170.550(h)(3)(i) through (ix). Therefore, we propose to expire all the references to § 170.315(d)(13) in § 170.550(h)(3)(i) through (ix) by time-limiting the applicability of § 170.315(d)(13) in § 170.550(h)(3)(i)

[181] NIST Special Publication 800–63B: *https://pages.nist.gov/800-63-3/sp800-63b.html;* ISO 27001: *https://www.iso.org/standard/27001.*

[182] *https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html.*

through (ix) for the time period up to and including December 31, 2027.

We clarify that Health IT Modules certified to § 170.315(g)(10) and § 170.315(g)(30), on and after January 1, 2028, would be required to support MFA for patient scopes or patient-facing authentication use cases, rather than non-patient (*i.e.,* clinical user) and system-level use cases. We also clarify that Health IT Modules certified to § 170.315(b)(3) on and after January 1, 2028, would have the option of meeting the requirement to support MFA in this certification criterion by supporting user level MFA for electronic prescribing of a controlled substance.[183] With respect to Health IT Modules certified to § 170.315(b)(3) that do not support electronic prescribing of a controlled substance, we propose that they must still demonstrate support for MFA for some other user authentication use case. We welcome comment on these proposals. We also request comment on whether we should consider in the final rule exempting Health IT Modules from the MFA requirement when they are only designed to support non-controlled substance electronic prescribing. We would also appreciate any statistics, if available, on the market segment that would be affected by this specific policy.

Finally, we propose to modify § 170.550(h)(3)(viii) to require that Health IT Modules certified to § 170.315(g)(20) and (g)(30) through (36), in addition to § 170.315(g)(7) through (g)(10) as is currently required, are also certified to the certification criteria specified in § 170.315(d)(1), (9), (12), and, for the time period up to and including December 31, 2027, § 170.315 (d)(13); and (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), or (10). We similarly propose, in § 170.550(h)(3)(x), that Health IT Modules certified to any criterion proposed in § 170.315(j) are 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), and (12). We welcome comment on this proposal including whether we should require testing for § 170.315(d)(13) in any of the certification criteria in § 170.315(j).

18. Revised Computerized Provider Order Entry—Laboratory Criterion

The laboratory-based workflow is initiated when a clinician orders a test (such as part of a routine screening or a diagnostic work up). If the clinician does not provide all of the information requested in the test order, or if the test order does not request specific data, the laboratory or the public health authority receiving the laboratory results will not have complete information. Such missing information could include patient demographics, creating gaps in understanding and addressing issues related to health equity, in addition to direct issues with contact tracing and patient outreach that could slow down the spread of infectious disease.

Laboratory orders are often initiated in EHR systems when ordered by clinicians practicing in hospitals or large healthcare organizations. The laboratory provides the results from the test back to the ordering clinician by various means via their Laboratory Information Management Systems (LIMS) or Laboratory Information Systems (LIS). Ensuring that systems that create orders are also capable of transmitting orders and receiving associated results and values back electronically, according to national standards, will create more complete patient information available to clinicians throughout the laboratory workflow.

We propose to revise the ''computerized provider order entry—laboratory'' certification criterion in § 170.315(a)(2) by requiring Health IT Modules certified to this criterion to create and transmit laboratory orders electronically, to be performed according to the Lab Orders Interface (LOI) Implementation Guide proposed at 170.205(g)(2) and the Lab Results Interface (LRI) Implementation Guide proposed in § 170.2015(g)(3). Specifically, we propose to implement our proposed revisions by moving our existing § 170.315(a)(2) requirements into paragraphs § 170.315(a)(2)(i) that expire on January 1, 2026, and by including new standards-based requirements for lab orders in § 170.315(a)(2)(ii) that must be met on and after January 1, 2028.

We propose to revise § 170.315(a)(2) by establishing a new subparagraph in § 170.315(a)(2)(ii) to include requirements for Health IT Modules certified to § 170.315(a)(2) to enable a user to create and transmit laboratory orders electronically, to be performed according to the LOI Implementation Guide (§ 170.205(g)(2)) cross-referenced in § 170.315(a)(2)(ii)(B). We further propose to require Health IT Modules certified to § 170.315(a)(2) to enable a user to receive and validate laboratory results according to the LRI Implementation Guide (§ 170.205(g)(3)) cross-referenced in § 170.315(a)(2)(ii)(C).

As discussed in our proposals relevant to § 170.315(f)(3), in section III.B.13.d., the LRI and LOI IGs reduce some of the optionality that is present in currently implemented specifications, which may improve the completeness of information. For example, the LRI and LOI implementation guides require ordering provider, patient address, patient phone number, and patient race. Further, the LRI IG aligns with Clinical Laboratory Improvement Amendments of 1988 (CLIA) requirements in place for laboratories. The update to these specifications, and the inclusion of the receipt of orders in § 170.315(f)(3), as well as the receipt of results in § 170.315(a)(2), ensure that functions throughout the lifecycle of the laboratory order, from entry, to result, to reporting to public health authority, is covered by electronic requirements with the associated national standard.

We propose that for the time period up to and including December 31, 2027, a Health IT Module certified to § 170.315(a)(2) must meet either the requirements specified in paragraph (a)(2)(i), or the requirements specified in paragraph (a)(2)(ii). On and after January 1, 2028, for Health IT Modules certified to § 170.315(a)(2), we propose that such Health IT Modules must meet the requirements specified in paragraph (a)(2)(ii).

We welcome comment on these proposals.

19. Revised Standardized API for Patient and Population Services Criterion To Align With Modular API Capabilities

As part of our overall proposal, we propose to revise the structure of the regulation text in § 170.315(g)(10) for clarity as well as phrasing consistency with other proposed API certification criteria in this proposed rule (*e.g.,* the proposed applicable § 170.315(j) criteria). These revisions to the regulation text's structure are intended to improve readability and how the certification criterion's requirements are organized. Generally, these specific reorganizing revisions are not intended to introduce substantive changes to current conformance requirements. A notable exception is the proposed reference to certification criterion requirements proposed in § 170.315(j)(10)(ii), which would be a new requirement for user authorization revocation. We also note that we have included proposals that introduce new, substantive requirements as well to § 170.315(g)(10) with applicable conformance timing. These details are discussed below and, as applicable,

[183] Multi-factor authentication for electronic prescribing of controlled substances is required to meet the Electronic Prescribing of Controlled Substances (EPCS) requirements set by Drug Enforcement Administration (DEA).

proposed § 170.315(j) certification criteria requirements will be discussed along with current and proposed § 170.315(g)(10) requirements to show a complete view of all proposed revisions to the § 170.315(g)(10) certification criterion's regulation text.

We propose to revise the § 170.315(g)(10) certification criterion to reference applicable proposed § 170.315(j) certification criteria to make the regulation text of § 170.315(g)(10) more concise, clear, and consistent with the other proposed API certification criteria. In section III.B.16 of this proposed rule, we discuss our proposal to add a new category of certification criteria in § 170.315(j) titled ''Modular API capabilities.'' The § 170.315(j) certification criteria, if finalized, would allow for specific API certification requirements to be demonstrated independently or in different combinations through the Program in circumstances where meeting all of § 170.315(g)(10)'s requirements would not be applicable. These proposed changes, taken together, would help the Program support APIs across clinical, public health, administrative, and other use cases.

a. Proposed Revisions for Registration

We propose to reorganize and rephrase the application registration requirements currently in § 170.315(g)(10)(iii). The current application registration requirements in § 170.315(g)(10)(iii) require support for an application to register with the Health IT Module's ''authorization server'' to support retrieval of data for a single patient's data and multiple patients' data. No standard is currently specified for registration. We propose to rename § 170.315(g)(10)(i) as ''Registration,'' and move the existing application registration requirements from § 170.315(g)(10)(iii) to § 170.315(g)(10)(i). We also propose to clarify in § 170.315(g)(10)(i) which app types are currently required to be supported for functional registration (confidential and public apps). Clarifying these app types required for functional registration does not introduce new requirements since confidential and public apps were already required to be supported for functional registration according to the current requirements in § 170.315(g)(10)(iii). We note that we propose to no longer specifically reference the ''confidential app'' profile from the SMART App Launch implementation guide in the § 170.315(g)(10) certification criterion. Instead, we propose to refer to the app types of ''confidential app'' and ''public app'' as described in the section of this rule titled ''SMART App Launch 2.2.'' In addition to this move and clarification, we also propose that on and after January 1, 2028, both the capabilities proposed in § 170.315(g)(10)(i)(A) and (B) would be required to support the full scope of API capabilities required in the § 170.315(g)(10) certification criterion. This includes as part of the regulation text reordering new proposed language in § 170.315(g)(10)(i)(A) to reference § 170.315(j)(1) to support ''functional registration'' and new proposed language in § 170.315(g)(10)(i)(B) to reference § 170.315(j)(2) to support ''dynamic registration.'' We clarify that the capability described at proposed § 170.315(g)(10)(i)(A) is not intended to substantively change the application registration requirements with which health IT developers are currently familiar, but instead clarify the nature of the functional requirements and detail which app types are required to be supported for functional registration (confidential and public apps). To accommodate the distinct proposal to require dynamic client registration as part of § 170.315(g)(10), the proposed § 170.315(g)(10)(i)(B) focuses on dynamic client registration for patient and user access as proposed in § 170.315(g)(10)(ii) and system access at (iii).

b. Proposed Revisions for Patient and User Access

In the context of retrieving data for a single patient, we propose to restructure and rephrase the data response requirements currently in § 170.315(g)(10)(i)(A), supported search operations requirements in § 170.315(g)(10)(ii)(A), secure connection requirements in § 170.315(g)(10)(iv)(A), authentication and authorization for patient and user scopes requirements in § 170.315(g)(10)(v)(A), and patient authorization revocation requirements in § 170.315(g)(10)(vi). We propose reorganizing those requirements to all be under proposed § 170.315(g)(10)(ii) to make clear which requirements support data retrieval for a single patient's data. Specifically, we propose to rename § 170.315(g)(10)(ii) to be ''*Patient and user access*'' and include these paragraphs as follows.

We propose to revise the paragraph in § 170.315(g)(10)(ii)(A) and add subparagraphs in § 170.315(g)(10)(ii)(A)(*1*) and (*2*) to include, with revisions, the requirements for secure connection currently in § 170.315(g)(10)(iv)(A), authentication and authorization for patient and user scopes currently under § 170.315(g)(10)(v)(A), and patient authorization revocation requirements currently in § 170.315(g)(10)(vi). We also propose to add a multi-factor authentication requirement in § 170.315(g)(10)(ii)(A)(*1*)(*iii*) for patient-facing uses. The specific alignment between current regulatory text paragraphs and proposed new paragraphs is detailed in each of the bullets that follow.

- Proposed § 170.315(g)(10)(ii)(A)(*1*)(*i*), § 170.315(g)(10)(ii)(A)(*2*)(*i*), and § 170.315(g)(10)(ii)(B)(*1*) maintain the existing requirement in § 170.315(g)(10)(iv)(A) to support a secure connection and authentication and authorization for apps requesting patient and user scopes according to the SMART App Launch and US Core implementation guides. We propose to no longer explicitly mention ''secure connection'' since we believe it is redundant as the referenced implementation guides already include such requirements for secure connections. The ''App Protection'' section of the SMART App Launch IG requires the use of secure TLS connections and is required as part of the requirements at proposed § 170.315(g)(10)(ii)(A)(*1*)(*i*) and § 170.315(g)(10)(ii)(A)(*2*)(*i*) by reference to proposed § 170.315(j)(9) and § 170.315(j)(10)(i) respectively. Proposed § 170.315(j)(9) and § 170.315(j)(10)(i) require support for authorization according to capabilities from one of the SMART App Launch IGs adopted in § 170.215(c), which in turn necessitates the use of secure TLS connections as required in the ''App Protection'' section of the SMART App Launch IG. Additionally, the ''Security'' section of the US Core IG requires the use of secure TLS connections and is required as part of the requirements at proposed § 170.315(g)(10)(ii)(B)(*1*). Proposed § 170.315(g)(10)(ii)(B)(*1*) requires support for responding to requests for patient data according to the one of the US Core IGs adopted in § 170.215(b)(1), which in turn necessitates the use of secure TLS connections as required in the ''Security'' section of the US Core IG.
- We propose to revise the organization of authentication and authorization requirements for patient-facing apps and use-facing apps for § 170.315(g)(10) to be under § 170.315(g)(10)(ii)(A). We propose authentication and authorization requirements for patient access to be under § 170.315(g)(10)(ii)(A)(*1*) and authentication and authorization requirements for user access be under

§ 170.315(g)(10)(ii)(A)(*2*). The proposed revisions in § 170.315(g)(10)(ii)(A)(*1*)(*i*) and § 170.315(g)(10)(ii)(A)(*2*)(*i*) maintain the requirements currently in § 170.315(g)(10)(v)(A) for authentication and authorization for patient and user scopes (scopes being information access permissions as represented in the OAuth 2.0 Authorization Framework) according to SMART App Launch capabilities as currently referenced in § 170.215(c) and OpenID Connect Core as currently referenced in § 170.215(e). The proposed revisions in § 170.315(g)(10)(ii)(A)(*1*)(*i*) reference the proposed certification criterion in § 170.315(j)(9) ''SMART patient access for standalone apps,'' which requires the SMART App Launch capabilities that are currently required to be supported for authentication and authorization of patient-facing apps. The proposed revisions in § 170.315(g)(10)(ii)(A)(*2*)(*i*) reference the proposed certification criterion in § 170.315(j)(10) ''SMART clinician access for EHR launch,'' which requires the SMART App Launch capabilities currently required for authentication and authorization of user-facing apps. Current OpenID Connect Core requirements would also be maintained by the proposed references to § 170.315(j)(9) ''SMART patient access for standalone apps'' and (10) ''SMART clinician access for EHR launch'' since those proposed certification criteria require the ''sso-openid-connect'' SMART App Launch capability by requiring the ''Single Sign-on'' section of one of the SMART App Launch IGs adopted in § 170.215(c). In addition to maintaining current requirements from § 170.315(g)(10)(v)(A) for authentication and authorization for patient and user scopes, the proposed references in the § 170.315(g)(10) certification criterion to § 170.315(j)(9) and (10) would also add requirements to support SMART App Launch capabilities for authentication and authorization for patient-facing apps and user-facing apps according to the implementation specification of SMART App Launch 2.2.0, proposed in this rule to be adopted in § 170.215(c)(3). The proposed certification criteria in § 170.315(j)(9) and (10) would also include conformance dates for each set of required SMART capabilities. Conformance to each set of required SMART capabilities would be in alignment with the following: (1) expiration of SMART App Launch 1.0.0, adopted in § 170.215(c)(1), for use in the Program on January 1, 2026 as finalized in the HTI–1 Final Rule (89 FR 1292); (2) the proposed expiration of SMART App Launch 2.0.0, adopted in § 170.215(c)(2), for use in the Program on January 1, 2028; and (3) the proposed adoption of SMART App Launch 2.2.0 in § 170.215(c)(3). Please see the section titled ''SMART App Launch 2.2'' of this rule for additional details regarding the proposed expiration and adoption of SMART App Launch 2.0.0 and 2.2.0 respectively. For more information regarding how SMART App Launch capabilities as currently required and proposed to be required correspond to the proposed certification criteria in § 170.315(j)(9) and (10), including specific capabilities and their conformance dates, please refer to section III.B.16 ''New Certification Criteria for Modular API Capabilities.''

- The requirements currently in § 170.315(g)(10)(v)(A)(*1*)(*ii*), § 170.315(g)(10)(v)(A)(*1*)(*iii*), and § 170.315(g)(10)(v)(A)(*2*) regarding the issuance of refresh tokens are mirrored in the proposed paragraphs in § 170.315(g)(10)(ii)(A)(*1*)(*i*) and (*2*)(*ii*) via cross references to the certification criteria proposed in § 170.315(j)(9) ''SMART patient access for standalone apps'' and (10) ''SMART clinician access for EHR launch'' respectively, which reference the proposed certification criterion in § 170.315(j)(6) ''SMART App Launch user authorization,'' wherein the language has been simplified to consolidate existing refresh token requirements and remove extraneous references to refresh token requirements already included in referenced implementation guides. Additionally, we include the authentication and authorization requirements that are currently in § 170.315(g)(10)(ii)(A)(*1*)(*i*) and (*ii*) in our proposals in § 170.315(g)(10)(ii)(A)(*1*) ''Authentication and authorization for patient access'' and (*2*) ''Authentication and authorization for user access,'' which reference the proposed criteria at § 170.315(j)(9) ''SMART patient access for standalone apps'' and (10) ''SMART clinician access for EHR launch,'' which both reference the proposed certification criterion in § 170.315(j)(6) ''SMART App Launch user authorization.'' We reiterate the existing conformance expectations established in the COVID–19 Public Health Emergency Interim Final Rule (85 FR 70076) that health IT developers can determine the method(s) they use to support interactions with native apps and that health IT developers are not required to support all methods that third-party application developers seek to use. Further, we propose to revise the requirements that enable persistent access to confidential apps on subsequent connections which are currently required in § 170.315(g)(10)(v)(A)(*2*)(*ii*) to instead require support for a user to enable for confidential apps persistent access to patient information without requiring user re-authentication or re-authorization until authorization revocation at the user's direction. Additionally, we propose moving this requirement to part of one of the modular API capabilities in (j), specifically in § 170.315(j)(6)(iii). As proposed, § 170.315(j)(6)(iii) is referenced by the proposed certification criteria in § 170.315(j)(9) ''SMART patient access for standalone apps'' and (10) ''SMART clinician access for EHR launch,'' which are referenced by the proposed revised certification criterion in § 170.315(g)(10). Revising the requirement in this manner is intended to provide developers more flexibility in implementing persistent access for confidential apps while maintaining the requirement that patients and users can authorize persistent access to patient data to confidential apps until revoking that access.

- We propose to move the current ''patient authorization revocation'' requirement in § 170.315(g)(10)(vi) to § 170.315(j)(6) ''SMART App Launch user authorization,'' specifically § 170.315(j)(6)(iv) ''User authorization revocation.'' These requirements are referenced by the proposed certification criterion in § 170.315(j)(9) ''SMART patient access for standalone apps'' which is referenced by the proposed revised certification criterion in § 170.315(g)(10)(ii)(A)(*1*)(*i*). We propose a new requirement to require support for user authorization revocation in § 170.315(g)(10)(ii)(A)(*2*)(*i*) which references the requirements at the proposed certification criterion in § 170.315(j)(10)(ii), and is proposed to take effect on and after January 1, 2028. This would require a Health IT Module's authorization server to be able to revoke and must revoke an authorized application's access at a user's direction within 1 hour of the request. This is distinct from the existing patient authorization revocation requirement currently in § 170.315(g)(10)(vi) and proposed in § 170.315(j)(6)(iii) which requires support for revocation of a patient's authorization but does not require support for revocation of a clinician's authorization. We propose introducing this requirement in § 170.315(g)(10)(ii)(A)(*2*)(*i*) to support revocation of clinician authorizations to enable clinicians to have greater control

over their authorizations for applications to access patient data.

- We propose new requirements for authentication for dynamically registered patient-facing and user-facing apps in § 170.315(g)(10)(ii)(A)(*1*)(*ii*) and (*2*)(*ii*) respectively, with a compliance date on and after January 1, 2028. We refer readers to the ''Revision of Standardized API for Patient and Population Services to Support Dynamic Client Registration'' in section III.B.15.c of this proposed rule for additional details of the proposed § 170.315(g)(10) requirements for authentication and authorization of dynamically registered patient-facing apps and dynamically registered user-facing apps.
- The proposed revisions in § 170.315(g)(10)(ii)(A)(*1*)(*iii*) would require multi-factor authentication to be supported for patient-facing authentication on and after January 1, 2028, according to the requirements specified in the proposal at § 170.315(d)(13)(ii). We believe this update aligns with industry information security best practices, and that it is necessary to help better protect electronic health information. See the proposal for updating § 170.315(d)(13) and referencing § 170.315(d)(13)(ii) across certain certification criteria with authentication use cases at section III.B.17.

We propose to reorganize as part of § 170.315(g)(10)(ii)(B) the text for the current requirements for single patient data response currently in § 170.315(g)(10)(i)(A) and single patient supported search operations requirements currently in § 170.315(g)(10)(ii)(A), with proposed subparagraphs as follows:

- The proposed language in § 170.315(g)(10)(ii)(B)(*1*) maintains the existing requirements for data response and search support but simplifies the language by consolidating references to implementation guides. As part of our revisions, we propose to no longer explicitly mention the requirement in the API certification criteria language regarding ''mandatory'' and ''must support'' because this was done for emphasis in our prior rulemaking and, we believe, consistent with long standing Program policy, that when we adopt standards and implementation specifications that all requirement aspects of those need to be addressed for conformance purposes. Additionally, to reflect our policy interests to advance imaging availability as described in section III.B.6, we propose to also include support for imaging links in § 170.315(g)(10)(ii)(B)(*1*) indicating that imaging links must be supported as part of data response and search requirements on and after January 1, 2028.
- We also propose in § 170.315(g)(10)(ii)(B)(*2*) that on and after January 1, 2028, support for the issuance of verifiable health records as specified by the requirements in proposed § 170.315(j)(22) be supported. We propose requiring support for verifiable health records in § 170.315(g)(10)(ii)(B)(*2*) to support the ability for patients to access their immunization and infectious disease-related laboratory test information in a format that is easily portable and verifiable by third parties, which is the underlying benefit of the SMART Health Card standard proposed as part of § 170.315(j)(22).
- Proposed § 170.315(g)(10)(ii)(B)(*3*) requires on and after January 1, 2028, support for subscriptions as a server for patient-facing apps and user-facing apps according to the requirements specified in § 170.315(j)(23). We refer readers to subsequent section III.B.19.e for additional details about this proposal.

c. Proposed Revisions for System Access

We propose reorganizing under § 170.315(g)(10)(iii) the data response requirements currently in § 170.315(g)(10)(i)(B), supported search operations requirements currently in § 170.315(g)(10)(ii)(B), secure connection requirements in § 170.315(g)(10)(iv)(B), and authentication and authorization for system scopes requirements currently in § 170.315(g)(10)(v)(B). We believe these proposals will make it more efficient to understand the requirements necessary to support data retrieval for multiple patients' data. Specifically, we propose to revise § 170.315(g)(10)(iii) to be called ''*System access*'' and include the following paragraphs.

- We propose to organize authentication and authorization requirements for system access under the paragraph in § 170.315(g)(10)(iii)(A). We propose to add a paragraph in § 170.315(g)(10)(iii)(A)(*1*) which, by reference to the proposed certification criterion in § 170.315(j)(7), maintains requirements for secure connection currently in § 170.315(g)(10)(iv)(B) and authentication and authorization for system scopes in accordance with the ''SMART Backend Services: Authorization Guide'' currently in § 170.315(g)(10)(v)(B). We do not include specific mention of ''secure connection'' in the proposed paragraphs in § 170.315(g)(10)(iii)(A)(*1*) or § 170.315(j)(7) since we believe it is redundant as the referenced implementation guides already include such requirements for secure connections. The proposed paragraph in § 170.315(g)(10)(iii)(A)(*1*) maintains the existing system authentication and authorization requirements currently in § 170.315(g)(10)(v)(B) by referencing the proposed § 170.315(j)(7) certification criterion. Proposing to require conformance to the proposed § 170.315(j)(7) certification criterion maintains the requirements for SMART Backend Services while using consistent language across API certification criteria in the Program. The § 170.315(j)(7) certification criterion also facilitates reference to the updated location of the SMART Backend Services specification, which has been moved from the Bulk Data Access guide to the SMART App Launch guide in subsequent versions of those guides. We also propose to include language in § 170.315(g)(10)(iii)(A)(*1*) which clarifies that authentication and authorization for system access in accordance with SMART Backend Services is only required for functionally registered system apps.
- Proposed § 170.315(g)(10)(iii)(A)(*2*) would support the dynamic registration proposal described in section III.B.15.c of this proposed rule to support authentication and authorization of dynamically registered system apps. The paragraph in § 170.315(g)(10)(iii)(A)(*2*) describes the new proposed requirements to support authentication and authorization for dynamically registered system apps according to the ''Business-to-Business'' section of the UDAP Security IG v1 proposed in § 170.215(o) and proposes that a Health IT Module certifying to § 170.315(g)(10) must support the specified sections of the UDAP Security IG v1 on and after January 1, 2028 for system apps dynamically registered using the capabilities in proposed § 170.315(g)(10)(i)(B). We refer readers to the ''Revision of Standardized API for Patient and Population Services to Support Dynamic Client Registration'' in section III.B.15.c of this proposed rule for additional details of the proposed § 170.315(g)(10) requirements for authentication and authorization of dynamically registered system apps.
- We propose to organize system information access requirements under proposed paragraph § 170.315(g)(10)(iii)(B). We propose to maintain the data response requirements currently in § 170.315(g)(10)(i)(B) and include those requirements in proposed § 170.315(g)(10)(iii)(B)(*2*) and (*i*). We note that the existing supported search operations requirements at current § 170.315(g)(10)(ii)(B) are not applicable

to the export of multiple patients' data according to the Bulk Data Access implementation guide adopted under § 170.215(d), since search requests are not distinct from the data export requests as defined in that guide. As a result, we propose to remove the existing requirements language currently in § 170.315(g)(10)(ii)(B) but do not anticipate any change to the substance of the § 170.315(g)(10) certification criterion requirements given such requirements are subsumed by the data response requirements proposed in § 170.315(g)(10)(iii)(B)(*2*) and (*i*). The proposed language in § 170.315(g)(10)(iii)(B)(*2*) and (*i*) maintains the existing requirements for data response but simplifies the language by removing redundant language for requirements already required through reference to implementation guides and thus as we noted above, we have removed the explicit reference to ''mandatory'' and ''must support'' in this revised paragraph. Additionally, to reflect our policy interests to advance imaging availability as described in section III.B.6, we propose to also include support for imaging links in § 170.315(g)(10)(iii)(B)(*2*) and (*i*) indicating that imaging links must be supported as part of data response requirements for multiple patients on and after January 1, 2028. The requirements as proposed at and under § 170.315(g)(10)(iii)(B)(*2*) are rephrased such that the Bulk Data Access implementation guide features required for the § 170.315(g)(10) certification criterion (*e.g.,* group export) are explicitly enumerated in the criterion instead of in the reference to Bulk Data Access implementation guide in § 170.215(d). Also, to accommodate the distinct proposal to support the ''_type'' query parameter in § 170.315(g)(10) described in section III.B.14 of this rule, we propose adding paragraph § 170.315(g)(10)(iii)(B)(*2*)(*ii*) indicating that parameter must be supported. Both the ''_type'' query parameter and use of the parameter to support bulk data retrieval of imaging links would need to be supported on and after January 1, 2028.We propose that the paragraph in § 170.315(g)(10)(iii)(B)(*1*) requires support to respond to requests from system apps for patient data consistent with the search criteria included in the FHIR standard adopted in § 170.215(b) and one of the US Core IGs as adopted in § 170.215(b)(1) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 and, on and after January 1, 2028, imaging links. We refer readers to subsequent section III.B.19.e for additional details about this proposal. Proposed § 170.315(g)(10)(iii)(B)(*3*) requires on and after January 1, 2028, support for subscriptions as a server for system apps according to the requirements specified in § 170.315(j)(23). We refer readers to subsequent section III.B.19.e for additional details about this proposal.

d. Other Restructured Requirements

We propose to continue to require the token introspection requirements currently in § 170.315(g)(10)(vii) by moving such requirements language to the proposed § 170.315(j)(6) and (7) API certification criteria, and then referencing those criteria directly or indirectly where appropriate in the § 170.315(g)(10) certification criterion. The existing token introspection requirements apply to tokens issued for both patient and user scopes, and system scopes. Thus, we propose in § 170.315(g)(10)(ii)(A)(*1*)(*i*) to continue to require token introspection for tokens issued to patient-facing apps by referencing § 170.315(j)(9), which references § 170.315(j)(6). Next, we propose in § 170.315(g)(10)(ii)(A)(*2*)(*i*) to continue to require token introspection for user-facing apps by referencing § 170.315(j)(10), which references § 170.315(j)(6). Next, we propose in § 170.315(g)(10)(iii)(A)(*1*) to continue to require token introspection for system apps by referencing § 170.315(j)(7). Furthermore, we propose a new requirement in § 170.315(g)(10)(iii)(A)(*2*), by requiring conformance to § 170.315(j)(8) on and after January 1, 2028, to require token introspection according to the SMART App Launch implementation guide for dynamically registered system apps on and after January 1, 2028.

Lastly, we propose to move the API documentation requirements currently required in § 170.315(g)(10)(viii) to the API Conditions and Maintenance of Certification requirements in § 170.404(a)(2)(i), which would result in this paragraph no longer being part of § 170.315(g)(10) as part of the overall revision to this certification criterion. We do not intend to introduce new documentation requirements for the § 170.315(g)(10) certification criterion with this proposal. Instead, the goal of this proposal is to consolidate API documentation requirements across the Program where possible as described in additional detail in section III.B.20.d. We seek comment on the proposed revisions we have discussed for § 170.315(g)(10).

e. Proposed Requirements for System Read and Search API, Subscriptions, and Workflow Triggers for Decision Support Interventions

We propose several new requirements for the Standardized API for Patient and Population Services certification criterion in § 170.315(g)(10) to support enhanced interoperability and advanced workflows to overall reduce developer burden and barriers to accessing and utilizing patient health information. We propose support for a ''Read and search API'' for system access in § 170.315(g)(10)(iii)(B)(*1*), HL7 FHIR subscriptions for patient and user access in § 170.315(g)(10)(ii)(B)(*3*) and system access in § 170.315(g)(10)(iii)(B)(*3*), and workflow triggers for decision support interventions in § 170.315(g)(10)(iv), as described further below.

We previously only required Health IT Modules certified to § 170.315(g)(10) to support the ''Bulk FHIR API'' for system access, and only required the US Core IG read and search capabilities for patient and user scopes. We propose to include a read and search API according to the ''US Core Server CapabilityStatement'' for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 in § 170.315(g)(10)(iii)(B)(*1*) in order to explicitly require that certified Health IT Modules support system applications to perform read and search operations for patient health information using a standardized API. The proposal includes optional support for imaging links requests as of the effective date of the rule. On and after January 1, 2028, requests for imaging links must be supported.

We propose support for HL7 FHIR subscriptions as part of the Standardized API for Patient and Population Services for patient and user access in § 170.315(g)(10)(ii)(B)(*3*) and for system access in § 170.315(g)(10)(iii)(B)(*3*). The proposals require Health IT Modules to support subscriptions as a server according to the requirements specified in § 170.315(j)(23), which includes several infrastructure capabilities to support HL7 FHIR Subscriptions and a list of HL7 FHIR Resources that must be supported for subscription notifications and accompanying data elements that must be supported for subscription filtering. The proposed certification criterion in § 170.315(j)(23) is discussed further in this rule in section III.B.15.b.iii.

We propose to require support for workflow triggers for decision support interventions under proposed

§ 170.315(g)(10)(iv). We propose that the Health IT Module must support capabilities in § 170.315(j)(20) (where we have proposed to adopt the ''workflow triggers for decision support interventions'' certification criterion) to enable workflow triggers to call decision support services, including support for ''patient-view'' and ''order-sign'' CDS Hooks according to at least one of the versions of the implementation specification adopted in § 170.215(f)(1). We propose support for ''patient-view'' and ''order-sign'' because these CDS Hooks are at maturity level ''5—Mature'' according to the CDS Hooks IG and can be used to support a wide variety of workflow processes. We further clarify and propose in 170.315(g)(10)(iv) that developers may support workflow triggers for decision support interventions for the time period up to and including December 31, 2027 and must support workflow triggers for decision support interventions on and after January 1, 2028.

20. Patient, Provider, and Payer APIs

In this section, we propose to adopt a set of certification criteria in § 170.315(g)(30)–(36) to support data exchange between health care payers, providers, and patients. These proposed certification criteria would enable the exchange of data including clinical and coverage information, drug formulary information, and prior authorization information, between patients, providers, and payers as appropriate to each exchange. These proposed certification criteria are based on a series of recent policies finalized by CMS which we describe in detail in the following section. If finalized, these certification criteria would be available for health IT developers (which may include payers and other developers providing technology to payers) seeking voluntary certification for health IT products supporting these use cases.

a. Background on CMS Interoperability Rulemaking

On May 1, 2020, the ''Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage (MA) Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers'' final rule (85 FR 25510) was published in the **Federal Register** (hereinafter referred to as the ''CMS Interoperability and Patient Access Final Rule''). CMS required impacted payers [184] to implement and maintain a FHIR-based Patient Access API to allow patients, through the health application of their choice, to easily access their claims and encounter information as well as clinical data, including laboratory results, and provider remittances and enrollee cost-sharing pertaining to such claims, if maintained by the impacted payer (85 FR 25559). CMS also required impacted payers to implement a Provider Directory API to make available information such as contracted provider names, addresses, and phone numbers (85 FR 25563).

On February 8, 2024, the ''Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program'' (CMS Interoperability and Prior Authorization Final Rule) was published in the **Federal Register** (89 FR 8758). Final policies in this rule included: expanding the content available via the existing Patient Access API to include information about prior authorizations; requiring impacted payers to implement and maintain a Provider Access API to make patient data available to in-network providers with whom the patient has a treatment relationship; and requiring impacted payers build and maintain a Payer-to-Payer API to exchange patient data when a patient moves between payers or has concurrent payers. CMS also required impacted payers to implement and maintain a Prior Authorization API to facilitate electronic prior authorization processes. Finally, the rule added electronic prior authorization measures to the Medicare Promoting Interoperability Program and the MIPS Promoting Interoperability performance category.

[184] For the purposes of the CMS Interoperability and Patient Access and Interoperability and Prior Authorization Final Rules discussed in this section, impacted payers include Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

In the CMS Interoperability and Patient Access Final Rule (85 FR 25510 through 25640) and the CMS Interoperability and Prior Authorization Final Rule (89 FR 8758 through 8988), CMS requires impacted payers to use certain standards and implementation guides which ONC has adopted in § 170.215, as well as the USCDI standard in § 170.213. Specifically, CMS has finalized technical requirements for the following APIs: Patient Access API (85 FR 25558 through 25559, 89 FR 8784 through 8787), Provider Access API (89 FR 8817 through 8820), Payer-to-Payer API (89 FR 8855 through 8856), Prior Authorization API (89 FR 8897 through 8901), and the Provider Directory API (85 FR 25563 through 25564). In the CMS Interoperability and Prior Authorization Final Rule, CMS also recommended a number of implementation guides that may be used to support effective implementation of the required payer APIs (89 FR 8945).

b. Proposal Overview

We propose certification criteria below in § 170.315(g)(30)–(36) for Health IT Modules that can be used to support more effective exchange of clinical, coverage, and prior authorization information. The proposed certification criteria, if finalized, would support the availability of health IT that can enable payers and health care providers to meet requirements established in the Interoperability and Patient Access Final Rule (85 FR 25522 through 25569) and the Interoperability and Prior Authorization Final Rule (89 FR 8768 through 8946). As part of the proposals below, we include further discussion of how each proposed certification criterion would support the availability of information and enable functionality CMS has identified as part of corresponding requirements. We intend to continue to work with CMS in the future to ensure Health IT Modules certified to the proposed criteria in § 170.315(g)(30)–(36) enable efficient and effective support for CMS policies.

In general, we believe that use of technology meeting these certification criteria would help to enable exchange of information that promotes a more effective marketplace, increases competition, and provides benefits to patients, including: increased consumer choice, improved outcomes in healthcare services, and more robust care coordination through improved availability and exchange of health care provider information. Increased electronic exchange and automation of such information, as supported by the proposed certification criteria, would

enable patients to better manage their own care, allow providers to make more timely and informed treatment decisions, and reduce costs for both payers and providers by reducing the amount of manual intervention required in the exchange and authorization processes addressed by the proposed certification criteria.

These proposed certification criteria reference a set of API implementation specifications that ONC proposes to adopt, on behalf of the Secretary, in § 170.215(j), (k), (m), and (n).[185] These specifications are based upon HL7® FHIR® R4. In concert with CMS, ONC has led or participated in a variety of activities related to monitoring and evaluating the standards and implementation specifications identified in this proposed rule, utilizing available mechanisms for gathering input on these standards from stakeholders and experts. Several of these proposed implementation specifications were developed by the HL7® Da Vinci Project.[186] The Da Vinci Project is a private sector initiative that brings together payers, health IT developers, providers, and other public participants to facilitate the definition, design, and creation of use case specific reference implementations of solutions based upon the HL7 FHIR platform that involve managing and sharing clinical and administrative data between industry partners. Because the Da Vinci Project is aligned with HL7, solutions developed through the project may become industry standards. The Da Vinci Project's use case requirements, test scenarios, and test data, as well as the resulting implementation guides and reference implementations, are available without licensing requirements.

The proposed implementation specifications referenced in the proposed certification criteria in § 170.315(g)(30)–(36) include the required and recommended implementation specifications identified in CMS' finalized policies for payer API requirements (89 FR 8945). We propose to adopt current versions of the IGs that CMS recommended in the CMS Interoperability and Prior Authorization Final Rule and propose to require these IGs as part of the certification criteria proposed in § 170.315(g)(30)–(36). In the CMS Interoperability and Prior Authorization Final Rule, CMS discussed its approach to recommending, rather than requiring, certain IGs for payer APIs. CMS stated that its goal in recommending the specific IGs for each API was to provide directional guidance to the industry without locking payers into the versions available at the time of the CMS Interoperability and Prior Authorization proposed rule, due to the maturity of the versions available at that time (89 FR 8921). CMS sought to ensure that payers could use subsequent versions of those IGs without being restricted to those versions. CMS further stated that it intended to monitor IG development and would consider proposing to require versions of these IGs in future rulemaking (89 FR 8937).

We believe that proposing to adopt the current versions of the IGs recommended by CMS in the rulemaking described above is appropriate for the proposed certification criteria at this time. Adopting and specifying use of these IGs is necessary to ensure that Health IT Modules certified to the criteria proposed in this section are implemented consistently and enable interoperable exchange of information. We also note that adoption of these IGs would support CMS policies established in their Interoperability and Prior Authorization Final Rule. Furthermore, if the adoption of these IGs is finalized, we would review and potentially approve future versions of these standards under the SVAP for voluntary use in the Program as they become available. The flexibility provided under the SVAP would ensure that developers are able to voluntarily update to later versions of these standards as future improvements are made, without waiting for updated versions to be proposed and finalized in regulation. In addition, we will continue to work with CMS to identify updated versions of these standards for potential future adoption in regulation at appropriate intervals so that the adopted versions of standards are the most up-to-date available and are feasible for real-world implementation.

The proposed certification criteria in § 170.315(g)(30)–(36) also incorporate certification criteria for modular API capabilities proposed in § 170.315(j) in section III.B.17 of this proposed rule, including capabilities for registration (§ 170.315(j)(1)–(2)), authentication and authorization (§ 170.315(j)(5)–(7)), workflow triggers for decision support interventions (§ 170.315(j)(20)–(21)), and subscriptions (§ 170.315(j)(23)–(24)).

Below, we describe each certification criterion and our intent to certify Health IT Modules to these certification criteria to support interoperability. However, we note that the certification of any Health IT Module by a health IT developer is voluntary. The proposals in this proposed rule would not establish requirements for health IT beyond those Health IT Modules submitted for certification for these criteria under the Program, nor does the availability of these certification criteria require any individual or entity to use certified health IT, including payers subject to the CMS requirements. Our goal in proposing these certification criteria and the related implementation specifications is to support health IT developers building these capabilities (and customers implementing them) in a manner that is consistent with nationally recognized standards and supports testing and conformance to these standards through the ONC Health IT Certification Program. ONC's adoption of certification criteria, standards, and implementation specifications are part of an effort to advance a set of minimum technical requirements, increase the availability of health IT leveraging such requirements, and provide the healthcare community with an improved, interoperable health IT infrastructure.

We reiterate that, if finalized, certification to these criteria would be available for health IT developers (which may include payers and other developers providing technology to payers) seeking voluntary certification and any requirements for a certification criterion are only required in the sense that they are necessary to achieve certification. ONC does not establish requirements for whether and in what ways patients, health care providers, payers or others use health IT. Instead, we enable the certification of Health IT Modules that may support a wide range of users. In this way, the Program helps to advance standards for certified Health IT Modules and increases the availability of interoperable health IT across healthcare and health related use cases.

Finally, we note that CMS has not proposed to require that impacted payers subject to the API requirements in the CMS Patient Access and Interoperability and CMS Interoperability and Prior Authorization Final Rules obtain or implement Health IT Modules certified to the criteria in this proposed rule. We also note that CMS has not identified health IT certified to the ''prior authorization API—provider'' criterion proposed below in § 170.315(g)(34) as necessary to complete the finalized electronic prior

[185] For a more detailed discussion of APIs generally, we refer readers to the Application Programming Interfaces Condition of Certification and Maintenance of Certification preamble language in the ONC Cures Act Final Rule at 85 FR 25739.

[186] For more information about the Da Vinci Project, please visit *https://www.hl7.org/about/davinci/*.

authorization measures in the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of MIPS. If this certification criterion is finalized, we would work with CMS on appropriate updates to the Medicare Promoting Interoperability Program and the MIPS Promoting Interoperability performance category to identify health IT certified to this criterion as an element of CEHRT necessary to report on the electronic prior authorization measures. As CMS noted in the Interoperability and Prior Authorization Final Rule, use of health IT certified to support electronic prior authorization transactions can help to ensure that the actions associated with these measures are executed in a consistent fashion across the health care providers participating in these programs (89 FR 8802).

c. Proposed Certification Criteria

We propose to adopt the following new certification criteria for Patient, Provider, and Payer APIs:

i. Patient Access API (§ 170.315(g)(30))

We propose to adopt a ''patient access API'' certification criterion in § 170.315(g)(30) to specify requirements for Health IT Modules that can enable patients to access their health and administrative information by using a health application of their choice. While many of the requirements introduced in the ONC Cures Act Final Rule (85 FR 25642) expanded patient access to clinical information contained within health IT, such as EHRs, broadening this electronic access to include coverage and payer information can help expand the information available to help patients with decision-making.

We propose in § 170.315(g)(30)(i) to require support for two registration pathways for a Health IT Module certified to the ''patient access API'' criterion: a functional registration pathway for applications that are unable to meet the requirements for dynamic registration and a dynamic registration pathway for applications that can support automated, scalable registration. We propose in § 170.315(g)(30)(i)(A) that the Health IT Module must support functional registration according to the requirements included in § 170.315(j)(1) whereby confidential and public apps can register using a non-standardized method. We propose in § 170.315(g)(30)(i)(B) to require the Health IT Module to support a dynamic registration pathway for confidential apps according to the requirements in § 170.315(j)(2).

We propose in § 170.315(g)(30)(ii) to require authentication and authorization for patient access. To enable patients to authorize access to patient data by functionally and dynamically registered apps, we propose in § 170.315(g)(30)(ii)(A) that the Health IT Module must support authentication and authorization according to the SMART App Launch IG during the process of granting access to patient data, according to the requirements in § 170.315(j)(9). To enable authentication of dynamically registered apps, we propose in § 170.315(g)(30)(ii)(B) that the Health IT Module must support asymmetric certificate-based authentication according to the requirements in § 170.315(j)(5) for patient-facing apps dynamically registered using the capabilities in § 170.315(g)(30)(i)(B). We refer readers to the proposals in sections III.B.16. (''New Certification Criteria for Modular API Capabilities'') and III.B.15. (''New Requirements to Support Dynamic Client Registration Protocol in the Program'') for more information about our proposed certification criteria in § 170.315(j) and proposal for dynamic registration respectively.

We propose later in this section that Certified API Developers with API technology certified to the criterion in § 170.315(g)(30) would need to adhere to the API Condition and Maintenance of Certification requirements proposed in § 170.404. This would mean that such developers would need to publish trust community information necessary for dynamic registration, as proposed in § 170.404(b)(2)(iii).

We propose in § 170.315(g)(30)(ii)(C) to require multi-factor authentication for patient-facing authentication on and after January 1, 2028, as proposed in § 170.315(d)(13)(ii) in section III.B.17. of this proposed rule. We believe this update is in line with industry information security best practice for an important authentication use case in health IT and that it is necessary to help better protect EHI.

To make information available about a payer's list of preferred drugs, we propose in § 170.315(g)(30)(iii) that the Health IT Module must publish information regarding the payer's drug formulary information according to at least one of the versions of the implementation specification adopted in § 170.215(m), including the requirements described in the ''US Drug Formulary Server Capability Statement.'' We propose to adopt the HL7 FHIR® Da Vinci—Payer Data Exchange (PDex) US Drug Formulary Implementation Guide, Version 2.0.1—STU2 (PDex US Drug Formulary IG) [187] in § 170.215(m)(1) and incorporate it by reference in § 170.299. We propose to adopt this implementation specification under PHSA section 3004 and make it available for HHS use. This implementation specification can enable consumers, members, and patients to understand the costs and alternatives for drugs that have been prescribed, and to compare their drug costs across different insurance plans. If we adopt subsequent versions of the PDex US Drug Formulary IG under the paragraph in § 170.215(m), our proposals that require the use of at least one of the versions of the implementation specification adopted in § 170.215(m) would enable health IT developers to use any version adopted at this location, unless we specify an ''expiration'' date which indicates a certain version of the specification may no longer be used after that date.

To support the exchange of formulary data that is integrated with protected health information (PHI) or personally identifiable information (PII), such as enabling a payer to provide personalized information to the patient based on their medications, we propose in § 170.315(g)(30)(iii)(A) that the Health IT Module must provide support for the ''Authenticated API'' according to at least one of the versions of the implementation specification adopted in § 170.215(m) (where we have proposed to adopt the PDex US Drug Formulary IG Version 2.0.1—STU2) and the requirements proposed in § 170.315(g)(30)(i) and (ii) related to registration as well as authentication and authorization. To support the exchange of formulary data that is publicly available, and which does not contain PHI or PII, we propose in § 170.315(g)(30)(iii)(B) that the Health IT Module must provide support for an ''Unauthenticated API'' according to at least one of the versions of the implementation specification adopted in § 170.215(m).

We propose in § 170.315(g)(30)(iv) requirements for a Health IT Module certified to the ''patient access API'' criterion to support access to patient health, coverage, and claims information. We propose in § 170.315(g)(30)(iv)(A) that the Health IT Module must allow patients to access and share clinical and coverage information via a standardized API(s) according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2). Under this paragraph, in § 170.215(k)(2)(i), we propose to adopt the HL7 FHIR Da Vinci

[187] *See https://hl7.org/fhir/us/davinci-drug-formulary/STU2.0.1/.*

Payer Data Exchange (PDex) Implementation Guide Version 2.0.0—STU2 [188] and incorporate it by reference in § 170.299. We propose to adopt this implementation specification under PHSA section 3004 and make it available for HHS use. This implementation specification enables a payer to create a member's health history using clinical resources based on US Core profiles. If we adopt subsequent versions of the PDex IG in § 170.215(k)(2), our proposals that require use of at least one of the versions of the implementation specification adopted in § 170.215(k)(2) would enable health IT developers to use any version adopted at this location, unless we specify an ''expiration'' date which indicates a certain version of the specification may no longer be used after that date.

We note that a version 2.1.0 of the PDex IG is currently under development and available for interested parties to review.[189] We propose as an alternative, to adopt PDex IG version 2.1.0 if the standard is balloted and published before the issuance of the HTI–2 Final Rule. We note several important enhancements to the PDex IG version 2.1.0 from 2.0.0—STU2 to align with the Interoperability and Patient Access Final Rule (85 FR 25522 through 25569) and the Interoperability and Prior Authorization Final Rule (89 FR 8768 through 8946). For example, version 2.1.0 supports US Core 6.1.0, which supports USCDI v3, as well as drops required support for aspects of prior authorization that are viewed as unnecessary or complicating to successful execution of the transaction in version 2.0.0 of the PDex IG. Version 2.1.0 also includes an important use case for bulk data access based on the finalization of the Bulk Data Access IG as a required standard under the Payer API requirements finalized in CMS' rules.

We believe that continued alignment among industry, government, and standards development organizations involved with the payer data exchange use cases is necessary and we believe that if PDex IG version 2.1.0 is balloted and published before issuance of the HTI–2 Final Rule, adoption of version 2.1.0 would support such alignment.

In order to enable patient access to information and allow patients to incorporate their data into apps or systems of their choice with minimal effort, we propose in § 170.315(g)(30)(iv)(A)(*1*) that the Health IT Module must support the ability for patients to authenticate and share information with an application, service, or health plan according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2). Specifically, we propose in § 170.315(g)(30)(iv)(A)(*1*)(*i*) that the Health IT Module must support the requirements associated with the ''OAuth2.0 or SMART-on-FHIR Member-authorized Exchange'' exchange method, including the requirements in the section ''OAuth and FHIR API.'' We propose in § 170.315(g)(30)(iv)(A)(*1*)(*ii*) that the Health IT Module must support the requirements included in the ''PDEX Server CapabilityStatement'' and the HL7 FHIR Profiles, Resources, and operations included in Section 4.5.4 ''CapabilityStatement'' [190] according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2).

Finally, in § 170.315(g)(30)(iv)(A)(*1*)(*iii*) we propose that the Health IT Module must support the capabilities described in ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) (where we have adopted US Core IG version 3.1.1, which expires on January 1, 2026, US Core IG version 6.1.0, which we propose will expire on January 1, 2028, and where we propose to adopt US Core IG version 7.0.0). We further propose that the Health IT Module must support the capabilities in ''US Core Server CapabilityStatement'' for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 (where we have adopted USCDI version 1, which expires on January 1, 2026, USCDI version 3, which we propose will expire on January 1, 2028, and where we propose to adopt USCDI version 4). We note that while most of the USCDI and US Core requirements are met through the PDEX Server CapabilityStatement requirements in § 170.315(g)(30)(iv)(A)(*1*)(*iii*), we have added this requirement to ensure the Health IT Module supports availability of all of the data classes and data elements in at least one of the versions of the USCDI adopted in § 170.213.

We note that in section III.B.6 of this proposed rule, ''New Imaging Requirements for Health IT Modules,'' we propose to revise certification criteria for ''transitions of care'' in § 170.315(b)(1); ''application access—all data request'' in § 170.315(g)(9); and ''standardized API for patient and population services'' in § 170.315(g)(10) by adding new provisions to include support of a link to diagnostic imaging. The CMS API requirements for impacted payers, which we are seeking to support with the proposed certification criteria in § 170.315(g)(30)–(36), reference the versions of the USCDI available in § 170.213, which do not include imaging links as a data element at this time. Therefore, in order to maintain alignment with current CMS requirements for impacted payers, we have not proposed to separately require support for imaging links by a Health IT Module certified to the proposed certification criteria in § 170.315(g)(30), (32), and (33). We request comment on our decision to not propose to include imaging links, and whether interested parties believe a requirement to support imaging links, in a manner similar to the proposed requirements for the certification criteria mentioned above, would be appropriate and desirable for the proposed certification criteria in § 170.315(g)(30), (32), and (33).

We propose in § 170.315(g)(30)(iv)(B) that the Health IT Module must allow patients to access their claims information via a standardized API(s) according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1). In § 170.215(k)(1)(i), we propose, independent of the certification criterion proposal, to adopt the HL7 FHIR Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) Implementation Guide version 2.0.0—STU 2 [191] and incorporate it by reference in § 170.299. We propose to adopt this implementation specification under PHSA section 3004 and make it available for HHS use. This implementation specification supports providing a set of resources that payers can display to consumers, primarily financial (claims and encounter) data, with some limited associated clinical data. If we adopt subsequent versions of the CARIN IG for Blue Button® in § 170.215(k)(1), our proposals that require the use of at least one of the versions of the implementation specification adopted in § 170.215(k)(1) would enable health IT developers to use any version adopted at this location, unless we specify an ''expiration'' date

[188] *See https://hl7.org/fhir/us/davinci-pdex/STU2/.*

[189] *See https://build.fhir.org/ig/HL7/davinci-epdx/.*

[190] For more information, *see https://hl7.org/fhir/us/davinci-pdex/STU2/introduction.html#capabilitystatement.*

[191] *See https://hl7.org/fhir/us/carin-bb/.*

which indicates a certain version of the specification may no longer be used after that date.

We propose in § 170.315(g)(30)(iv)(B)(*1*) that the Health IT Module must support the ''Authentication and Authorization Requirements'' section of at least one of the versions of the implementation specification adopted in § 170.215(k)(1) (where we have proposed to adopt the CARIN IG for Blue Button® version 2.0.0—STU 2). These requirements establish authentication and privacy requirements to protect patient health information. We propose in § 170.315(g)(30)(iv)(B)(*2*) that the Health IT Module support the requirements described in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

We request comments on this proposal.

Support for CMS Requirements

The ''patient access API'' certification criterion proposed in § 170.315(g)(30), if finalized, would support the availability of certified health IT that can enable impacted payers [192] to meet CMS requirements to implement and maintain a Patient Access API, as specified in 42 CFR 422.119, 431.60, 457.730, 438.242(b)(5), and 457.1233(d) and 45 CFR 156.221. Specifically, a Health IT Module certified to the proposed ''patient access API'' would facilitate access to data held by the payer, including: adjudicated claims (including cost); encounters with capitated providers; provider remittances; enrollee cost-sharing; all data classes and data elements included in a version of the USCDI standard at 45 CFR 170.213, formularies or preferred drug lists, and certain information about prior authorizations requests and decisions, as finalized in the CMS Interoperability and Patient Access Final Rule (85 FR 25542) and the CMS Interoperability and Prior Authorization Final Rule (89 FR 8784). We further note that we have proposed in section III.B.20.d. of this proposed rule to apply the API Conditions of Certification § 170.404(a), including transparency requirements in § 170.404(a)(2), and certain API Maintenance of Certification requirements in § 170.404(b), to the proposed ''patient access API'' and other criteria. These Conditions of Certification would, among other provisions, align with the API requirements finalized by CMS related to ''Documentation requirements for APIs,'' for instance, the requirement at 42 CFR 422.119(d) for MA organizations.

ii. Provider Access API—Client (§ 170.315(g)(31)) and Provider Access API—Server (§ 170.315(g)(32))

We propose to adopt ''provider access API—client'' and ''provider access API—server'' certification criteria in § 170.315(g)(31) and § 170.315(g)(32), respectively. The proposed certification criteria would enable a health care provider to access information on patients' claims, including information about the patient's encounters, providers, organizations, locations, dates of service, diagnoses (conditions), procedures and observations. The proposed certification criteria could further enable access by a health care provider to clinical information maintained by the payer from sources other than claims, such as: laboratory results, clinical data from documents formatted in accordance with the Common Clinical Data Architecture (C–CDA), information from admit, discharge, and transfer (ADT) messages, information received from immunization registries, and information related to medications from pharmacy networks. Such information can provide a more complete clinical profile for the provider, as well as allow the provider to make appropriate treatment decisions based on both the clinical information and the patient's individual coverage information.

We propose that a Health IT Module certified to the ''provider access API—client'' in § 170.315(g)(31) support specified capabilities to enable a provider to request and receive patient clinical and coverage information from a payer and receive and process the response. We propose in § 170.315(g)(31)(i) that the Health IT Module must support the ability to request patient history according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2).

Under § 170.315(g)(31)(ii), we propose that the Health IT Module must support specified API interactions as a client. First, in § 170.315(g)(31)(ii)(A) we propose that the Health IT Module support the capability to read and search the API. Specifically, in § 170.315(g)(31)(ii)(A)(*1*) we propose that the Health IT Module support the ability to interact with a ''PDEX Server'' as a client including support for all the corresponding client capabilities for requirements described in the ''PDEX Server CapabilityStatement'' and the HL7 FHIR Profiles, Resources, and operations included in Section 4.5.4 ''CapabilityStatement,'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2). In § 170.315(g)(31)(ii)(A)(*2*) we propose that the Health IT Module must support all the corresponding client capabilities for requirements included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1) (where we have proposed to adopt the CARIN IG for Blue Button® version 2.0.0—STU 2). In § 170.315(g)(31)(ii)(A)(*3*) we propose that the Health IT Module must support the corresponding client capabilities described in ''US Core Server CapabilityStatement'' according to an implementation specification adopted in § 170.215(b)(1) (where we have adopted US Core IG versions 3.1.1, which expires on January 1, 2026, US Core IG version 6.1.0, and proposed to adopt the US Core IG version 7.0.0) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 (where we have adopted USCDI version 1, which expires on January 1, 2026, USCDI version 3, which we propose will expire on January 1, 2028, and where we propose to adopt USCDI version 4).

To support the transfer of information on groups of patients, we propose in § 170.315(g)(31)(ii)(B) that the Health IT Module must support the ability to request and receive information as a client according to at least one of the versions of the standard adopted in § 170.215(a) (where we have adopted FHIR® R4) and at least one of the versions of the implementation specification adopted in § 170.215(d) (where we have adopted the Bulk Data Access IG v1.0.0—STU 1, which we have proposed for expiration on January 1, 2028, and the Bulk Data Access IG v2.0.0—STU 2) for each of the data included in § 170.315(g)(31)(ii)(A), as described above.

Additionally, we propose for the time period up to and including December 31, 2027, the Health IT Module must meet either the requirements specified in paragraph (g)(31)(ii)(B)(*1*) (proposed

[192] As noted above, for the purposes of the CMS Interoperability and Patient Access and Interoperability and Prior Authorization Final Rules discussed in this section, impacted payers include Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

to be the ''GroupLevelExport'' operation) or both (*1*) and (*2*) (proposed to be the ''_type'' query parameter for each of the data included in 170.315(g)(31)(ii)(A)) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). We propose that on and after January 1, 2028, the Health IT Module must meet the requirements specified in paragraph (g)(31)(ii)(B)(*1*) and (*2*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). For further discussion of these proposed requirements, which we have also proposed to include in other certification criteria that reference the Bulk Data Access IG, we refer readers to section III.B.14 of this proposed rule.

We propose in § 170.315(g)(31)(iii) that the Health IT Module must support the ability to receive, parse, and write patient health history and coverage information to the Health IT Module for the following information. For clinical and coverage information, we propose in § 170.315(g)(31)(iii)(A) to include all FHIR Profiles and Resources included in the ''PDEX Server CapabilityStatement'' and the FHIR Profiles and Resources included in the Section 4.5.4 ''FHIR CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2). In § 170.315(g)(31)(iii)(B) we propose to include the information included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1) (where we have proposed to adopt CARIN IG for Blue Button® version 2.0.0—STU 2). Finally, in § 170.315(g)(31)(iii)(C) we propose to include the capabilities described in the ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) (where we have adopted US Core IG version 3.1.1, which expires on January 1, 2026, US Core IG version 6.1.0, which we propose will expire on January 1, 2028, and where we propose to adopt US Core IG version 7.0.0) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 (where we have adopted USCDI version 1, which expires on January 1, 2026, USCDI version 3, which we propose will expire on January 1, 2028, and where we propose to adopt USCDI version 4).

We propose that a Health IT Module certified to the ''provider access API—server'' certification criterion in § 170.315(g)(32) would support capabilities to enable providers to request and receive patient health history and coverage information from payers. Similar to the ''patient access API'' certification criterion proposed in § 170.315(g)(30), we propose to require support for two registration pathways for Health IT Modules certified to the criterion. We propose in § 170.315(g)(32)(i)(A) that the Health IT Module must support functional registration for confidential apps according to the requirements included in § 170.315(j)(1). We propose in § 170.315(g)(32)(i)(B) that the Health IT Module must support dynamic registration according to the requirements in § 170.315(j)(2).

We propose in § 170.315(g)(32)(ii) the authentication and authorization requirements for a Health IT Module certified to the ''provider access API—server'' criterion. We propose in § 170.315(g)(32)(ii)(A) that the Health IT Module must support the ability to authenticate and authorize an app during the process of granting access to patient data to users according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2) and at least one implementation specification adopted in § 170.215(c) (where we have adopted the SMART Application Launch Framework IG Release 1.0.0, which expires on January 1, 2026, the SMART App Launch IG Release 2.0.0, which we have proposed for expiration on January 1, 2028, and proposed to adopt the SMART App Launch IG Release 2.2.0). We propose in § 170.315(g)(32)(ii)(A)(*1*) that the Health IT Module must support asymmetric certificate-based authentication according to the requirements in § 170.315(j)(11) for user-facing apps dynamically registered using the capabilities in § 170.315(g)(32)(i)(B).

We propose authentication and authorization requirements for system access in § 170.315(g)(32)(ii)(B), including that the Health IT Module must support the ability to authenticate and authorize an app during the process of granting access to patient data to system apps according to at least one of the versions of the standard adopted in § 170.215(a) (where we have adopted FHIR R4) and at least one of the versions of the implementation specification adopted in § 170.215(d) (where we have adopted the Bulk Data Access IG v1.0.0—STU 1, which we have proposed for expiration on January 1, 2028, and proposed to adopt the Bulk Data Access IG v2.0.0—STU 2). We propose in § 170.315(g)(32)(ii)(B)(*1*) that the Health IT Module must support system authentication and authorization according to the requirements in § 170.315(j)(7) for system apps functionally registered using the capabilities in § 170.315(g)(32)(i)(A). We also propose in § 170.315(g)(32)(ii)(B)(*2*) the Health IT Module must support asymmetric certificate-based system authentication and authorization according to the requirements in § 170.315(j)(8) for system apps dynamically registered using the capabilities in § 170.315(g)(32)(i)(B).

We propose in § 170.315(g)(32)(iii) that the Health IT Module must support specified capabilities to allow a provider to request patient health history and coverage information from a payer and to receive a response. Specifically, we propose in § 170.315(g)(32)(iii)(A) that the Health IT Module must support the ability for a client to request patient health history, coverage, and claims information according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2). We propose in § 170.315(g)(32)(iii)(B) that the Health IT Module support the ability to identify patient clinical, coverage, and claims information based on the information provided by the client in 170.315(g)(32)(iii)(A).

We propose in § 170.315(g)(32)(iii)(C)(*1*) that the Health IT Module must support the requirements described in the ''PDEX Server CapabilityStatement'' and the HL7 FHIR Profiles and operations included in Section 4.5.4 ''CapabilityStatement'' via a standardized API according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2). We propose in § 170.315(g)(32)(iii)(C)(*2*) that the Health IT Module support claims information by supporting the requirements included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1) (where we have proposed to adopt CARIN IG for Blue Button® version 2.0.0—STU 2). We propose in § 170.315(g)(32)(iii)(C)(*3*) that the API must support the capabilities described in ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) (where we have

adopted the US Core IG versions 3.1.1, which expires on January 1, 2026, the US Core IG version 6.1.0, and proposed to adopt the US Core IG version 7.0.0) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 (where we have adopted USCDI Version 1, which expires on January 1, 2026, USCDI version 3, which we propose will expire on January 1, 2028, and where we propose to adopt USCDI version 4).

We propose in § 170.315(g)(32)(iii)(D) that the Health IT Module must support returning patient clinical, coverage, and non-financial claims and encounter information according to at least one of the versions of the implementation specification in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2) for each of the data included in § 170.315(g)(32)(iii)(C)(*1*), (*2*) and (*3*), as described above.

To support the transfer of information on groups of patients, we propose in § 170.315(g)(32)(iii)(E) that the Health IT Module must support responding to requests for patient data according to at least one of the versions of the standard adopted in § 170.215(a) (where we have adopted FHIR R4), and at least one of the versions of the implementation specification adopted in § 170.215 (d) (where we have adopted the Bulk Data Access IG v1.0.0—STU 1, which we have proposed for expiration on January 1, 2028, and the Bulk Data Access IG v2.0.0—STU 2) for each of the data included in § 170.315(g)(32)(C)(*1*), (*2*) and (*3*), as proposed above. For the time period up to and including December 31, 2027, we propose that the Health IT Module must meet either the requirements specified in (g)(32)(iii)(E)(*1*) (proposed to be the ''GroupLevelExport'' operation) or both (*1*) and (*2*) (proposed to be the ''_type'' query parameter for each of the data included in § 170.315(g)(32)(C), (D) and (E)), of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). On and after January 1, 2028, we propose the Health IT Module must meet the requirements specified in paragraph § 170.315(g)(32)(iii)(E)(*1*) and (*2*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

We request comments on this proposal.

Support for CMS Requirements

The ''provider access API—server'' certification criterion proposed in § 170.315(g)(32), if finalized, would support the availability of certified health IT that can enable impacted payers [193] to meet CMS requirements to implement and maintain a Provider Access API as specified in 42 CFR 422.121(a), 431.61(a), 457.731(a), 438.242(b)(7), and 457.1233(d) and 45 CFR 156.222(a). Specifically, a Health IT Module certified to the proposed ''provider access API—server'' criterion would facilitate access to data held by the payer, including: claims and encounter data (excluding provider remittances and patient cost-sharing information), all data classes and data elements derived from a version of the USCDI standard adopted at 45 CFR 170.213, and certain information about prior authorizations requests and decisions, as required in the CMS Interoperability and Prior Authorization Final Rule (89 FR 8817).

In addition, the proposed ''provider access API—client'' certification criterion in § 170.315(g)(31) would establish the requirements for APIs to facilitate a provider request for this information, to ensure that providers can use certified health IT to access the information made available through a payer's Provider Access API.

iii. Payer-to-Payer API (§ 170.315(g)(33))

We propose to adopt a ''payer-to-payer API'' certification criterion in § 170.315(g)(33) to specify requirements for Health IT Modules that can be used by payers to support electronic exchange between payer systems when patients transition between payers. Payer-to-payer data exchange that allows health data to follow the patient when they switch payers can enable improved coordination of care, increased patient empowerment, and reduced administrative burden.

Similar to the proposed ''provider access API—client'' and ''provider access API—server'' certification criteria, the proposed ''payer-to-payer API'' certification criterion would support the electronic request and sending of payer information related to both beneficiary coverage information and the clinical condition and care of the patient.

We propose two registration pathways for a Health IT Module certified to the proposed ''payer-to-payer API'' criterion. We propose in § 170.315(g)(33)(i)(A) that the Health IT Module must support registration for confidential apps according to the functional registration requirements in § 170.315(j)(1). We further propose in § 170.315(g)(33)(i)(B) that the Health IT Module must support dynamic registration according to requirements in § 170.315(j)(2).

We propose requirements for authentication and authorization in § 170.315(g)(33)(ii). In § 170.315(g)(33)(ii)(A) we propose that the Health IT Module must support system authentication and authorization according to the requirements in § 170.315(j)(7) for system apps functionally registered using the capabilities in § 170.315(g)(33)(i)(A). In § 170.315(g)(33)(ii)(B), we propose that the Health IT Module must support asymmetric certificate-based system authentication and authorization according to the requirements in § 170.315(j)(8) for system apps dynamically registered using the capabilities in § 170.315(g)(33)(i)(B).

We propose in § 170.315(g)(33)(iii)(A) that the Health IT Module must support the requirements included in the ''Payer-to-Payer Exchange'' section of at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2), as a client and server, including support for the following ''Data Retrieval Methods'' to allow access to information in § 170.315(g)(33)(iii)(B), (C), and (D): ''Query all clinical resource individually,'' ''$patient-everything operation,'' and ''Bulk FHIR Asynchronous protocols.'' We specifically request comment on the ''Data Retrieval Methods'' we should require as part of the ''payer-to-payer API'' certification criterion.

To support the transfer of information on groups of patients, we propose in § 170.315(g)(33)(iii)(A)(*2*) that, for the time period up to and including December 31, 2027, the Health IT Module must respond to requests for patient data according to at least one of the versions of the standard adopted in § 170.215(a) (where we have adopted FHIR R4), and at least one of the versions of the implementation specification adopted in § 170.215(d) (where we have adopted the Bulk Data Access IG v1.0.0—STU 1, which we have proposed for expiration on January 1, 2028, and the Bulk Data Access IG v2.0.0—STU 2) for each of the data included in § 170.315(g)(33)(iii)(B), (C) and (D), as described below. Additionally, we propose for the time

[193] As noted above, for the purposes of the CMS Interoperability and Patient Access and Interoperability and Prior Authorization Final Rules discussed in this section, impacted payers include Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

period up to and including December 31, 2027, the Health IT Module must meet either the requirements specified in paragraph (g)(33)(iii)(A)(*2*)(*i*) (proposed to be the ''GroupLevelExport'' operation) or both (*i*) and (*ii*) (proposed to be the ''_type'' query parameter for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). We propose that on and after January 1, 2028, the Health IT Module must meet the requirements specified in paragraph (g)(33)(iii)(A)(*2*)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

We propose in § 170.315(g)(33)(iii)(B) that the Health IT Module must support the requirements described in the ''PDEX Server CapabilityStatement'' as a client and server via a standardized API according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) (where we have proposed to adopt the PDex IG version 2.0.0—STU2). We propose in § 170.315(g)(33)(iii)(C) that the Health IT Module must support sharing of claims information by supporting the data included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1) (where we have proposed to adopt CARIN IG for Blue Button® version 2.0.0—STU 2). We propose in § 170.315(g)(33)(iii)(D) that the Health IT Module must support the capabilities described in ''US Core Server CapabilityStatement'' according to the implementation specification in § 170.215(b)(1) (where we have adopted US Core IG version 3.1.1, which expires on January 1, 2026, US Core IG version 6.1.0, which we propose will expire on January 1, 2028, and where we propose to adopt US Core IG version 7.0.0) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 (where we have adopted USCDI version 1, which expires on January 1, 2026, USCDI version 3, which we propose will expire on January 1, 2028, and where we propose to adopt USCDI version 4).

We request comments on this proposal.

Support for CMS Requirements

The ''payer-to-payer API'' certification criterion proposed in § 170.315(g)(33), if finalized, would support the availability of certified health IT that can enable impacted payers [194] to meet CMS requirements to implement and maintain a Provider Access API as specified in 42 CFR 422.119, 431.60, 457.730, 438.242(b)(5), and 457.1233(d) and 45 CFR 156.221. Specifically, a Health IT Module certified to the ''payer-to-payer API'' criterion would facilitate sharing between payers of claims and encounter data (excluding provider remittances and patient cost-sharing information), all data classes and data elements in at least one of the versions of the USCDI standard in § 170.213, and certain information about prior authorization requests and decisions, as required in the CMS Interoperability and Prior Authorization Final Rule (89 FR 8855).

iv. Prior Authorization API—Provider (§ 170.315(g)(34)) and Prior Authorization API—Payer (§ 170.315(g)(35))

Background on Electronic Prior Authorization

Prior authorization processes [195] have contributed significantly to patient and provider burden, for instance, through delays experienced by patients and clinicians as they seek to satisfy the requirements associated with prior authorization rules set by payers.[196] ONC's Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs,[197] released in 2020, identified challenges associated with the prior authorization process faced by patients and health care providers, including: (i) difficulty in determining whether an item or service requires prior authorization; (ii) difficulty in determining payer-specific prior authorization requirements for those items and services; (iii) inefficient use of provider and staff time to navigate communications channels such as fax, telephone, and various web portals; and (iv) unpredictable and lengthy amounts of time to receive payer decisions. The Strategy noted that payers and health IT developers have addressed prior authorization in an ad hoc manner with interfaces that reflect individual payer technology considerations, payer lines of business, and customer-specific constraints. A 2022 physician survey conducted by the American Medical Association demonstrated significant negative impacts associated with the current prior authorization and beneficiary information exchange processes.[198] Nearly 94 percent of physicians reported care delays associated with prior authorization, and 80 percent reported that issues related to the prior authorization process can sometimes lead to treatment abandonment. In addition, survey respondents reported that physicians and their staff spend almost two business days each week completing prior authorizations, with nearly 35 percent of physicians retaining staff who work exclusively on prior authorizations. Today, hospitals and provider practices widely continue to use telephone and fax to conduct prior authorization processes. According to the Council for Affordable Quality Healthcare, only 28 percent of 228 million prior authorization contacts were fully electronic in 2022.[199]

In 2020, ONC charged the HITAC to establish the Intersection of Clinical and Administrative Data (ICAD) Task Force to produce information and considerations related to the merging of clinical and administrative data for electronic prior authorization. The ICAD Task Force's final report,[200] approved in November 2020, recommended that ONC work with CMS, other Federal actors, and standards development organizations to ''establish standards for prior authorization workflows.'' Specifically, the Task Force recommended that entities should develop API specifications ''such that the authorization and related documentation may be triggered in workflow in the relevant workflow

[194] As noted above, for the purposes of the CMS Interoperability and Patient Access and Interoperability and Prior Authorization Final Rules discussed in this section, impacted payers include Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

[195] Generally defined as rules imposed by healthcare payers that require approval for a medication, procedure, device, or other medical service be obtained prior to payment for the item or service.

[196] Office of the National Coordinator for Health Information Technology. Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs [PDF file]. February 2020. Retrieved from *https://www.healthit.gov/sites/default/files/page/2020-02/BurdenReport_0.pdf.*

[197] Office of the National Coordinator for Health Information Technology. Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs [PDF file]. February 2020. Retrieved from *https://www.healthit.gov/sites/default/files/page/2020-02/BurdenReport_0.pdf.*

[198] *https://www.ama-assn.org/practice-management/prior-authorization/prior-authorization-research-reports.*

[199] *https://www.caqh.org/sites/default/files/2023-05/2022-caqh-index-report.pdf.*

[200] *https://www.healthit.gov/sites/default/files/facas/ICAD_TF_FINAL_Report_HITAC_2020-11-06_508_0.pdf.*

system where the triggering event for the authorization is created.''

In January 2021, ONC published an RFI titled ''Request for Information: Electronic Prior Authorization Standards, Implementation Specifications, and Certification Criteria'' to seek input from the public regarding electronic prior authorization standards, implementation specifications, and certification criteria that could be adopted within the ONC Health IT Certification Program (87 FR 3475). ONC received approximately 130 responses to this RFI from a wide range of entities. Comments on the RFI broadly supported the incorporation of electronic prior authorization capabilities within the Program, while highlighting concerns about the current readiness and maturity of available implementation specifications to support these capabilities. Commenters also provided input on how certification criteria related to electronic prior authorization should be structured and how certification criteria should address other Federal requirements around the use of standards for electronic prior authorization transactions. Finally, commenters provided input on the benefits of improving electronic prior authorization for patients, providers, health IT developers and payers, as well as potential challenges associated with implementation.

ONC also charged the HITAC to establish a Task Force in order to provide input and recommendations in response to the RFI; the Task Force's recommendations were approved and submitted to ONC on March 10, 2022.[201] The proposals in this section would implement several recommendations from the Task Force, specifically recommendations to:

- Create a suite of electronic prior authorization health IT certification criteria for health IT systems supporting both providers and payers that can enable health IT developers to certify to one or more specific functional capabilities that together, across participating health IT systems, enable the full electronic prior authorization workflow.
- Ensure new certification criteria for electronic prior authorization provide for health IT systems that perform prior authorization on behalf of payers to ensure that their solutions are compliant to consensus-based standards for electronic prior authorization and are able to send and receive information needed to meet the prior authorization business case.
- Work with the Da Vinci Project and key healthcare stakeholders (*e.g.,* providers, developers, patients) to develop appropriate health IT certification criteria that incorporate key functional capabilities for prior authorization.
- Ensure certification requirements that allow a FHIR-enabled process for prior authorization transactions do not require translation to X12.
- Prioritize criteria based on the Da Vinci Prior Authorization Support (PAS) IG that allow data, C–CDA or FHIR documents to be provided in a FHIR construct.

Proposals

We propose to adopt a ''prior authorization API—provider'' certification criterion in § 170.315(g)(34), which establishes requirements for Health IT Modules that can be used to facilitate a provider's request of coverage information and request for a prior authorization decision. We also propose to adopt a complementary ''prior authorization API—payer'' certification criterion in § 170.315(g)(35), which establishes requirements for Health IT Modules that can be used by a payer to accept prior authorization requests from a provider, send requested documentation and coverage information, and send prior authorization decisions. Together, these certification criteria would support real-time access for providers to payer approval requirements, documentation, and rules at point of service, as well as enable providers to request and receive authorization. We believe that technology certified to these capabilities would help to automate and streamline the prior authorization process for health care providers and payers, to ensure treatment decisions are made in a timely fashion, avoid delays in care, and reduce administrative burden on health care providers and payers associated with assembling and reviewing required documentation.

Both certification criteria are based on the HL7 FHIR Da Vinci Burden Reduction IGs, which we propose to adopt in § 170.215(j) and incorporate by reference in § 170.299:

- HL7 FHIR Da Vinci—Coverage Requirements Discovery (CRD) Implementation Guide, Version 2.0.1—STU 2 (proposed in § 170.215(j)(1)(i)) [202]
- HL7 FHIR Da Vinci—Documentation Templates and Rules (DTR) Implementation Guide, Version 2.0.1—STU 2 (proposed in § 170.215(j)(2)(i)) [203]
- HL7 FHIR Da Vinci—Prior Authorization Support (PAS) Implementation Guide, Version 2.0.1—STU 2 (proposed in § 170.215(j)(3)(i)) [204]

We propose to adopt these implementation specifications under PHSA section 3004 and make them available for HHS use. Taken together, these implementation specifications support a comprehensive workflow for conducting electronic prior authorization transactions. The proposed certification criteria below include proposals that require the use of at least one version for each of the implementation specifications adopted in § 170.215(j)(1)–(3). If we adopt subsequent versions of the implementation specifications in § 170.215(j)(1) (CRD IG), (j)(2) (DTR IG), and (j)(3) (PAS IG), respectively, proposals that require the use of at least one implementation specification adopted in one of these locations would enable health IT developers to use any version adopted at the specified location, unless we specify an adoption ''expiration'' date which indicates a certain version of the specification may no longer be used after that date.

First, we propose in § 170.315(g)(34)(i) and § 170.315(g)(35)(i) that the ''prior authorization API—provider'' and ''prior authorization API—payer'' certification criteria, respectively, must support capabilities related to coverage discovery. These proposals are intended to facilitate the automation of both information exchange and prior authorization and reduce the need for provider-end manual intervention. Health IT Modules certified to these certification criteria would be able to request coverage information from a payer, for instance when a future encounter is being scheduled for a patient, and to initiate prior authorization electronically when a treatment decision has been made. These requirements will ensure that providers can request and receive a wide variety of information including updates to coverage information, alternative services or products, documentation requirements and rules related to coverage, forms, and templates to complete, and indications of whether prior authorization is required.

For the ''prior authorization API—provider'' certification criterion, in § 170.315(g)(34)(i), we propose that a Health IT Module certified to the

[201] *https://www.healthit.gov/sites/default/files/page/2022-03/2022-03-10_ePA_RFI_Recommendations_Report_Signed_508.pdf.*

[202] *See https://hl7.org/fhir/us/davinci-crd/.*

[203] *See https://hl7.org/fhir/us/davinci-dtr/.*

[204] *See https://hl7.org/fhir/us/davinci-pas/.*

criterion must support capabilities to initiate and exchange information with payer systems as a client to support the identification of coverage requirements. In § 170.315(g)(34)(i)(A) we propose that the Health IT Module must support the requirements described in the ''Privacy, Security, and Safety'' section of at least one of the versions of the implementation specification adopted in § 170.215(j)(1) (where we have proposed to adopt the CRD IG version 2.0.1—STU 2). In § 170.315(g)(34)(i)(B), we propose that the Health IT Module must support capabilities in § 170.315(j)(20) (where we have proposed to adopt the ''workflow triggers for decision support interventions'' certification criterion) to enable workflow triggers to call decision support services, including support for ''appointment-book,'' ''encounter-start,'' ''encounter-discharge,'' ''order-dispatch,'' ''order-select,'' and ''order-sign'' CDS Hooks according to at least one of the versions of the implementation specification adopted in § 170.215(j)(1) and requirements in § 170.315(j)(20).

In § 170.315(g)(34)(i)(C), we propose that the Health IT Module must support the requirements applicable to ''CRD Clients'' in at least one of the versions of the implementation specification in § 170.215(j)(1) including, as proposed in § 170.315(g)(34)(i)(C)(*1*), the requirements in the ''CRD Client CapabilityStatement,'' and, as proposed in § 170.315(g)(34)(i)(C)(*2*) support for the ''SHOULD'' requirements applicable to ''CRD Clients'' in Section 5.8 ''Additional Data Retrieval.'' We request public input on whether we should instead finalize a policy that these ''SHOULD'' requirements are treated as ''SHALL'' requirements.

For the ''prior authorization API—payer'' certification criterion, we propose in § 170.315(g)(35)(i) that a Health IT Module certified to the criterion must support specified capabilities to exchange information with provider systems to support the identification of coverage requirements. We propose in § 170.315(g)(35)(i)(A) that the Health IT Module must support the ability to receive and respond to decision support requests as a service by supporting the capabilities in § 170.315(j)(21). In § 170.315(g)(35)(i)(B) we propose that the Health IT Module must support the requirements applicable to ''CRD Server'' included in at least one of the versions of the implementation specification adopted in § 170.215(j)(1) (where we have proposed to adopt the CRD IG version 2.0.1—STU 2) including the requirements in the ''CRD Server CapabilityStatement.''

In § 170.315(g)(34)(ii) and § 170.315(g)(35)(ii)(B) we propose requirements for the ''prior authorization API—provider'' and ''prior authorization API—payer'' certification criteria, respectively, related to documentation and rules exchange. The DaVinci DTR and CRD IGs utilize Clinical Quality Language (CQL) to allow payers to inspect a patient's record for the necessary information related to the required documentation for a proposed item (such as durable medical equipment), medication, procedure, or other service. The DTR IG details the use of a payer provided Questionnaire resource and results from CQL execution to generate a QuestionnaireResponse resource containing the necessary information. This IG can allow payer APIs to specify how rules may be executed in a provider context so that documentation requirements are met, while at the same time reducing provider burden by reducing manual data entry.

For the ''prior authorization API—provider'' certification criterion, we propose in § 170.315(g)(34)(ii) that a Health IT Module certified to the criterion must support the ability to request and populate prior authorization documentation templates and rules from payer systems according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2) (where we have proposed to adopt the DTR IG version 2.0.1—STU 2).

''Light'' DTR capabilities are applicable to EHRs that rely on a SMART on FHIR application to handle the form filling function of DTR. This requires the server to provide access to the specified resources to allow such an app to retrieve and edit QuestionnaireResponses and related resources. In § 170.315(g)(34)(ii)(A)(*1*), we propose the Health IT Module must support the capabilities included in the ''Light DTR EHR'' CapabilityStatement according to at least one versions of the implementation specification adopted in § 170.215(j)(2) (where we have proposed to adopt the DTR IG version 2.0.1—STU 2). In § 170.315(g)(34)(ii)(A)(*2*)(*i*), we propose that the Health IT Module must support functional registration of the ''DTR SMART Client'' according to the requirements included in § 170.315(j)(1). We also propose in § 170.315(g)(34)(ii)(A)(*2*)(*ii*) that the Health IT Module must support dynamic registration of the ''DTR SMART Client'' according to the requirements included in § 170.315(j)(2).

In § 170.315(g)(34)(ii)(A)(*3*), we propose that the Health IT Module must support launching the ''DTR SMART Client'' according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2) (where we have proposed to adopt the DTR IG version 2.0.1—STU 2) to allow providers to launch an app to complete documentation for prior authorization according to at least one of the versions of the implementation specification in § 170.215(j)(2). In § 170.315(g)(34)(ii)(A)(*3*)(*i*) we propose that the Health IT Module must support authentication and authorization during the process of granting access to patient data to users according to the requirements in § 170.315(j)(10). In § 170.315(g)(34)(ii)(A)(*3*)(*ii*) we propose that the Health IT Module must support asymmetric certificate-based authentication according to the requirements in § 170.315(j)(11) for the ''Light DTR Client'' dynamically registered using the capabilities in § 170.315(g)(34)(ii)(A)(*2*)(*ii*).

In contrast to ''Light DTR EHR'' capabilities, ''full'' DTR capabilities are relevant to EHRs that manage the form filling functions of DTR internally. In § 170.315(g)(34)(ii)(B), we propose that the Health IT Module must support the capabilities included in the ''Full DTR EHR'' CapabilityStatement according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2) (where we have proposed to adopt the DTR IG version 2.0.1—STU 2). Such EHRs need only support client capabilities for the Questionnaire Package, ValueSet Expand, and Next Question operations.

For the ''prior authorization API—payer'' certification criterion, we propose in § 170.315(g)(35)(ii) that a Health IT Module certified to the criterion must support specified capabilities to exchange prior authorization documentation requirements with provider systems. In § 170.315(g)(35)(ii)(A)(*1*), we propose that the Health IT Module support functional registration for the ''DTR SMART Client'' and ''Full DTR EHR'' according to the requirements included in § 170.315(j)(1). In § 170.315(g)(35)(ii)(A)(*2*), we propose that the Health IT Module support dynamic registration for the ''DTR SMART Client'' and ''Full DTR EHR'' according to the requirements included in § 170.315(j)(2).

In § 170.315(g)(35)(ii)(B)(*1*) we propose that the Health IT Module support system authentication and authorization according to the requirements in § 170.315(j)(7) for the ''DTR SMART Client'' and ''Full DTR

EHR'' functionally registered using the capabilities in § 170.315(g)(35)(ii)(A)(*1*). In § 170.315(g)(35)(ii)(B)(*2*) we propose that the Health IT Module support asymmetric certificate-based system authentication and authorization according to the requirements in § 170.315(j)(8) for the ''DTR SMART Client'' and ''Full DTR EHR'' dynamically registered using the capabilities in § 170.315(g)(35)(ii)(A)(*2*).

In § 170.315(g)(35)(ii)(C) we propose that the Health IT Module support the ability to receive and respond to a prior authorization documentation request with documentation templates and rules, according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2) (where we have proposed to adopt the DTR IG version 2.0.1—STU 2), including in § 170.315(g)(35)(ii)(C)(*1*), the capabilities included in the ''DTR Payer Service'' CapabilityStatement, according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2).

Finally, in § 170.315(g)(34)(iii) and § 170.315(g)(35)(iii), we propose that the ''prior authorization API—provider'' and ''prior authorization API—payer'' certification criteria must support capabilities related to the submission, receipt, and response to a prior authorization request.

For the ''prior authorization API—provider'' certification criterion, we propose in § 170.315(g)(34)(iii)(A) that the Health IT Module must support the ability to submit a prior authorization request to a payer system according to at least one of the versions of the implementation specification adopted in 170.215(j)(3) (where we have proposed to adopt the PAS IG version 2.0.1—STU 2). Specifically, we propose in § 170.315(g)(34)(iii)(A)(*1*) that the Health IT Module include support for the ''EHR PAS Capabilities'' CapabilityStatement according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3).

We propose in § 170.315(g)(34)(iii)(A)(*2*) that the Health IT Module support the ability to include documentation created in § 170.315(g)(34)(ii) in a prior authorization request to a payer system according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3). We propose in § 170.315(g)(34)(iii)(A)(*3*) that the Health IT Module support the ability to consume and process a ''ClaimResponse'' according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3). Finally, we propose in § 170.315(g)(34)(iii)(A)(*4*) that the Health IT Module support subscriptions as a client according to the requirements in § 170.315(j)(24) and an implementation specification in § 170.215(j)(3), in order to support ''pended authorization responses.''

For the ''prior authorization API—payer'' certification criterion, we propose in § 170.315(g)(35)(iii)(A)(*1*) that the Health IT Module must support functional registration according to the requirements included in § 170.315(j)(1), and propose in § 170.315(g)(35)(iii)(A)(*2*) to require support for dynamic registration according to the requirements included in § 170.315(j)(2). We propose in § 170.315(g)(35)(iii)(B)(*1*) that the Health IT Module must support system authentication and authorization according to the requirements in § 170.315(j)(7) for system apps functionally registered using the capabilities in § 170.315(g)(35)(iii)(A)(*1*). We propose in § 170.315(g)(35)(iii)(B)(*2*) that the Health IT Module must support asymmetric certificate-based system authentication and authorization according to the requirements in § 170.315(j)(8) for system apps dynamically registered using the capabilities in § 170.315(g)(35)(iii)(A)(*2*).

In § 170.315(g)(35)(iii)(C)(*1*)–(*4*), we propose that the API must support the ability to receive, process, and respond to a prior authorization request according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3) (where we have proposed to adopt the PAS IG version 2.0.1—STU 2). Specifically, we propose in § 170.315(g)(35)(iii)(C)(*1*) that the Health IT Module support ''Intermediary PAS Capabilities.'' We propose in § 170.315(g)(35)(iii)(C)(*2*) that the Health IT Module support an endpoint for receiving prior authorization requests. We propose in § 170.315(g)(35)(iii)(C)(*3*) that the Health IT Module support the ability to respond to a prior authorization request with a ''ClaimResponse.'' Finally, we propose in § 170.315(g)(35)(iii)(C)(*4*) that the Health IT Module must support subscriptions as a server according to the requirements in § 170.215(j)(3) to support ''pended authorization responses'' according to at least one of the versions of the implementation specification in § 170.215(j)(3).

We request comments on this proposal.

Organization of the Proposed Prior Authorization API Criteria

In the January 2021 ''Request for Information: Electronic Prior Authorization Standards, Implementation Specifications and Certification Criteria,'' we requested comment on the most appropriate way to structure health IT certification criteria enabling a health care provider to conduct electronic prior authorization transactions (87 FR 3480). We received a wide range of input on this topic with commenters noting that different types of systems, including EHRs, revenue cycle and patient management systems, and third-party applications may be responsible for different elements of the electronic prior authorization workflow. Some commenters recommended that ONC consider proposing individual criteria that map to each of the Da Vinci IGs (the CRD, DTR, and PAS IGs) which we discussed in the RFI and have proposed to adopt in this proposed rule. Other commenters suggested creating more granular certification criteria which reflect specific capabilities and key interactions within the prior authorization workflow, so that these capabilities can be implemented as stand-alone solutions to provide incremental value. The Task Force charged by the HITAC to provide a response to the January 2021 RFI also provided recommendations on this topic.[205]

In this proposed rule, we have proposed a single prior authorization certification criterion for health care providers in § 170.315(g)(34). However, existing guidance in the Program could provide flexibility around the use of distinct technology products that may be utilized to perform the capabilities that are outlined in the proposed certification criterion. Specifically, health IT developers are permitted to use ''relied upon software'' (76 FR 1276) to demonstrate compliance with certification criteria adopted at 45 CFR part 170, subpart C.[206] Relied upon software is typically third-party software that is not developed by the health IT developer presenting its health IT for testing and certification. Relied upon software may be used to demonstrate compliance with a portion of an adopted certification criterion or an entire certification criterion. When a health IT developer relies upon software to demonstrate compliance with a certification criterion, such relied upon software must be included in the scope of the certification issued to the Health IT Module or Complete EHR. In cases where a Health IT Module may be

[205] *https://www.healthit.gov/sites/default/files/page/2022-03/2022-03-10_ePA_RFI_Recommendations_Report_Signed_508.pdf.*

[206] For more guidance on relied upon software, *see: https://www.healthit.gov/sites/default/files/relieduponsoftwareguidance.pdf.*

paired with multiple ''relied upon software'' products for the same capability, it must be tested with at least one such product to demonstrate compliance with a certification criterion's requirements. Afterwards, the Health IT Module developer is permitted to list all additional ''relied upon software'' products for the same capability paired with the certified Health IT Module without having to test each one with the ONC–ATL. A health IT developer always remains responsible for its product's conformance to a certification criterion even when the ''relied upon software'' contributes to, or is the cause of, a non-conformity.

We invite additional comments on the most appropriate way to structure the proposed ''prior authorization API—provider'' certification criterion, as well as the ''prior authorization API—payer'' certification criterion. Specifically, we are interested in the public's input on how organization of the proposed certification criteria would affect the ability of developers to effectively offer certified health IT products that meet the criteria, and what impact the organization of the proposed criteria would have on customers who may already possess technology products that can be used to conduct electronic prior authorization transactions. We also request comment on whether or to what degree existing guidance for the Program, such as the relied upon software policy described above, would address scenarios in which distinct health IT products are used to support different elements of the prior authorization workflow. Finally, we invite comments on alternative approaches to organizing the ''prior authorization API'' certification criteria.

Support for CMS Requirements

The ''prior authorization API—payer'' certification criterion proposed in § 170.315(g)(35), if finalized, would support the availability of certified health IT that can enable impacted payers [207] to meet CMS requirements to implement and maintain a Prior Authorization API as specified in 42 CFR 422.122(b), 431.80(b), 457.732(b), 438.242(b)(7), and 457.1233(d) and 45 CFR 156.223(b), respectively. Specifically, a Health IT Module certified to the ''prior authorization API—payer'' certification criterion would enable payers to make available information about documentation required for approval of any items or services that require prior authorization; support an automated process for prior authorization request and response; and communicate whether the payer approves the prior authorization request (and the date or circumstance under which the authorization ends), denies the prior authorization request (with a specific reason), or requests more information, as required in the CMS Interoperability and Prior Authorization Final Rule (89 FR 8897).

The ''prior authorization API—provider'' certification criterion proposed in § 170.315(g)(34), if finalized, would support the availability of certified health IT that can enable health care providers to interact with the APIs established pursuant to the payer API requirements referenced above, using certified health IT. CMS finalized Electronic Prior Authorization measures for the Medicare Promoting Interoperability Program and the MIPS Promoting Interoperability Performance Category in the CMS Interoperability and Prior Authorization Final Rule (89 FR 8909) which are intended to incentivize health care providers to interact with these APIs in order to submit prior authorization requests. If finalized, adopting and using technology certified to this criterion would enable eligible clinicians, and eligible hospitals and CAHs, to complete the prior authorization request actions associated with these measures using certified health IT.

Administrative Simplification Requirements Under HIPAA

We note that, pursuant to the administrative simplification rules established under HIPAA, the Secretary must adopt electronic standards for use by ''covered entities,'' which is defined as including health plans, healthcare clearinghouses, and certain health care providers.[208] The two standards adopted for referral certification and authorization transactions under the HIPAA administrative simplification rules (45 CFR 162.1302) include: NCPDP Version D.0 for retail pharmacy drugs; and X12 Version 5010x217 278 (X12 278) for dental, professional, and institutional request for review and response for items and services. HHS has also proposed to adopt the X12 275 standard, which is used to transmit additional documentation to support the exchange of the additional information that is required for prior authorization, in the ''Administrative Simplification: Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard'' proposed rule (87 FR 78438).

Nothing in our proposed certification criteria related to electronic prior authorization would alter requirements for covered entities to use adopted HIPAA transaction standards. Moreover, the FHIR specifications we propose to adopt for these certification criteria would not conflict with the use of the adopted HIPAA standard, and we would expect covered entities using technology certified to these criteria to ensure compliance with applicable requirements.

We note that in March 2021, the CMS National Standards Group (NSG), on behalf of HHS, approved an application [209] from an industry group of payers, providers, and vendors for an exception under 45 CFR 162.940 from the HIPAA transaction standards for Da Vinci payers and their trading partners when using the FHIR standard for prior authorization. Under this exception, the group would test a prior authorization exchange using the HL7 FHIR Da Vinci standard without the X12 278 standard to determine whether this alternative standard for prior authorization could improve efficiency. HHS provides information about requests for exceptions from standards to permit testing of proposed modifications on the CMS HIPAA administrative simplification website.[210]

On February 28, 2024, CMS NSG, on behalf of HHS, announced an application of enforcement discretion for HIPAA covered entities that implement FHIR-based Prior Authorization APIs as described in the CMS Interoperability and Prior Authorization Final Rule (89 FR 8758).[211] HHS stated that this action was in response to feedback received on multiple notices of proposed rulemaking and extensive stakeholder outreach and is intended to promote efficiency in the prior authorization

[207] As noted above, for the purposes of the CMS Interoperability and Patient Access and Interoperability and Prior Authorization Final Rules discussed in this section, impacted payers include Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

[208] For more information, *see https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification.*

[209] *See https://confluence.hl7.org/display/DVP/Da+Vinci+HIPAA+Exception?preview=/113675673/113675685/Approval%20%232021031001.pdf.*

[210] Centers for Medicare & Medicaid Services (2022). Go-to-Guidance, Guidance Letters. Retrieved from *https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/subregulatory-guidance/letters.*

[211] *See https://www.cms.gov/files/document/discretion-x12-278-enforcement-guidance-letter-remediated-2024-02-28.pdf.*

process. Specifically, HHS stated that HIPAA Administrative Simplification enforcement action will not be taken against HIPAA covered entities that choose not to use the X12 278 standard as part of an electronic FHIR prior authorization process. HHS will continue to evaluate the HIPAA prior authorization transaction standards, including continuing to seek stakeholder input and evaluating the results of testing an all-FHIR-based transaction.

v. Provider Directory API—Health Plan Coverage (§ 170.315(g)(36))

We propose to adopt a ''provider directory API—health plan coverage'' certification criterion in § 170.315(g)(36) which would specify technical requirements for Health IT Modules that can enable publishing of information regarding the providers that participate in a payer's network. For beneficiary coverage and clinical information to be both useful to and utilized by patients and providers, it is necessary for patients to understand which providers, facilities, and pharmacies are covered by their current or future plan.

The proposed certification criterion is based on the HL7 FHIR Da Vinci Payer Data Exchange Plan Net (PDex Plan Net) Implementation Guide version 1.1.0—STU1.1.[212] We propose, independent of the certification criterion proposal, to adopt this implementation specification in § 170.215(n)(1) and incorporate it by reference in § 170.299. We propose to adopt this implementation specification under PHSA section 3004 and make it available for HHS use. Use of this implementation specification can enable third parties to develop applications through which consumers and providers can query the participants in a payer's network that may provide services that address their healthcare needs. We propose in § 170.315(g)(36) that a Health IT Module certified to the criteria must support the ability to publish a payer's insurance plans, their associated networks, and the organizations and providers that participate in these networks according to at least one of the versions of the implementation specification adopted in § 170.215(n), including the requirements described in the ''Plan-Net CapabilityStatement.'' If we adopt subsequent versions of the PDex Plan Net IG in § 170.215(n), our proposal to require the use of at least one of the versions of the implementation specification adopted in § 170.215(n) would enable health IT developers to use any version adopted at this location, unless we specify an adoption ''expiration'' date, which indicates a certain version of the specification may no longer be used after that date.

Support for CMS Requirements

The ''provider directory API—health plan coverage'' certification criterion proposed in § 170.315(g)(36), if finalized, would support the availability of certified health IT that can enable impacted payers [213] to meet CMS requirements to implement and maintain a Provider Directory API in 42 CFR 422.120, 431.70, 457.760, 438.242(b)(6), and 457.1233(d)(3), respectively. Specifically, a Health IT Module certified to the ''provider directory API—health plan coverage'' certification criterion would facilitate the availability of standardized information about a payer's provider networks, as well as pharmacy directory data, as required in the CMS Interoperability and Patient Access Final Rule (85 FR 25563).

We request comments on this proposal.

d. Revision and Addition of API Condition and Maintenance of Certification Requirements

Given that we have proposed to adopt new certification criteria that would be applicable to certified API technology under the Program, we propose to extend the applicability of the API Conditions of Certification in § 170.404(a) and certain API Maintenance of Certification requirements in § 170.404(b) to Certified API Developers with Health IT Modules certified to the criteria proposed for adoption in § 170.315(g)(20), § 170.315(g)(30)–(36), and § 170.315(j). If our proposals are finalized, this would mean that the API Condition and Maintenance of Certification requirements would include within its scope the certification criteria adopted in § 170.315(g)(7)–(10), § 170.315(g)(20), § 170.315(g)(30)–(36), and § 170.315(j). We propose to make corresponding and conforming edits to § 170.404, including revisions to both § 170.404(a) and in § 170.404(b), to specify which API-related certification criteria apply in the context of each Condition and Maintenance of Certification requirement. We believe this approach is essential to continue to fulfill the statutory requirements set forth in PHSA § 3001(c)(5)(D)(iv), in particular Congress' requirement that a developer of certified health IT has ''published application programming interfaces and allows health information from such technology to be accessed, exchanged, and used without special effort.'' As we described in the ONC Cures Act Final Rule (84 FR 7476 through 7477), we established the API Condition and Maintenance of Certification requirements to, among other outcomes, promote transparency and pro-competitive business practices among Certified API Developers in pursuit of a policy that would result in access, exchange, and use of EHI ''without special effort.'' We believe that these same requirements should apply to developers of these new API-related certification criteria in § 170.315(g)(20) and (g)(30)–(36), and that the proposals to reference these certification criteria in § 170.404 would continue to adhere to our statutory charge to advance nationwide interoperability.

We propose in § 170.404(a)(2) to consolidate and establish documentation requirements that are currently required in § 170.315(g)(7)(ii), § 170.315(g)(9)(ii), and § 170.315(g)(10)(viii). Correspondingly, we propose to remove those three specified ''documentation'' paragraphs from those respective certification criteria because the consolidated conformance requirements would now be stated in the proposed § 170.404(a)(2). We believe that these documentation requirements should also pertain to the other API-related criteria we propose to adopt in § 170.315(g)(20), (g)(30)–(36), and § 170.315(j), and we believe that such requirements better fit as a generally applicable API Condition of Certification requirement than a functional requirement specified in each individual API-related certification criterion.

Specifically, we propose in § 170.404(a)(2) that a Certified API Developer must publish complete business and technical documentation, including the documentation described in § 170.404(a)(2)(i)–(ii), via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. In § 170.404(a)(2)(i), we propose that this should include technical documentation currently in § 170.315(g)(7), (9), and (10) such as API syntax, function names, required and optional parameters supported and their

[212] *See https://hl7.org/fhir/us/davinci-pdex-plan-net/STU1.1/.*

[213] As noted above, for the purposes of the CMS Interoperability and Patient Access and Interoperability and Prior Authorization Final Rules discussed in this section, impacted payers include Medicare Advantage (MA) organizations, state Medicaid fee-for-service (FFS) programs, state Children's Health Insurance Program (CHIP) FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs).

data types, return variables and their types/structures, exceptions and exception handling methods and their returns. We propose that § 170.315(g)(7)(ii) and § 170.315(g)(9)(ii) be reserved. Further, we propose in § 170.404(a)(2)(i)(B) that this technical documentation should include 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); and in § 170.404(a)(2)(i)(C) that all applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server. We propose to revise § 170.404(a)(2)(ii) to require that API(s) must include complete accompanying business documentation that contains, at a minimum, the existing requirements currently in § 170.404(a)(2)(ii)(A) and (B).

In addition to the proposed modifications to § 170.404(a), we propose to revise the Maintenance of Certification requirements for Application Programming Interfaces, in § 170.404(b). Specifically, we propose that the same authenticity verification and registration requirements currently in § 170.404(b)(1) apply to Certified API Developers with a Health IT Module certified to one or more of the certification criteria in of § 170.315(g)(10), (20), (30), (32)–(35). Similarly, we propose in § 170.404(b)(1)(i) that 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 any of the certification criteria in § 170.315(g)(10), (20), (30), (32)–(35). We propose that this process shall not apply to API Users that are part of a trust community supported at an API Information Source deployment submitting registration requests conformant to the specifications in § 170.215(o). In § 170.404(b)(1)(ii) we propose that 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. If the API User is part of a trust community supported at an API Information Source deployment and submitted a valid registration request conformant to the specifications in § 170.215(o), we propose that the application must instead be enabled for production use within one business day.

We propose in § 170.404(b)(2) to modify the existing publication and format requirements for service base URLs. We propose to refer to service base URLs as ''API discovery details'' and propose in § 170.404(b)(2)(i)(A) that these must be published publicly and at no charge for all customers regardless of whether the Health IT Module is centrally managed by the Certified API Developer or locally deployed by an API Information Source. We also propose in § 170.404(b)(2)(i)(B) that these API discovery details are reviewed quarterly and updated as necessary.

We also propose revisions to the formatting requirements of these API discovery details by adding to the current regulation text in § 170.404(b)(2)(i)–(iii) an option to publish API discovery details and related API Information source details, including the API Information Source's name, location, and facility identifier, according to the ''User-access Brands and Endpoints'' specification in at least one implementation specification adopted in § 170.215(c). We propose this at revised § 170.404(b)(2)(iii) and consolidate the regulation text currently in § 170.404(b)(2)(i)–(iii) as § 170.404(b)(2)(ii)(A)–(C). We propose that publication of API discovery details for patient access applies to Certified API Developers with Health IT Modules certified to either of the criteria in § 170.315(g)(10) and (g)(30) and we have established timelines for Health IT Modules certified to these criteria to conform to requirements in § 170.404(b).

Specifically, we propose that for the time period up to and including December 31, 2027, Certified API Developers with Health IT Modules certified to § 170.315(g)(10) must meet either the API discovery detail requirements in (i) and (ii) or the requirements in (i), (iii), and (iv) of this section. On and after January 1, 2028, all Certified API Developers with Health IT Modules certified to § 170.315(g)(10) must meet the requirements in (i), (iii), and (iv) of this section. Certified API Developers with Health IT Modules certified to § 170.315(g)(30) must meet the requirements in (i), (iii), and (iv) of this section. We believe this cadence and combination of requirements will support a gradual improvement in consistently available, standards-based access for patients seeking to access their health information via APIs.

These Maintenance of Certification requirements are already established for Certified API Developers with a Health IT Module certified to the certification criterion adopted in § 170.315(g)(10), and we believe that extending these requirements to § 170.315(g)(30) is appropriate because this proposed certification criterion supports patient access to health and administrative (*e.g.,* payer) information. Requirements in § 170.404(b)(1) and (2) facilitate the use of patient-facing applications and enable patient users to discover details necessary to connect to their data using an application of their choice.

We request comment on these proposals.

In § 170.404(b)(3), we propose new Maintenance of Certification requirements for Certified API Developers with a Health IT Module certified to the certification criteria adopted in § 170.315(g)(32), § 170.315(g)(33), § 170.315(g)(35), or § 170.315(g)(36) to publish API discovery details. We propose in § 170.404(b)(3)(i) that the developer must publicly publish the API discovery details for all its customers, with Health IT Modules certified to § 170.315(g)(32), § 170.315(g)(33), § 170.315(g)(35) or § 170.315(g)(36) regardless of whether the Health IT Modules are centrally managed by the Certified API Developer or locally deployed by an implementer of the Certified API Developer.

We propose in § 170.404(b)(3)(ii) that the network information and related API Information Source details, including the API Information Source's name, location, and facility identifier, must be published in an aggregate vendor-consolidated Bundle according to the ''User-Access Brands and Endpoints'' specification in at least one implementation specification adopted in § 170.215(c). In § 170.404(b)(3)(iii) we propose that all API discovery details for payer information published according to this section must be reviewed quarterly and as necessary updated by the Certified API Developer.

While we recognize that this will require ongoing coordination between health IT developers and users of the Health IT Modules, as well as regular updates to the publicly available network information, we believe that making such information public is critical to establishing ongoing interoperability of administrative data. We welcome comment on these proposals.

Finally, we propose revisions to two key terms in § 170.404(c). We propose to revise *certified API technology* to mean 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), (g)(20), (g)(30) through (36), and (j). This revision would support our proposed

application of requirements in § 170.404 to the proposed APIs in § 170.315(g) and the proposed modular API capabilities in § 170.315(j). We also propose to revise *Certified API Developer* to mean a health IT developer that creates ''certified API technology.'' We believe this simplified definition for Certified API Developer will similarly support this term's application to the proposed API capabilities in § 170.315(g) and proposed modular API capabilities in § 170.315(j).

We request comment on these proposals.

e. Revisions to Real World Testing Requirements

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 [214] in the type of setting in which such technology would be marketed. As discussed in the ONC Cures Act Final Rule, 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 of a health IT's certification (85 FR 25766).

For reasons similar to our proposal to expand requirements in § 170.404 to the proposed certification criteria in § 170.315(g)(20), (g)(30) through (36), and 170.315(j), we propose to revise the real world testing requirements in § 170.405 by adding these proposed certification criteria in § 170.405(a). Given that each of these proposed new certification criteria is focused on interoperability and data exchange, we believe it is important that developers of certified health IT with Health IT Module(s) certified to these criteria participate in both Condition and Maintenance of Certification requirements. Per requirements in § 170.405(b) we also propose that developers of certified health IT with Health IT Modules certified to any one or more of the certification criteria in § 170.315(g)(20), (g)(30) through (36), and 170.315(j) also submit annual real world testing plans as well as annual real world testing results, which applies to any one or more of the criteria referenced in 170.405(a). We note that by including these criteria in § 170.405(a), that health IT developers may voluntarily avail themselves of SVAP flexibility so long as they 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.

Given that we are proposing to reference several certification criteria in § 170.315(j) across various certification criteria in § 170.315(g), we clarify that a health IT developer with Health IT Module(s) certified to any one or more criteria in § 170.315(g) that successfully tests the real world use of those Health IT Module(s) will be considered conformant to the real world testing requirements for the corresponding certification criteria in § 170.315(j). We do not intend for Health IT Modules certified to any certification criterion in § 170.315(g) to submit duplicative real world testing plans or results for corresponding certification criterion in § 170.315(j) and believe this clarification will help reduce potential confusion for developers certified to criteria in § 170.315(g).

We request comments on this proposal.

f. Addition of Criteria to the Base EHR Definition

Two of the certification criteria proposed in this section pertain to certified Health IT Modules intended for use by health care providers, specifically the ''provider access API—client'' and the ''prior authorization API—provider'' certification criteria in § 170.315(g)(31) and § 170.315(g)(34), respectively. We believe both certification criteria reflect fundamental capabilities, which would be appropriate for adoption by any health care provider using certified health IT. Technology certified to the ''provider access API—client'' criterion would enable a provider to receive key clinical and administrative information from a healthcare payer. Technology certified to the ''prior authorization API—provider'' criterion would enable a health care provider to conduct prior authorization requests and related interactions with payers that are widely used today.

We propose in § 170.102 in the definition of Base EHR to add the proposed certification criteria in § 170.315(g)(31) and § 170.315(g)(34) to the set of certification criteria adopted by the Secretary that are necessary to meet the Base EHR definition. We propose that the ''provider access API—client'' certification criterion in § 170.315(g)(31) would be necessary to meet the Base EHR definition on and after January 1, 2028. However, for the ''prior authorization API—provider'' certification criterion in § 170.315(g)(34), we propose that this criterion would be necessary to meet the Base EHR definition on and after January 1, 2027. This date is consistent with the policy finalized in CMS Interoperability and Prior Authorization Final Rule, which finalized an Electronic Prior Authorization measure in the Medicare Promoting Interoperability program and the MIPS Promoting Interoperability performance category which program participants must report on beginning with the CY 2027 EHR reporting period and CY 2027 performance period/2029 MIPS payment year, respectively (89 FR 8910).

We request comments on this proposal.

C. Conditions and Maintenance of Certification Requirements—Insights and Attestations

1. Insights Condition and Maintenance of Certification Requirements

a. Background

The Cures Act specified requirements in section 4002(c) to establish an Electronic Health Record (EHR) Reporting Program to provide reporting on certified health IT in the categories of interoperability, usability and user-centered design, security, conformance to certification testing, and other categories, as appropriate to measure the performance of EHR technology. Data collected and reported would address information gaps in the health IT marketplace and provide insights on the use of certified health IT. In the HTI–1 Final Rule (89 FR 1311), we established the EHR Reporting Program as the ''Insights Condition and Maintenance of Certification'' (also referred to as the ''Insights Condition'') and finalized in § 170.407 the first set of measures to reflect the interoperability category required by section 3009A(a)(3)(A)(iii) of the PHSA.

We refer readers to the HTI–1 Proposed Rule (88 FR 23831) for detailed background on how we engaged with the health IT community for the purpose of identifying measures that developers of certified health IT would be required to report on as a Condition and Maintenance of Certification under the Program, and how our proposals to modify the measures that the Urban Institute developed is consistent with section 3009A(a)(4) of the PHSA. Our proposals with respect to each requirement continue to reflect how we propose to

[214] Interoperability is 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.

modify the set of measures in Urban Institute's final report.[215] As such, we propose modifications in this proposed rule as part of the next iteration of the Insights Condition and Maintenance of Certification requirements and welcome comments on our proposals below.

b. Process for Reporting Updates

In the HTI–1 Proposed Rule (88 FR 23847), we stated that there may be other factors that could impact a developer of certified health IT's ability to easily collect data to comply with the Insights Condition's requirements. For example, a developer of certified health IT may have contracts or business agreements that inhibit the health IT developer's ability to collect data from its customers. We also proposed in the HTI–1 Proposed Rule that in such scenarios, developers of certified health IT would need to renegotiate their contracts. We further explained that we expected developers of certified health IT would work to mitigate any issues and provisions affecting their ability to comply with the Insights Condition requirements.

In the HTI–1 Final Rule (89 FR 1347), we did not finalize our proposal to require developers of certified health IT to renegotiate contracts, when needed, with their customers to comply with the Insights Condition requirements. Instead, we finalized in § 170.407(a)(1)(i)(C) that health IT developers will need to provide ONC with information on the degree to which the data they submit are complete, specifically by reporting the percentage of their total customers as represented by hospitals for products used in inpatient settings and clinician users for products used in outpatient settings, that are included in their reported data for each metric for which they submit a response. We stated that the percentage of health care providers that are represented in the data provides transparency regarding the degree to which the data are complete.

Detailed information regarding health care providers that are represented in the data would also help us further interpret the results of the data received and allow us to assess whether the data is nationally representative. This would also allow us to report results indicating whether, and how, the data are skewed. Therefore, we propose to add § 170.407(a)(1)(i)(D) to require developers of certified health IT to provide health care provider identifiers (*e.g.,* National Provider Identifier (NPI), CMS Certification Number (CCN), or other type of unique national identifier) for providers included in the data submitted. Note, given this proposal, we propose to make conforming grammatical edits to the list structure in § 170.407(a)(1)(i)(B) and (C) to accommodate the proposed addition of (D). We also propose to revise § 170.407(a)(1)(i)(C) to remove the word ''sites'' from ''hospital sites'' to align with our proposal relating to the minimum reporting qualifications requirement described in detail further below.

The additional health care provider identifier information would help determine the representativeness of the data. Using the unique health care provider identifiers, we could link to other data sources such as the National Provider and Payer Enumeration System (NPPES) and CMS program participant data that would allow us to identify the types of providers included in the data. Knowing the different types of providers included in the data would allow us to determine if the data are skewed towards providers with certain characteristics associated with differences in health IT adoption and use, such as size, rural location and ownership.[216] [217] [218] For example, based upon surveys of hospitals, larger hospitals tend to engage more in interoperability compared to smaller hospitals.[219] If the data disproportionately consist of larger hospitals, this could potentially skew the results towards higher performance on interoperability. To reduce burden, we intend to provide a template for developers of certified health IT to submit the data electronically, in a structured format, if our proposal is finalized.

We welcome comments on our proposal, and welcome comments on other alternatives that would offer a consistent approach for all health IT developers to report on the representativeness of the data provided to ONC. We continue to believe reporting the percentage of ''clinicians'' (for products primarily used in outpatient settings) and ''hospitals'' (for products primarily used in inpatient settings) in § 170.407(a)(1)(i)(C) is the best approach given that this aligns with CMS programs and is used to determine whether developers meet the threshold for reporting on the Insights Condition of Certification, however, we are open to considering alternatives that provide a consistent manner for developers to provide transparency on the degree to which the data are complete. This may also include removing the requirement for developers to provide the percentage of total customers that are represented in the data in § 170.407(a)(1)(i)(C), and instead only require developers to provide health care provider identifiers if that would provide a more consistent approach across developers and also allow us to gauge the representativeness of the data while reducing burden. We seek public feedback on approaches to understand the types and number of providers that are included in the data submitted, relative to the broader population of providers using the products of a developer of certified health IT. We also request comments for alternatives that may shift measurement from provider-based measures to patient-centered measures such as percentage and/or number of encounters or patients included in the data.

In the HTI–1 Final Rule (89 FR 1346), we finalized the Insights Condition reporting frequency to annually (once per year) for any Health IT Module that has or has had an active certification at any time under the ONC Health IT Certification Program during the prior six months in § 170.407(b). We stated that developers of certified health IT who do not meet the minimum reporting qualifications would submit a response to specify that they do not meet the qualifications under the Insights Condition. In this way, all developers of certified health IT would report on all measures, even if some report that they do not meet the minimum reporting qualifications (89 FR 1345).

We propose to revise § 170.407(b)(1) to make clear that all developers must provide responses to the Insights Condition of Certification on an annual basis regardless of how long a developer

[215] *https://www.urban.org/research/publication/electronic-health-record-ehr-reporting-program-developer-reported-measures.*

[216] Strawley C., Everson J., Barker W. Hospital use of APIs to Enable Data Sharing Between EHRs and Apps. Office of the National Coordinator for Health Information Technology. Data Brief: 68. 2023. *https://www.healthit.gov/data/data-briefs/hospital-use-apis-enable-data-sharing-between-ehrs-and-apps.*

[217] Pylypchuk Y., J. Everson. (January 2023). Interoperability and Methods of Exchange among Hospitals in 2021. ONC Data Brief, no. 64. Office of the National Coordinator for Health Information Technology: Washington DC. *https://www.healthit.gov/data/data-briefs/interoperability-and-methods-exchange-among-hospitals-2021.*

[218] Pylypchuk Y., J. Everson, D. Charles, and V. Patel. (February 2022). Interoperability Among Office-Based Physicians in 2015, 2017, and 2019. ONC Data Brief, no.59. Office of the National Coordinator for Health Information Technology: Washington DC. *https://www.healthit.gov/data/data-briefs/interoperability-among-office-based-physicians-2019.*

[219] Pylypchuk Y., J. Everson. (January 2023). Interoperability and Methods of Exchange among Hospitals in 2021. ONC Data Brief, no. 64. Office of the National Coordinator for Health Information Technology: Washington DC. *https://www.healthit.gov/data/data-briefs/interoperability-and-methods-exchange-among-hospitals-2021.*

has or has had an active certification under the Program. Since all developers of certified health IT within the Program are required to submit a response, as finalized in HTI–1 Final Rule (89 FR 1345), we believe this revision will simplify and clarify expectations.

We propose in § 170.407(b)(1)(ii) that the response a developer of certified health IT submits per the requirements of the Insights Condition, must be applicable to all their certified health IT as of January 1st of each year, beginning January 2026. For example, a developer of certified health IT who is submitting their response July 2027, would include data from all their applicable certified health IT from the prior year between January to December 2026 for their July 2027 submission. This has been the expectation from what we finalized in HTI–1 (89 FR 1348); however, we believe codifying the date of January 1st is necessary so that all health IT developers can determine whether they are required to report on a measure 18 months in advance of the response submission. This is similar to real world testing reporting requirements which has a specified date for all developers of certified health IT to assess their eligibility on submitting a real world testing plan per § 170.405. We strongly encourage developers of certified health IT to assess whether they meet the minimum reporting qualifications for the Insights Condition on January 1st of each year beginning in 2026. We intend to provide resources, outreach efforts, and other communications to aid developers of certified health IT in understanding the Insights Condition requirements. Our goal is to ensure there is adequate time allotted for reporting, clarity related to requirements, and an ability to address developers' questions and educational needs well in advance of any reporting deadlines. We welcome comments on our proposal and welcome alternative approaches that helps us achieve this goal.

We include a table below as an example, and welcome comments on this approach and the proposed date, such as whether the date of January 1st should be earlier in the year (such as August 31st to align with Real World Testing eligibility date) [220] to allow more time for developers to assess whether or not it meets the minimum reporting requirements for the upcoming data collection period.

Table 1B. Dates and Actions for Insights Condition Data Collection and Attestation

Dates	Action
January 1, 2026 (annually thereafter)	Developers to assess whether they meet Insights Condition requirements as of this date
January 1 - December 31, 2026 (annually thereafter)	Data collection period for those who meet Insights Condition requirements
July 1 - July 31, 2027 (annually thereafter)	Submission window for reporting measures or attestation

We also propose in § 170.407(b)(2) that if developers update their certified health IT using Inherited Certified Status after January 1 of the year prior in which the responses are submitted, a health IT developer must include the newer version of the certified Health IT Module(s) in its annual responses to the Insights Condition of Certification. Many health IT developers update their certified Health IT Module(s) on a regular basis, leveraging the flexibility using Inherited Certified Status. This updating can cause an existing certified Health IT Module to be recognized as new within the Program due to the way ONC issues certification identifiers, and could result in existing certified Health IT Modules being inadvertently excluded from the Insights Condition requirements.

In the HTI–1 Final Rule (89 FR 1344), we stated that we intend to make responses (the metrics and required documentation) to the Insights Condition made publicly available on ONC's website. We also stated that if health IT developers wish to provide additional information as part of the optional documentation, we strongly encourage them to not include any proprietary, trade secret, or confidential information in their submission. We also indicated that we intend to provide a method for health IT developers to first indicate whether they plan to share proprietary, trade secret, and/or confidential information for purposes of either required or optional documentation, and if a health IT developer provided an affirmative indication, ONC would engage the developer in dialogue about potential alternative means of meeting either required documentation requirements or providing optional documentation (*e.g.,* in other generalized or descriptive ways that may achieve the same goal) (89 FR 1344 through 1345).

To improve alignment and consistency with ONC's other certification requirements, we propose to revise § 170.407(a)(1)(i)(B) to specify that documentation must be available via a publicly accessibly hyperlink instead. We note that this applies to both required and optional documentation. This avoids health IT developers from sharing any potential proprietary, trade secret, and/or confidential information with ONC. We note that this process is consistent with other documentation reporting processes that are part of the Program.

c. Minimum Reporting Qualifications

In the HTI–1 Final Rule (89 FR 1345 through 1346), we finalized minimum reporting qualifications in a way that does not unduly disadvantage small and startup developers of certified health IT. We finalized in § 170.407(a)(2) that a developer of certified health IT must have at least 50 hospital sites or 500 individual clinician users across the developer's certified health IT to report on the measure. We noted that the 50 hospital sites threshold is applicable to Health IT Modules used in inpatient or emergency department settings, while the 500 individual clinician users' threshold is applicable to Health IT Modules used in outpatient/ambulatory settings (non-inpatient). We propose to revise § 170.407(a)(2) by removing ''sites'' from hospital sites as the term could be misinterpreted.

[220] *See* HTI–1 Final Rule Inherited Certified Status 89 FR 1198

In addition, to ensure consistency in how health IT developers are interpreting and reporting on these terms, and to ensure there is no confusion regarding the types of hospitals and clinicians included, we clarify that the term ''hospital'' refers broadly to include various types of hospitals and is not limited to non-Federal acute care hospitals. This could include (but is not limited to) long term care hospitals, critical care hospitals, federally owned hospitals such as those operating under the U.S. Department of Veterans Affairs (VA), the U.S. Department of Defense (DOD), or the Indian Health Service (IHS), children's hospitals, psychiatric hospitals, etc. These hospitals could be identified with a CMS Certification number (CCN) or other unique identifier such as NPI or the American Hospital Association identifier.

We clarify the term ''clinician users,'' to include health care professionals consisting of a variety of backgrounds, including but not limited to:

- Physicians (including Doctor of Medicine, osteopathy, dental surgery, dental medicine, podiatric medicine, and optometry)
- Osteopathic practitioners
- Chiropractors
- Physician assistants
- Nurse practitioners
- Clinical nurse specialists
- Certified registered nurse anesthetists
- Physical therapists
- Occupational therapists
- Clinical psychologists
- Qualified speech-language pathologists
- Qualified audiologists
- Registered dietitians or nutrition professionals
- Clinical social workers
- Certified nurse midwives

Although we seek to broadly define both ''hospitals'' and ''clinicians'' we realize that there may be benefits to aligning these terms with existing definitions as these are known and have been utilized over time. We are considering various options regarding whether to align the minimum reporting qualifications with definitions established for hospitals and clinicians by CMS, or in the Public Health Service Act (PHSA). For example, we are considering referring to the definition of ''health care provider'' as defined in section 3000(3) of the PHSA for ''hospitals'', however, this definition may be too broad for the purposes of the Insights Condition. We are also considering the definition of ''clinicians'' as defined by CMS [221] in their Merit-based Incentive Payment System (MIPS) program which would provide alignment and scope for provider types but may also be too restrictive since we require reporting from developers beyond those participating under CMS programs. Although the types of clinicians we provided as examples above are defined by CMS as ''clinicians'', we do not wish to limit reporting for the Insights Condition to data that only relates to those participating in CMS programs given that many clinicians do not participate fully in these programs.[222] We seek comment on whether to keep our approach, or to align it with existing definitions to provide greater clarification and alignment with other requirements. Commenters are encouraged to specify alternatives that we should consider that would bring consistency and comparability across developers who will report under the Insights Condition. We are also considering and seek input from commenters on excluding clinicians who may only have an administrative role, which we would define as a clinician who does not treat patients. We note that this exclusion would not apply to a clinician conducting clinical research if the clinician directly treats patients.

d. Measure Updates

Individuals' Access to Electronic Health Information Through Certified Health IT Measure

In the HTI–1 Final Rule (89 FR 1314), we finalized the ''individuals' access to electronic health information through certified health IT'' measure in § 170.407(a)(3)(i), which states that if a health IT developer has a Health IT Module certified to § 170.315(e)(1) or (g)(10) or both, the developer must submit responses for the number of unique individuals who access electronic health information (EHI) overall and by different methods of access through certified health IT. We specified that the related metrics only count individuals' access to their EHI and stated in the HTI–1 Final Rule that we may incorporate patient-authorized representatives in future rulemaking (89 FR 1315). Therefore, we propose to revise § 170.407(a)(3)(i) to include both individuals and individuals' authorized representatives accessing their EHI (rather than just individuals alone).

We believe it would be beneficial to align our measure with the Medicare Promoting Interoperability Program (PI) Measure for patient access (''Provide Patients Electronic Access to Their Health Information''),[223] which counts access by patients or their authorized representatives for measuring patient access using portals or apps. Therefore, we propose to expand the measuring of access to include access by individuals or their authorized representatives in § 170.407(a)(3)(i). We do not expect this additional measurement specificity will add substantive development effort for health IT developers as this proposal would align with how CMS operationalizes their measure for patient access.

C–CDA Reconciliation and Incorporation Through Certified Health IT Measure

In the HTI–1 Final Rule (89 FR 1317), we finalized the ''consolidated clinical document architecture (C–CDA) problems, medications, and allergies reconciliation and incorporation through certified health IT'' measure in § 170.407(a)(3)(ii). The measure is intended to capture the use of C–CDAs in alignment with capabilities specified for the ''clinical information reconciliation and incorporation'' certification criterion in § 170.315(b)(2). Given the proposed updates to § 170.315(b)(2) discussed elsewhere in this proposed rule, we also propose conforming updates for this measure to ensure alignment with the certification criterion. We refer readers to section III.B.7 of this proposed rule for detailed discussion on the proposed revisions specific to § 170.315(b)(2). Therefore, we propose to revise the name of this measure to ''C–CDA reconciliation and incorporation through certified health IT'' in § 170.407(a)(3)(ii).

In further alignment with the proposed revisions to the certification criteria in § 170.315(b)(2), we propose to require developers to submit responses on specific data classes and elements from C–CDA documents obtained and subsequently reconciled and incorporated both through manual and automated processes in § 170.407(a)(3)(ii)(E). Note, given this proposal, we propose to make conforming grammatical edits to the list structure in § 170.407(a)(3)(ii)(C) and (D) to accommodate the proposed addition of (E). If finalized as proposed in § 170.407(a)(3)(ii)(E), we would also provide technical updates resulting in

[221] *https://qpp.cms.gov/mips/how-eligibility-is-determined.*

[222] Apathy NC, Everson J. High Rates of Partial Participation in The First Year of The Merit-Based Incentive Payment System. Health Aff (Millwood). 2020 Sep;39(9):1513–1521. doi: 10.1377/hlthaff.2019.01648. PMID: 32897783; PMCID: PMC7720898.

[223] *https://qpp.cms.gov/docs/pi_specifications/Measure%20Specifications/2023MIPSPIMeasuresProvidePatientsElectronicAccess.pdf.*

additional metrics in the accompanying measure specification sheet which we discuss in further detail below under ''technical updates.''

To provide adequate time for associated technical development and then reporting, we propose in § 170.407(b)(1)(i)(D) that any metrics in the accompanying measure specification sheet related to § 170.407(a)(3)(ii)(E) would be reported beginning July 2030, with data collection starting in 2029. We expect that several developers would likely provide information similar to the metrics described above in their 2023 Real World Testing Results, which would indicate the feasibility of generating these metrics.[224] We welcome comments on our proposals.

Technical Updates in Measure Specification Sheets

As proposed above, the proposed ''individuals' access to electronic health information through certified health IT'' measure consists of three metrics, as specified in the measure specification sheet, one of which is the number of unique individuals who accessed their EHI using technology certified to the ''standardized API for patient population services'' under § 170.315(g)(10). As we stated in the HTI–1 Final Rule (89 FR 1313), the measure specification sheets provide granular definitions and other information needed to operationalize the metrics to ensure they are implemented in a consistent manner across health IT developers. In the measure specification sheet, we defined measuring access to EHI for this measure by counting an individual's authorization, as indicated by an access token, at least once during the reporting period.[225] We intend to modify this definition in an updated version of the measure specification sheet as a technical update as it does not change the substance of this measure, since there may be instances where individuals authorize access to their data (via an access token) but no requests are made to retrieve the data. Given that our intent is to measure individuals' access to EHI (versus just authorizing access), we plan to update this definition in the measure specification sheet for this metric to further specify that access to EHI should be measured by counting the number of individuals where at least one FHIR resource was returned when using the ''standardized API for patient population services'' under § 170.315(g)(10) during the reporting period.

We request comment on whether this definition should be updated in the measure specification in this manner, or alternatively, whether we should update it so that access to EHI is measured by counting the number of individuals where at least one FHIR request was made to access information using the ''standardized API for patient population services'' under § 170.315(g)(10) during the reporting period. We acknowledge that there may be concerns related to defining in terms of FHIR requests as we may technically be including unauthorized requests as a measure of access to EHI. We welcome comments and suggestions regarding modifying the original definition. As stated above, our website at the following link (*www.healthit.gov/proposedrule*) will have an accompanying measure specification sheet reflecting the technical specifications related to the substantive proposals in this proposed rule for commenters to view and consider. We refer readers to the HTI–1 Final Rule (89 FR 1312) where we explained that while the substantive requirements for each measure are defined through rulemaking, we determined that measure specification sheets are a logical and accessible method for the public to view the technical specifications that support those requirements.

We stated in the HTI–1 Final Rule (89 FR 1322) that if regulatory baselines associated with the metrics change in the future—such as a revision to a criterion through notice and comment rulemaking—the measure specification would also be changed to ensure alignment with the revised criterion. Therefore, we expect to update the metrics for the proposed ''C–CDA reconciliation and incorporation through certified health IT'' measure, within the accompanying measure specification sheet to align with the proposed broader set of data referenced by the criterion specified in § 170.315(b)(2) if finalized as proposed. As stated above, the accompanying measure specification sheet reflecting the technical updates to align with the proposed broader set of data in this proposed rule will be available on ONC's website for review to support public comment in a transparent manner. Specifically, we intend to replace references in the measure specification sheet for problems, medications, and allergies and intolerances with a reference to the proposed data specified in § 170.315(b)(2) and, consistent with the policy established in the HTI–1 Final Rule (see 89 FR 1312), we intend to continue to align measure specification sheets with any modifications to certification criteria finalized via notice and comment rulemaking—in this instance, specifically for § 170.315(b)(2). The specific data classes and elements proposed in § 170.407(a)(3)(ii)(E), that we intend to list in the measurement specification sheet as technical updates, are selected from the additional data that would be included in proposed § 170.315(b)(2) listed below:

- The data elements Substance (Medication) and Substance (Drug Class) in the Allergies and Intolerances data class.
- The data elements Patient Goals and SDOH Goals in the Goals data class.
- The data element Immunizations in the Immunizations data class.
- The data element Values/Results in the Laboratory data class
- The data element Medications in the Medications data class.
- The data element Unique Device Identifier—Implantable for a patient's implantable device(s) in the Medical Devices data class.
- The data element Assessment and Plan of Treatment in the Assessment and Plan of Treatment data class.
- The data element Problems and SDOH Problems/Health Concerns in the Problems data class.

We would provide technical updates resulting in additional metrics in the accompanying measure specification sheet that capture (1) the number of specific data elements obtained in the reporting period, and (2) the reconciliation of specific data, such as the number of problems reconciled and incorporated by various means. Together, this data would allow ONC to calculate how often problems and other data elements are reconciled and incorporated by various means using the number of each data element obtained and other existing metrics (such as the number of encounters) as denominators. We request comment on whether that approach would provide beneficial information commensurate with the potential burden for developers.

Given the number of data elements that Health IT Modules certified to

---

[224] *https://www.eclinicalworks.com/wp-content/uploads/2024/01/eCW-Real-World-Testing-2023-Results-Report-Jan-2024.pdf.*

https://www.epic.com/content/epiccare2023results.pdf.

https://www.oracle.com/a/ocom/docs/industries/healthcare/2023-cerner-real-world-testing-results.pdf.

https://www.azaleahealth.com/wp-content/uploads/2024/01/2023-RWT-Results-Report-Azalea-EHR.pdf.

https://cantatahealth.com/wp-content/uploads/2024/01/Cantata-Health-Real-World-Testing-Results.pdf.

[225] *https://www.healthit.gov/sites/default/files/page/2023-12/Measure_Spec_Individual_Access_508.pdf.*

§ 170.315(b)(2) would be able to reconcile and incorporate following the proposed revisions for the certification criteria, we have specified a limited set of Data Elements and Data Classes for which developers would count the number of Elements obtained and the number of Elements reconciled and incorporated for the Insights Condition in the measurement specification accompanying this proposed rule. We request comment on the specific Data Classes or Elements on which such metrics should focus. For instance, metrics specifically focused on reconciliation of medications may provide the most value in informing how often medication information is updated to accurately reflect care received from other organizations and allow for effective decision support; in contrast, metrics on reconciliation and incorporation of vital signs may provide relatively limited value.

We also request comment on whether metrics should focus on specific data elements or should aggregate data elements to the data class level. For example, it may be more valuable and feasible to include a metric on the aggregate total number of substance (Medication) and substance (Drug Class) data elements within the Allergies and Intolerances data class rather than two separate metrics, one focused on Substance (Medication) and another focused-on Substance (Drug Class). We request comment on the feasibility and value of separate metrics by Data Element and aggregate elements by some or all Data Elements within a Data Class, which may differ by specific Element and Class.

We are also considering approaches to capture use of the proposed requirements for § 170.315(b)(2), if finalized as proposed, to support automatic reconciliation and incorporation in the accompanying measure specification sheet. As in prior versions of the measurement specification, the metric on the number of total C–CDAs obtained equals the sum of the metric on the number of total C–CDA documents obtained that were pre-processed and the metric on the number of total C–CDA documents obtained that were not pre-processed. We clarify that all documents for which reconciliation and incorporation is completed through fully automated processes would be considered to have been pre-processed for the purpose of this metric.

The measurement specification sheet further differentiates four metrics for pre-processed C–CDA documents: the first and second metrics respectively count pre-processed C–CDA documents that had data reconciled and incorporated via manual processes and fully automated processes, and the third and fourth metrics respectively count pre-processed C–CDA documents that were determined to have no data that modifies the patient record through manual processes and fully automated processes. These four metrics address pre-processed C–CDA documents that are manually acted upon or fully automated for reconciliation and incorporation but do not capture those C–CDAs that were obtained and pre-processed but not further acted upon by manual or fully automated processes.

The metric on the number of total C–CDA documents obtained that were not pre-processed is further differentiated by two metrics: the first metric counts C–CDA documents that were not pre-processed that had data reconciled and incorporated via manual processes, and the second metric counts C–CDA documents that were not pre-processed that were determined to have no data that modifies the patient record through manual processes. These two metrics account for all C–CDAs that are obtained, not pre-processed, and are then acted upon and do not include those C–CDAs that are obtained, not pre-processed, and not acted upon. While these sets increase the number of metrics to report, we believe they will clarify and simplify measuring and categorizing C–CDA documents.

In the HTI–1 Final Rule, we defined ''Reconciled and Incorporated via Any Method'' to be an approach to reconciling and incorporating information in the Health IT Module, including but not limited to, manual processes performed by a clinician or their delegate only; a mix of manual and automated processes; or fully automated processes (89 FR 1319). Given the focus on automatic reconciliation and incorporation capabilities in this proposed rule for § 170.315(b)(2), we anticipate aligning the measure specification sheet by dividing the metrics that call for reporting on the total number of C–CDA documents that were reconciled and incorporated by ''any method'' into two categories: (1) C–CDA documents where data were reconciled and incorporated via manual processes performed by a clinician or their delegate only; and (2) a C–CDA documents where any data was reconciled and incorporated via fully automated processes. These additional metrics are intended to generate insight into the use of automatic capabilities and how often C–CDAs are reconciled and incorporated by fully automatic means.

We have chosen these two categories to capture instances where the reconciliation and incorporation process is at least partly completed by automated means and because we believe that instances in which *all* data contained in a C–CDA are reconciled and incorporated via fully automated processes will be rare given the scope of data proposed to be included in the proposed § 170.315(b)(2). Alternatively, we could include an additional metric in the measure specification sheet to capture documents in which data is reconciled and incorporated through a mix of manual and automated processes, which would occur, for example, when problems were reconciled by automated processes and medications were reconciled by manual processes.

We also intend to complement the existing metric focused on C–CDA documents that were determined to have no new information by pre-processes or fully automated processes with an additional metric. The additional metric would capture the number of C–CDA documents that were determined to have no new information by manual processes performed by a clinician or their delegate only. These two metrics focused on determining that there was no new information would therefore directly mirror the two metrics focused on reconciliation and incorporation following pre-processes. In revising these metrics, we are also considering alternatives that would describe the varied ways in which data contained within C–CDAs could lead to modification or reconciliation with the patients record. We request comment on whether metrics in the updated measure specification sheet that include the term 'no new data' clearly exclude instances where information in C–CDAs lead to a change to the patient's record. For example, if information in the patient record is deleted or modified in response to information in the C–CDA, the intention is that this be counted as an instance where information is reconciled and incorporated (either via manual or automated processes) and NOT as an instance where documents were determined to have no new data. If the current metrics are not clear, would it be more effective to revise the metrics on ''no new data'' as listed below:

- Number of total C–CDA documents obtained that were pre-processed and determined to have no data specified in § 170.315(b)(2) that modifies the patient record by manual processes performed by a clinician or their delegate.
- Number of total C–CDA documents obtained that were pre-processed and

determined to have no data specified in § 170.315(b)(2) that modifies the patient record by pre-processes or fully automated processes.

- Number of total C–CDA documents obtained that were not pre-processed and determined to have no new data specified in § 170.315(b)(2) that modifies the patient record via manual processes performed by a clinician or their delegate only.

As noted earlier, please see the measure specification sheet that will be posted on ONC's website for review.

We request public comment on the definitions provided in that measure specification sheet for manual processes, and fully automated process as well as the feasibility of separately measuring those processes. We also request comment on whether the resulting separate metrics would effectively capture the use of the proposed new capabilities to automatically reconcile and incorporate information for § 170.315(b)(2), and request comment on the value of including a metric capturing when a ''mix'' of automated and manual processes were used to reconcile and incorporate data.

We also plan to make a technical update by revising the number of unique patients with an associated C–CDA document measure to instead capture the number of unique patients with an encounter and associated C–CDA document. The revised metric would be a direct subset of the existing metric Number of Unique Patients with an Encounter. The current metric comprehensively captures the number of patients with C–CDAs but may include some C–CDAs for patients who are not treated by a provider using the product during the reporting period. We do not anticipate any change in burden, and are requesting comment on the relative value of the altered metric.

In the HTI–1 Final Rule (89 FR 1326), we finalized the ''use of FHIR in apps through certified health IT'' in § 170.407(a)(3)(iv). This measure captures the volume and type of FHIR resources transferred to apps from certified health IT relative to the number of active certified API technology deployments. We intend to make a technical update in the accompanying measure specification sheet to provide additional implementation information specifying that reporting by user type should be done according to three mutually exclusive categories: patient-facing only, non-patient facing only, and both patient-facing and non-patient facing.

In the HTI–1 Final Rule (89 FR 1332), we finalized the ''immunization administrations electronically submitted to immunization information systems through certified health IT'' measure in § 170.407(a)(3)(vi). We stated that this measure would report on the volume of immunization administrations electronically submitted to an immunization information system through certified health IT. In the accompanying measure specification sheet, we indicated that the number of immunizations administered that were electronically submitted successfully to IISs overall was defined as the total number of messages submitted to IISs, minus acknowledgements with the error of severity level E. We intend to make a few technical updates to this measure specification sheet. First, we intend to add metrics to separately count the number of immunizations administered electronically submitted to IISs that returned with an acknowledgement with the error of severity level E during the reporting period overall, and by IIS and age category. These additional metrics would enable us to identify potential issues associated with submissions to the IIS. We do not expect any additional burden associated with reporting this metric. We also request comment on the value and burden associated if we have the metrics count the immunizations administered electronically returned by their acknowledgement code (by IIS and age) instead, which would allow us to understand the number of messages that were rejected, had errors, and were accepted by IIS and age.

We also intend to make another technical update to the measure specification sheet by adding metrics to separately count the number of immunizations administered that were electronically submitted to IIS where an acknowledgement from an IIS is not received by certified health IT overall, and by IIS and age category. The current measure specification sheet indicates health IT developers optionally report on number of submissions that did not receive acknowledgement as part of the supplemental documentation. These separate metrics would enable monitoring the occurrence of these communication failures between certified health IT and IIS more systematically. We do not expect substantive additional burden associated with this metric. We also request comment on the value and burden associated with reporting a count of the subset of messages sent to third party intermediaries where the third-party intermediary does not provide an acknowledgement that the message was sent to an IIS. Finally, we intend to make a technical update that would clarify that the immunization administration submitted would include HL7 Z22 messages, and request comment on this approach. This aligns with the ''immunization history and forecasts through certified health IT'' measure specification sheet where we indicate that ''the successful response received from IIS'' include HL7 Z42 and Z32 messages.

In the HTI–1 Final Rule (89 FR 1336), we finalized the ''immunization history and forecasts through certified health IT'' measure in § 170.407(a)(3)(vii). This measure captures the use of certified health IT to query information from an IIS under the ''transmission to immunization registries'' (§ 170.315(f)(1)) criterion. In the accompanying measure specification sheet, we indicated that the number of immunization queries sent to IISs overall metric would be defined as the total number of messages sent to IISs, minus acknowledgements with errors (severity level E). We intend to make a technical update and modify this definition in the measure specification sheet as it does not change the substance of this measure. We plan to update this definition so that the number of immunization queries sent to IISs overall metric should be measured by only counting the total number of immunization queries sent to IISs during the reporting period. This metric no longer requires subtracting the number of acknowledgements with the error of severity level E. Instead, we are adding separate metrics in the measure specification sheet which would report on the total number of queries responses that returned with acknowledgements that had an error of severity level E, overall and by IIS, during the reporting period. This would enable us to understand how many queries were rejected by an IIS (as indicated by an ''E'' code) during the reporting period. We do not expect any additional burden associated with metric. We also plan to make a technical update to the definition of ''queries sent'' to IISs such that the definition of queries sent applies to HL7 Z34 and HL7 Z44 messages. This approach would provide consistency in how queries sent are defined across developers. Additionally, it would align the definition of ''queries sent'' with ''successful response received from IIS,'' which is based upon the receipt of HL7 Z42 and Z32 messages. We also request comment on the value and burden associated if we have the metrics count the query responses returned by their acknowledgement code (by IIS) instead,

which would allow us to understand the number of queries sent where data was found, no data was found, or multiple candidates exist, or where query messages that were rejected, had errors, and were accepted by IIS.

In the HTI–1 Final Rule (89 FR 1338) we also received a couple comments noting that a significant portion of messaging failures are communication failures where there will be no response received. A commenter suggested that messages with no response from the IIS (in the case of downtime, for example) would be considered successful (89 FR 1338). In response, we stated that at this time, we will not require health IT developers to provide separate counts for communication failures and counts of the descriptive context levels, and encouraged developers capture information about communication failures as their functionality permits and include this explanation in the supplemental documentation. We also stated that we would collaborate with the community to monitor how these instances impact the measure's interpretation and determine if it should be revised in the future.

Given the potential value of understanding the frequency of these communication failures, we plan to make a technical update in the accompanying measure specification sheet to create additional metrics which would report on the total number of queries sent but where no acknowledgement was received from the IIS overall, and by IIS. The separate metric to count no acknowledgements would allow us and the CDC to monitor the occurrence of these communication failures between certified health IT and IIS rather than relying on supplemental reporting to gather this information. We do not expect substantive additional burden associated with this metric. We also request comment on the value and burden associated with reporting a count of the queries sent to third party intermediaries where the third-party intermediary does not provide an acknowledgement the query was sent onto an IIS.

2. Attestations Condition and Maintenance of Certification Requirements

The Cures Act amended section 3001(c)(5) of the PHSA by adding the requirements 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 EHI. In the ONC Cures Act Final Rule, we established both Assurances (§ 170.402) and Attestations (§ 170.406) Conditions and Maintenance of Certification requirements (88 FR 75718 and 88 FR 25781, respectively).

In the HTI–1 Proposed Rule (88 FR 23782) and Final Rule (89 FR 1237), we proposed and finalized the adoption of the certification criterion, ''decision support interventions'' in § 170.315(b)(11) as part of the ''care coordination certification criteria,'' in § 170.315(b). In the HTI–1 Final Rule, we narrowed the overall scope of technologies impacted by finalized requirements in § 170.315(b)(11) (89 FR 1251 through 1252). We finalized minimal, uniform requirements for all Health IT Modules certified to § 170.315(b)(11) while also maintaining a construction that enables a developer of certified health IT to certify a Health IT Module to § 170.315(b)(11) without being obligated to author, develop, or otherwise directly provide Predictive DSIs to its customers. Specifically, we finalized a configuration nexus for several requirements in § 170.315(b)(11) that centered on whether the developer of certified health IT supplied a Predictive DSI as part of its Health IT Module.

We also finalized in the HTI–1 Final Rule a supportive Maintenance of Certification requirement as part of the Assurances Condition of Certification in § 170.402(b) for § 170.315(b)(11). We finalized in § 170.402(b)(4) that starting January 1, 2025, and on an ongoing basis, developers of Health IT Modules certified to § 170.315(b)(11) must review and update, as necessary, source attribute information in § 170.315(b)(11)(iv)(A) and (B), risk management practices described in § 170.315(b)(11)(vi), and summary information provided through § 170.523(f)(1)(xxi) (89 FR 1253 through 1254). These policies establish ongoing requirements for developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) to address circumstances where a developer chooses to supply a Predictive DSI as part of its Health IT Module after its initial certification to § 170.315(b)(11), as well as circumstances where a developer that formerly supplied a Predictive DSI as part of its Health IT Module when initially certifying to § 170.315(b)(11) no longer chooses to do so.

We propose to add a conforming update to the Attestation Condition of Certification by revising § 170.406(a)(2) to address the Assurance Maintenance of Certification requirement in § 170.402(b)(4). We note that as a function of providing attestations twice yearly, developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) would be expected to affirm conformance to the Assurances Maintenance of Certification requirement in § 170.402(b)(4); specifically, they would attest that they have reviewed and updated, as necessary, the required attribute information and documentation during the time covered by the attestation. We welcome comment on this proposal.

D. Administrative Updates

1. Program Correspondence

We propose to revise the Program correspondence provision (§ 170.505(a)(2)) to clarify that under Program regulations, the applicant for ONC-Authorized Testing Lab (ONC–ATL) status, the applicant for an ONC-Authorized Certification Body (ONC–ACB), an ONC–ONC–ACB, an ONC–ATL, health IT developer or any party to proceeding under subpart E of part 170 will be considered to have received correspondence or other written communications from ONC or the National Coordinator when the first of the following three scenarios occurs: (1) the date on which ONC or the National Coordinator receives a response to the correspondence via written or verbal communication methods; (2) the date of the delivery confirmation to the address on record for correspondence sent by express or certified mail; or (3) the date of the seventh business day after the date on which the email, express, or certified mail was sent.

ONC explained in the ONC Cures Act Proposed Rule preamble that ''we consider a 'business day' to include the normal workdays and hours of operation during a week (Monday through Friday), excluding Federal holidays and weekends.'' [226] We propose to codify in 45 CFR 170.102 a definition of ''business days'' that would include the same days as our explanation in the ONC Cures Act Proposed Rule. ONC's definition of business days for purposes of 45 CFR part 170 would also include those days on which the Office of Personnel Management has announced that Federal agencies in the Washington, DC area are closed, reflecting the nationwide scope of the Program. The ''business days'' definition proposed in § 170.102 would provide clarity about

[226] *https://www.federalregister.gov/d/2019-02224/p-889.*

which days would be counted when determining the date of the seventh business day after the date on which the email, regular, express, or certified mail was sent, as proposed in § 170.505(a)(2)(iii).

In the ONC Cures Act Proposed Rule at 84 FR 7503, referencing a statement the Enhanced Oversight and Accountability Final Rule (EOA Final Rule) (81 FR 72404), we signaled our intent to send notices of potential non-conformity, non-conformity, suspension, proposed termination, and termination *via certified mail* (81 FR 72429). We solicited comments on the ONC Cures Act Proposed Rule regarding the nature and types of non-conformities with the Conditions and Maintenance of Certification requirements that ONC should consider in determining the method of correspondence. Specifically, we asked whether certain types of notices under direct review should be considered more critical than others and, thus, might require a specific method of correspondence (84 FR 7504). In the ONC Cures Act Final Rule, we finalized the proposal to use the provisions in § 170.505 for correspondence regarding compliance with the Conditions and Maintenance of Certification requirements with minor revisions outlining specific considerations for when we would provide notice beyond email (85 FR 25784).

When we finalized our proposal in the ONC Cures Act Final Rule, we did not anticipate the several challenges we encountered with certain correspondence beyond email during the COVID–19 pandemic. As the volume of correspondence and communication required to fulfill ONC review and enforcement responsibilities for the Conditions and Maintenance of Certification requirements (subpart D of 45 CFR part 170) has increased, we have experienced difficulties with delivery of paper-based correspondence that we did not experience with email.

To avoid undue delays in addressing non-conformities with Program requirements or resolving other matters, we propose in § 170.505(a)(2)(iii) that seven business days after a written communication is sent is the latest of three dates on which we would consider the communication to have been received by the recipient. In § 170.505(a)(2)(i), where we receive a communication from the ONC–ACB, ONC–ATL, applicant, developer, or other party in response to a written correspondence, we believe that response is sufficient to demonstrate the communication has been received. Similarly, in § 170.505(a)(2)(ii) a delivery confirmation date, such as from the United States Postal Service (USPS) for certified mail, that is fewer than seven business days after the communication was sent would be considered the day the communication was received.

We welcome comments on this proposal and whether we should consider moving away from using non-electronic means of communication for anything except courtesy copies of communications.

2. ONC-Authorized Certification Bodies (ACB) Surveillance of Certain Maintenance of Certification Requirements

a. Background and Proposal Summary

To better support health IT developers' ability to consistently meet their obligations under subpart D of 45 CFR part 170, we propose to adopt new requirements in § 170.523 principles of proper conduct (PoPCs) for ONC–ACBs and new procedures for in-the-field surveillance of the maintenance of certification for Health IT in § 170.556 that would build on ONC–ACBs' existing surveillance responsibilities and obligations. More specifically, we propose to adopt new surveillance reporting requirements in § 170.523(i), reporting for corrective action plan (CAP) non-compliance in § 170.523(x), new oversight responsibilities of certain Maintenance of Certification requirements in § 170.523(p) and (q), new and revised surveillance requirements in § 170.556(b), and new and revised procedures for CAPs in § 170.556(d).

We believe these proposed new and revised surveillance and PoPC requirements would promote Program efficiency and encourage Program-participating developers to maintain, or when necessary, regain, conformity with Program requirements for the applicable Maintenance of Certification requirements as required by the Program regulations promulgated under the Cures Act. Section 4002(a) of the Cures Act amended section 3001(c)(5) of the PHSA by adding paragraph (c)(5)(D), which requires the Secretary, through notice and comment rulemaking, to require certain conditions of certification and maintenance of certification for the Program. In the ONC Cures Act Final Rule, we established Conditions and Maintenance of Certification requirements pursuant to PHSA 3001(c)(5)(D)(i) through (vi) in subpart D of 45 CFR part 170 (85 FR 25783). In the HTI–1 Final Rule, we established the Insights Condition and Maintenance of Certification requirements (§ 170.407) pursuant to PHSA 3001(c)(5)(D)(vii) and the Assurances Maintenance of Certification requirement for health IT developers to update and provide their Health IT Modules (§ 170.402(b)(3). We also established in § 170.402(b)(4) an Assurances Maintenance of Certification requirement for Predictive Decision Support Intervention transparency (89 FR 1371), and in section III.C.2 of this proposed rule, we propose to establish a conforming update to the Attestation Condition and Maintenance of Certification in § 170.406(a)(2) to address the adopted § 170.402(b)(4) DSI Maintenance of Certification requirement.

In addition to the Conditions and Maintenance of Certification requirements, in the ONC Cures Act Final Rule we established that ONC would enforce compliance with the 45 CFR subpart D Condition and Maintenance of Certification requirements (85 FR 25783). However, we also established ONC–ACB responsibilities (PoPCs). These responsibilities included the review and approval for submission of developers' § 170.406 attestations (§ 170.523(q)) and § 170.405 real world testing plans and results (§ 170.523(p)) (85 FR 25951). The ONC Cures Act Final Rule also established a PoPC in § 170.523(s) requiring ONC–ACBs to report any information that could inform whether ONC should exercise direct review of noncompliance with the Conditions and Maintenance of Certification requirements to ONC (85 FR 25783).

ONC–ACBs' PoPC responsibilities under the currently codified requirements in § 170.523(p) have encouraged and helped Program-participating developers to achieve a high rate of compliance with the real world testing Maintenance of Certification requirements in § 170.405. Under § 170.523(p), ONC–ACBs are required to confirm the completeness of developers' real world testing plans and results, and to confirm the developer timely submitted materials for public availability in accordance with § 170.405(b). We believe a similarly supportive dynamic exists for developers' compliance with attestations requirements in § 170.406 and insights reporting requirements in § 170.407, for which ONC–ACBs have explicitly aligned PoPC responsibilities as described in § 170.523(q) and (u).

Informed by our experience with ONC–ACB support in monitoring and encouraging developers' compliance with certain 45 CFR 170 subpart D requirements over the past three years, and pursuant to the authority in PHSA

section 3001(c)(5)(E) to ''encourage compliance with the conditions of certification,'' we now propose new ONC–ACB PoPC requirements in § 170.523 to encourage and support developers' compliance with Maintenance of Certification requirements in § 170.402 and 170.404. In parallel, we propose to update ONC–ACBs' responsibilities for conducting reactive surveillance in accordance with § 170.556(b) and working with developers to encourage remediation of observed non-conformities with Program requirements in § 170.556(d).

Our proposal in § 170.556(b) would require ONC–ACBs to initiate surveillance when they become aware of facts or circumstances that would cause a reasonable person to question whether a health IT developer has satisfied certain Maintenance of Certification requirements. As a result of our proposals in § 170.556(b) and additional proposals in § 170.523(i), we are proposing to require ONC–ACBs perform reactive and randomized surveillance based on the specified Maintenance of Certification requirements in §§ 170.402(b)(1)–(4), 170.404(b)(1) and (2), 170.405(b)(1) and (2), 170.406(b), and 170.407(b). In case of non-conformities, we would require an ONC–ACB to notify health IT developers and require a CAP, in addition to the existing requirements in § 170.556 consistent with their accreditation under PoPCs in § 170.523(a) and ISO/IEC 17065. In § 170.556(d), we further propose revisions to the required elements of a CAP for identified non-conformities with respect to Program requirements codified in subpart D for which we propose an ONC–ACB would have responsibility under § 170.523. Under these proposals in § 170.523 and § 170.556, an ONC–ACB would have the duty to confirm a health IT developer's compliance with, and initiate surveillance whenever it becomes aware of each non-conformity to, the Maintenance of Certification requirements in §§ 170.402(b)(1)–(4), 170.404(b)(1) and (2), 170.405(b)(1) and (2), 170.406(b), and 170.407(b).

b. Updates to Principles of Proper Conduct for Maintenance of Certification Requirements

In the ONC Cures Act Final Rule, we adopted Conditions and Maintenance of Certification requirements for health IT developers outlined in section 4002 of the Cures Act (85 FR 25717) and implemented them with further specificity in the Program, expressing initial and ongoing certification requirements for the health IT developers and their certified health IT products (85 FR 25718). We adopted certain responsibilities for the ONC–ACB's to ensure developers have met their obligations for certain Conditions and Maintenance of Certification requirements. We also provided that, if the monitoring processes implemented by ONC–ACBs are not adhered to by developers, the ONC–ACB, in accordance with Program reporting requirements, should follow its processes to institute a CAP. Should the developer fail to engage in the CAP process the ONC–ACB would alert ONC of the developer's failure to comply with the Conditions and Maintenance of Certification requirements (85 FR 25720 through 25721).

To ensure developers of health IT were meeting the requirements of the Program, we adopted requirements for ONC–ACBs in § 170.523. Specifically, we adopted PoPCs for ONC–ACBs in §§ 170.523(m), 170.523(p), 170.523(q), and 170.523(t) that aligned with certain Maintenance of Certification requirements, tasking ONC–ACBs to review and confirm certain information is submitted by health IT developers in response to the real world testing and attestation Maintenance of Certification requirements. ONC–ACBs are required to share additional information, as it relates to certain Maintenance of Certification requirements, with the National Coordinator regarding developer compliance with Program requirements (85 FR 25784 through 25785).

We now propose to expand an ONC–ACB's responsibilities to require additional oversight of certain Maintenance of Certification requirements be included in the ONC–ABC's surveillance reports and to provide certain documentation to the National Coordinator as part of its surveillance. We propose new PoPC requirements for ONC–ACBs specifically aligned to encourage transparency and support developers' compliance with Maintenance of Certification Requirements in 45 CFR part 170 subpart D, including redesignating § 170.523(p) through (u) as paragraphs (r) through (w). We propose to revise § 170.523(p) to add new requirements that ONC–ACBs verify and confirm a health IT developer's compliance with Attestation Maintenance of Certification requirements in accordance with § 170.402(b), and revise § 170.523(q) to add oversight requirements for developer compliance with API Maintenance of Certification requirements in accordance with § 170.404(b). Our proposed redesignation would mean the current requirements in § 170.523(p) real world testing, § 170.523(q) attestations, § 170.523(r) test results from ONC–ATLs, § 170.523(s) information for direct review, § 170.523(t) Health IT Module voluntary standards and implementation specifications updates notices, and § 170.523(u) insights would be shifted to § 170.523(r), (s), (t), (u), (v), and (w), respectively. We note that we do not propose to revise the requirements in proposed § 170.523(r), (s), (t), (u), (v) or (w) (currently codified as § 170.523(p), (q), (r), (s), (t), and (u), respectively).

Under these proposals in § 170.523, we would require that an ONC–ACB confirm and verify a health IT developer's compliance with the requirements in §§ 170.402(b)(1)–(4), 170.404(b)(1) and (2), 170.405(b)(1) and (2), 170.406(b), and 170.407(b) and, where a non-conformity rather than compliance is observed, to initiate surveillance in accordance with our proposals in § 170.556 (discussed in III.D.2.c below) and notify the health IT developer of each observed non-conformity. Each proposal in § 170.523(p) references a corresponding requirement for health IT developers in § 170.402(b), so that requirements in § 170.523(p)(1) references § 170.402(b)(1), our proposal for § 170.523(p)(2) references § 170.402(b)(2) and (b)(3), and our proposal for § 170.523(p)(3) references § 170.402(b)(4). Health IT developer requirements in § 170.404(b)(1) and (2) are also incorporated into our proposals for APIs in § 170.523(q). Similarly, the insights requirement in § 170.523(w) (finalized in the HTI–1 Final Rule as § 170.523(u) (89 FR 1435)) for ONC–ACBs was proposed and finalized simultaneously with corresponding developer requirements for Insights Condition and Maintenance of Certification requirements in § 170.407.

We propose to limit the ONC–ACB oversight requirements to those certain Maintenance of Certification requirements mentioned above because of the administrative nature of these requirements (comparative to requiring, for example, investigation, analysis, or assessment). As stated above, ONC–ACBs already have responsibilities in § 170.523(p), (q), and (u) (which we propose to shift to § 170.523(r), (s), and (t), respectively) to verify and confirm that developers are meeting their obligations in §§ 170.405(b)(1) and (2), 170.406, and 170.407. These Maintenance of Certification requirements require developers to submit documentation to ONC–ACBs, notify ONC–ACBs when a non-

conformity arises during real world testing, and provide an attestation for compliance with certain certification criteria under the Program. We consider these obligations as strictly administrative, and their successful completion does not implicate developer behaviors that rise to the level of oversight that would be necessary for initial ONC review. Likewise, we consider the Maintenance of Certification requirements in §§ 170.402(b)(1)–(4) and 170.404(b)(1) and (2) to also be administrative in nature. We believe the proposed addition of § 170.402(b)(1)–(4) in § 170.523(p)(1)–(3) and § 170.404(b)(1) and (2) in § 170.523(q)(1) and (2) is suitable considering the ONC–ACBs experience with confirming and verifying that a developer has met the requirements in §§ 170.405(b)(1) and (2), 170.406, and 170.407.

We note that we do not propose to include in § 170.523 the oversight of a health IT developer's compliance with the requirements in § 170.401, Information Blocking, and § 170.403(b), Communications Maintenance of Certification requirements. Unlike the requirements in § 170.402(b)(1)–(4) and § 170.404(b)(1) and (2), which we consider administrative, the oversight and enforcement of Information Blocking addresses practices that interfere with the access, exchange or use of EHI, and the Communications Maintenance of Certification requirements focuses on the update of agreements with clients that could limit ongoing collaboration and coordination. These Maintenance of Certification requirements compel developers to design, implement, and maintain business practices that align with ONC standards, facilitate data exchange, and actively engage in practices that ensure that their products remain compliant. Centralizing the oversight of these Maintenance of Certification requirements under ONC removes the possibility of having these conflicts, ensuring a standardized and consistent approach to enforcing these requirements.

While we consider the ONC–ACBs' Maintenance of Certification responsibilities as administrative, we also believe transparency is important regarding all Program requirements and propose to revise and add new PoPC surveillance reporting requirements for ONC–ACBs in § 170.523(i). As discussed, in § 170.556(b) and (d) we propose to add the Maintenance of Certification requirements proposed in § 170.523 to the ONC–ACBs' surveillance responsibilities. We propose that this responsibility would include initiating surveillance (§ 170.556(b)(2) and (3)), initiating CAP procedures (§ 170.556(d)(1)), initiating suspensions (§ 170.556(d)(5)) when a developer fails to engage with the CAP process for Maintenance of Certification non-conformities, and withdrawals (§ 170.556(d)(6)) when the health IT developer does not complete the actions necessary to reinstate the suspended certification (we refer readers to section III.D.2.c below for a discussion of these proposals). To better achieve transparency of the proposed surveillance activities, we propose to revise § 170.523(i)(2)(iii) to require ONC–ACBs, when conducting surveillance of certified health IT in accordance with their accreditation, to include the Maintenance of Certification requirements it surveilled in its quarterly surveillance results report.

We also propose to add a requirement in § 170.523(i)(4) that an ONC–ACB, as part of its responsibilities to conduct surveillance of certified health IT in accordance with its accreditation, and proposed requirements in § 170.556, shall notify the National Coordinator prior to initiating the suspension or withdrawal of a certification as specified in § 170.556 for a non-conformity pertaining to a Maintenance of Certification requirement for which the ONC–ACBs have responsibilities. We propose this revision because, as a common practice, ONC–ACBs notify ONC before suspending a certification for a certified Health IT Module when a developer fails to engage with the CAP process pertaining to a certification requirement non-conformity, and before withdrawing a certified Health IT Module when the health IT developer has not completed the actions necessary to reinstate the suspended certification. We propose to explicitly codify this practice for enforcement activities pertaining to certain Maintenance of Certification non-conformities.

To further our stated goals of increased transparency in the Program and encourage developer compliance, we also propose to add a new PoPC in § 170.523(x) ''Reporting for non-compliance with approved corrective action plans.'' We propose to require that ONC–ACBs report to ONC, pursuant to our proposal in § 170.556(d)(7)(ii), (discussed in detail in section III.D.2.c.iv below), the developer's failure to timely complete a CAP specific to a Maintenance of Certification requirement for which an ONC–ACB has specific responsibilities under § 170.523. We propose to require the ONC–ACBs to include all documentation pertaining to the identified non-conformity, including but not limited to the following information: (1) the Health IT Module and associated product(s); (2) the nature of the non-conformity(ies); (3) the corrective action plan documentation; (4) communications and records of proceedings; and (5) any additional information requested by ONC.

We believe the proposed required documentation in § 170.523(x) is necessary and valuable to support the National Coordinator's review of a health IT developer's actions or practices without requiring ONC to engage in duplicative fact-finding processes for applicable cases of non-conformities. The proposed documentation in § 170.523(x) would also inform the National Coordinator on whether the ONC–ACB met their obligations to notify the developer of the non-conformity and initiate corrective action procedures under §§ 170.523 and 170.556. Furthermore, requiring the proposed stated documentation would provide clarity and consistency for developers of health IT and ONC–ACBs on our expectations for the degree of accuracy and detail required for documenting a non-conformity with a Maintenance of Certification requirement for which an ONC–ACB has specific responsibilities under § 170.523. The documentation requirements would also help construct an accurate record that could inform whether the National Coordinator should exercise direct review under § 170.580(a).

Lastly, in § 170.523(i)(1), as part of an ONC–ACBs obligations to conduct surveillance of certified health IT in accordance with its accreditation and § 170.556, ONC requires ONC–ACBs to submit an annual surveillance plan to the National Coordinator. The ONC–ACBs submit their annual plans in September with an effective date of January 1 in the following year. As such, if we adopt the Maintenance of Certification requirements proposals in §§ 170.523 and 170.556, ONC–ACBs would need to include them as part of their annual surveillance plans for January 1, 2026.

We welcome comments on these proposals.

c. Updates to Surveillance for Maintenance of Certification Requirements

In the 2015 Edition Final Rule, we finalized that CAP requirements applied across-the-board to all types of surveillance and confirmed non-conformities (80 FR 62714). We reiterated that our goal for surveillance requirements was to ensure that health IT users, implementers, and purchasers

would be alerted to potential non-conformities in a timely and effective manner, consistent with the patient safety, program integrity, and transparency objectives described in the 2015 Edition Proposed Rule (80 FR 62716 through 62717). We received support from commenters to specify certain required elements and procedures for CAPs (80 FR 62716). We also finalized reporting requirements for CAPs and extended these requirements to all cases in which an ONC–ACB confirms a non-conformity and subsequently approves a CAP (80 FR 62717).

We continued to build upon surveillance and CAP requirements by adopting the ONC direct review regulatory framework in the EOA Final Rule (81 FR 72468 through 72471), which permits the Program to provide enhanced oversight for safety and health IT developer accountability. The EOA Final Rule emphasized the importance of protecting public health and safety while also strengthening transparency and accountability in the Program. Following the EOA Final Rule, in the ONC Cures Act Final Rule we addressed enforcement processes for new requirements established in the Cures Act. 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 expanded the focus of the Program requirements beyond the certified health IT itself (85 FR 25648 through 25649). Equally important, section 4002(a) of the Cures Act also provides (in section 3001(c)(5)(E) of the PHSA) that the Secretary may encourage compliance with the Conditions and Maintenance of Certification requirements and take action to discourage noncompliance. In the ONC Cures Act Final Rule, we, therefore, finalized an 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 finalized processes 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 also finalized in §§ 170.580 and 170.581 requirements to utilize the processes previously established for ONC direct review of certified health IT in the enforcement of the Conditions and Maintenance of Certification requirements.

We noted that 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) (85 FR 25782 through 25783). When we originally distinguished between the Conditions and Maintenance of Certification requirements that focus on actions and business practices of health IT developers versus technical interoperability of health IT, we did not further distinguish exclusively administrative functions that are required of a health IT developer to meet certain Maintenance of Certification requirements in part 170 subpart D. Rather, we determined that ONC should be responsible for addressing non-conformities pertaining to all Maintenance of Certification requirements (85 FR 25782 through 25783). We also clarified that ONC–ACBs are not responsible for enforcement of the Conditions and Maintenance of Certification requirements, and that they 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. We noted that ONC–ACBs also address non-conformities with technical and other Program requirements through surveillance and by working with health IT developers through CAPs. We stressed that, as finalized in the EOA Final Rule (81 FR 72427 through 72428) and per § 170.580(a)(3)(v), 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 (85 FR 25785).

Since publication of the ONC Cures Act Final Rule, we now have enforcement experience with Maintenance of Certification requirements in 45 CFR 170 subpart D. More specifically, ONC conducted 13 direct reviews in 2023, of which 10 were in connection to the non-conformity to the API Maintenance of Certification requirement in § 170.404(b)(3) for failure to comply with the rollout of § 170.315(g)(10); two for failure to submit their real world testing results leading to a non-conformance with § 170.406(b)(2); and, one for failure to submit their annual attestation related to § 170.406(b). We have conducted multiple direct reviews of non-conformities specific to developers of certified health IT missing a document-submission or other deadline for Maintenance of Certification requirements in 45 CFR 170 subpart D. During these direct reviews, we have coordinated with the ONC–ACBs the corrective actions and communications with the developers. Based on this enforcement experience, we have found that some non-conformities specific to certain Maintenance of Certification requirements may be better and more quickly resolved without immediate ONC involvement in certain cases and are better suited to initial oversight by the ONC–ACBs.

With this experience, we recognize that ONC–ACBs are equally well suited to conduct surveillance and work with developers of certified health IT through CAPs to remedy non-conformities beyond certification requirements in *certain circumstances.* We no longer believe that keeping enforcement for certain Maintenance of Certification requirements exclusively within ONC oversight benefits the Program and could, in fact, result in Program inefficiencies to the detriment of the Program, users of certified health IT, and developers of certified health IT. The inclusion of certain Maintenance of Certification requirements within ONC–ACB oversight would increase transparency and result in more expedient determinations of whether a non-conformity exists, along with its resolution. In our experience, the collaboration between ONC–ACBs, health IT developers of certified health IT, and users in examining potential non-conformities, along with ONC–ACB's oversight of specific Maintenance of Certification requirements, facilitates quicker resolutions leading to more efficiency in the Program. This efficiency stems from the ONC–ACBs' capacity to engage and communicate with developers promptly as well as their extensive expertise in surveilling certified Health IT Modules for continued conformity to the requirements of their certifications.

i. Reactive Surveillance

We propose to revise the reactive surveillance requirements in § 170.556(b) to account for the specified Maintenance of Certification requirements in subpart D for which an ONC–ACB would have oversight pursuant to revisions to § 170.523. We propose in § 170.556(b) to require an ONC–ACB to initiate surveillance (including, as necessary, in-the-field

surveillance required by paragraph (a) of this section) whenever it becomes aware of facts or circumstances that would cause a reasonable person in the ONC–ACB's position to question one or more of the following: (1) a certified Health IT Module's continued conformity to the requirements of its certification; (2) a developer's satisfaction of the Maintenance of Certification requirements in § 170.402(b)(1); and (3) an applicable developer's satisfaction of the Maintenance of Certification requirements for which an ONC–ACB has a responsibility under § 170.523 to confirm compliance.

We propose the surveillance requirements for the Maintenance of Certification requirements in § 170.556(b)(2) and (3) as two distinct elements because of the diverse obligations in 45 CFR part 170 subpart D that health IT developers must satisfy to remain in compliance with the Program. To ensure health IT developer accountability, and as discussed above, we have adopted the Maintenance of Certification requirements in part 170 subpart D to express ongoing requirements for health IT developers and their applicable Health IT Module(s) certified to specific certification criteria. The Maintenance of Certification requirements in 45 CFR part 170 subpart D do not always apply to all health IT developers participating in the Program. The Program is voluntary and health IT developers may certify their Health IT Module(s) to one, some, or all the certification criteria adopted by the Secretary, and they are not required to certify their Health IT Module(s) to every certification criterion to participate in the Program. Also as discussed in the previous section, we propose in § 170.523(p)(1) that ONC–ACBs confirm that health IT developers retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the Program in accordance with § 170.402(b)(1). Our proposal in § 170.523(p)(1) would require ONC–ACBs to confirm that health IT developers are meeting the requirements in § 170.402(b)(1) and, in the proposed § 170.523(i)(2)(iii), we would require the ONC–ACBs to conduct surveillance of the Maintenance of Certification requirements and include the results in its quarterly report to the National Coordinator, in accordance with its accreditation and § 170.556(a) and (e)(1). To support the PoPC proposals in § 170.523, our proposal in § 170.556(b)(2) would require an ONC–ACB to initiate surveillance (including, as necessary, in-the-field surveillance) whenever it becomes aware of facts or circumstances that would cause a reasonable person in the ONC–ACB's position to question a developer's satisfaction of the Maintenance of Certification requirements in § 170.402(b)(1). The proposed requirements in § 170.523(i)(2)(iii) and in § 170.523(p)(1), taken together with our proposal in § 170.556(b)(2), would result in the ONC–ACB initiating and conducting surveillance of a health IT developers' satisfaction of its obligations in § 170.402(b)(1).

Similar to our proposal in § 170.523(p)(1), we propose in § 170.523(p)(2) and (3), 170.523(q), (r), (s), and (w) to require the ONC–ACBs to confirm health IT developers are meeting their obligations, as applicable, under the Maintenance of Certification requirements in §§ 170.402(b)(2)–(4), 170.404(b)(1) and (2), 170.405(b)(1) and (2), 170.406(b), and 170.407(b); and in § 170.523(i)(2)(iii) to conduct surveillance of the Maintenance of Certification requirements listed in § 170.523, in accordance with their accreditation and § 170.556(b)(3). To help meet these obligations, for the proposed requirement in § 170.556(b)(3), we propose to require an ONC–ACB to initiate surveillance (including, as necessary, in-the-field surveillance) when it becomes aware of facts or circumstances that would cause a reasonable person in its position to question an applicable developer's satisfaction of the Maintenance of Certification requirements for which an ONC–ACB has a responsibility under § 170.523 (that is, §§ 170.402(b)(2)–(4), 170.404(b)(1) and (2), 170.405(b)(1) and (2), 170.406(b), and 170.407(b)).

Overall, the proposals in § 170.556(b)(2) and (3) would mean that as part of the requirement to confirm a health IT developer met its obligation(s) in part 170 subpart D, an ONC–ACB must initiate surveillance when it reasonably finds a health IT developer failed to meet the Maintenance of Certification subpart D requirements for which the ONC–ACB would have oversight of in § 170.523. We propose to distinguish between the proposed requirements in § 170.556(b)(2) and (3) because all health IT developers participating in the Program are required to comply with requirements in § 170.402(b)(1), whereas only health IT developers with Health IT Modules certified to those certification criteria listed in the requirements in §§ 170.402(b)(2)–(4), 170.404(b)(1) and (2), 170.405(b)(1) and (2), 170.406(b), and 170.407(b) are required to comply with the applicable Maintenance of Certification requirements. Given these considerations and our proposal to expand ONC–ACB oversight of specific Maintenance of Certification requirements listed in § 170.523, we propose to include requirements that ONC–ACBs must initiate surveillance of the specified Maintenance of Certification requirements in § 170.556(b)(2) and (3) reactive surveillance whenever it becomes aware of facts or circumstances that would cause a reasonable person in the ONC–ACB's position to question a developer's satisfaction of its obligations under 45 CFR part 170 subpart D.

Additionally, we propose to revise § 170.556(b)(1) by moving the current verification requirements of § 170.523(k) listed in § 170.556(b)(1) to be part of § 170.556(b)'s overall language. Our proposal would not change or modify the ONC–ACBs' current responsibilities to initiate in-the-field-surveillance requirements in § 170.556(a) or the randomized surveillance considerations in § 170.556(c).

We welcome comments on these proposals.

ii. Corrective Action Plan and Procedures

In the 2015 Edition Final Rule, we adopted requirements in § 170.556(d)(1) that require an ONC–ACB to notify a developer when it determines that a non-conformity exists and require the developer to submit a proposed CAP for the applicable certification criterion, certification criteria, or certification requirement (80 FR 62758). We propose to revise the corrective action plan and procedures in § 170.556(d)(1) to include the Maintenance of Certification requirements specified in subpart D for which we propose an ONC–ACB would have responsibilities for under § 170.523 (discussed in the section III.D.2.b above). We expect the ONC–ACB to initiate surveillance as necessary to assess whether the developer has met the Condition and Maintenance of Certification requirements obligations under subpart D of part 170—for which we propose the ONC–ACB to have oversight responsibilities—in the same manner as it initiates surveillance for other Program requirements. We propose to require that an ONC–ACB notify the developer of health IT, when an ONC–ACB determines, through surveillance under § 170.556 or otherwise, that the health IT developer is out of compliance with the specified Maintenance of Certification requirement and to require the developer submit a proposed CAP for the applicable Maintenance of Certification requirement.

In addition to the corrective action procedures adopted in the 2015 Edition Final Rule, ONC also specified certain baseline required elements for CAPs in § 170.556(d)(3) (80 FR 62758 through 62759). Specifically, we finalized in § 170.556(d)(3)(i)–(vi) six minimum required elements that an ONC–ACB must verify are included in the CAP submitted by the developer of health IT. We now propose to revise § 170.556(d)(3), which requires the ONC–ACB to verify the elements of the CAP, to account for the proposed addition of certain Maintenance of Certification requirements that we propose an ONC–ACB must include in its surveillance activities.

We do not find all existing CAP requirements equally necessary for non-conformities that involve the proposed new responsibilities for ONC–ACBs to initiate corrective procedures for specified subpart D Maintenance of Certification requirements, we also propose to specify different minimum required CAP elements based on the type of non-conformity the plan addresses. We believe that establishing certain minimum expectations and procedures for initiating CAP procedures for specified subpart D Maintenance of Certification requirements would provide ONC–ACBs, as well as health IT developers and users, with greater clarity and predictability regarding this aspect of the Program. Furthermore, ONC–ACBs have unique experience working directly with developers to remedy identified non-conformities to the requirements of certification codified in subparts A, B, C, and E, as well as verifying and confirming a developer has met its obligations with the Maintenance of Certification requirements for real world testing and attestations. This experience translates well to having ONC–ACBs conduct surveillance for certain Maintenance of Certification requirements for which we propose the ONC–ACBs have specific responsibilities. We note that our expectations regarding an ONC–ACBs' surveillance responsibilities specific to the oversight and enforcement requirements of certification would not change with the addition of certain Maintenance of Certification requirements under our revisions and additions proposed in § 170.556(b) reactive surveillance and (d) corrective action plan and procedures.

To better differentiate the requirements for each CAP, in § 170.556(d)(3)(i), we propose to list the minimum required elements for all CAPs pertaining to all non-conformities. In § 170.556(d)(3)(ii), we propose to list the minimum required elements for non-conformities with respect to any Program requirement codified in subparts A, B, C, or E of part 170. In § 170.556(d)(3)(iii), we propose to list the minimum required elements for non-conformities with respect to any Program requirement codified in subpart D of this part for which the ONC–ACBs would have responsibility under § 170.523. We discuss each proposed list of elements in detail in the following paragraphs.

We are retaining in § 170.556(d)(3) the currently required elements for identified non-conformities with respect to any Program requirements codified in subparts A, B, C, or E with proposed restructuring of the paragraph levels and minor proposed modifications. For the currently codified CAP elements, we propose to move the requirements in § 170.556(d)(3)(i), (v), and (vi) to § 170.556(d)(3)(i)(A), (B), and (C), respectively. We also propose to shift the currently codified CAP elements in § 170.556(d)(3)(ii), (iii), and (iv) to § 170.556(d)(3)(ii)(A), (B), and (C), respectively. The proposed revised elements are substantially the same elements currently codified in § 170.556(d)(3)(i)–(vi), and we do not propose revisions to the regulatory text in the newly shifted § 170.556(d)(3)(i)(A), (B), and (C) or § 170.556(d)(3)(ii)(A). For these elements, we only propose to revise the level of paragraphs.

To account for the proposed shifting of elements and the addition of the Maintenance of Certification to the ONC–ACBs' oversight responsibilities, we propose to revise paragraph (d)(3)(i) to specify that for each identified non-conformity with respect to any Program requirement, the ONC–ACB must verify that the associated CAP includes the following, at a minimum: a description of the identified non-conformities (§ 170.556(d)(3)(i)(A)); the timeframe under which corrective action will be completed (§ 170.556(d)(3)(i)(B)); and, an attestation by the developer that it has completed all elements of the approved CAP (§ 170.556(d)(3)(i)(C)). The proposed required elements would apply to proposed CAPs that aim to remedy identified non-conformities for a certified Health IT Module that does not conform to the applicable requirements of its certification and/or when the health IT developer is out of compliance with Maintenance of Certification requirements specified in subpart D of this part for which the ONC–ACB has specific responsibilities under § 170.523. We propose to require the minimum required elements in § 170.556(d)(3)(i)(A), (B), and (C) because we believe that certain elements should serve as the baseline of information for any type of non-conformity the CAP addresses.

We also believe certain minimum required elements should still apply regarding non-conformities with respect to any Program requirement codified in subparts A, B, C, or E of part 170. To account for our restructuring of the current minimum six elements in § 170.556(d)(3), in § 170.556(d)(3)(ii), we propose to shift and revise the other three remaining minimum required elements in paragraphs (d)(3)(ii), (iii), and (iv) as § 170.556(d)(3)(ii)(A), (B), and (C). For a Health IT Module that does not conform to the certification requirements codified in subparts A, B, C, or E of part 170, we propose in § 170.556(d)(3)(ii) that for each CAP submitted by the developer, the ONC–ACB shall verify the CAP includes the required elements specified in proposed § 170.556(d)(3)(ii)(A) through (C), in addition to the proposed required elements identified in § 170.556(d)(3)(i)(A), (B) and (C). We note that these proposed three minimum required elements are the same three minimum required elements that are codified in § 170.556(d)(3)(ii)–(iv), with proposed minor modifications. We propose to distinguish the elements in this way to account for the proposed elements identified in § 170.556(d)(3)(iii)(A) and (B) that we would not require for CAPs pertaining to non-compliance with the certification requirements codified in subparts A, B, C, and E of part 170.

The proposed elements listed in § 170.556(d)(3)(ii)(A) through (C) are substantially the same elements currently codified in § 170.556(d)(3)(ii) through (iv), with proposed minor modifications. For clarity, we propose to revise the proposed CAP element identified in § 170.556(d)(3)(ii)(B) (currently designated in § 170.556(d)(3)(iii)). We clarify that this required element for CAPs does not mean that on-site surveillance at a deployed site is the only means through which an ONC–ACB could identify a technical non-conformity. Thus, we propose in § 170.556(d)(3)(ii)(B) that the ONC–ACBs may identify a technical non-conformity at any location where surveillance procedures have been conducted resulting in an identified non-conformity, and for all other potentially affected customers and users.

We also propose a minor revision in § 170.556(d)(3)(ii)(C) (currently codified in § 170.556(d)(3)(iv)) to improve the readability of the required element. We note that in § 170.556(d)(3)(ii)(C), part of

the CAP required element addresses how the developer will ensure that all affected, and potentially affected customers and users are alerted to the identified non-conformities, including a detailed description of how the developer will assess the scope and impact of the problem and identify all potentially affected customers. We clarify our expectation with this requirement is two pronged. Satisfying the element would include (1) how the health IT developer identifies the potentially affected customers and (2) identifying who is the actual affected customer(s) by including a detailed description of how the health IT developer will promptly ensure that all potentially affected customers are notified of the non-conformity and plan for resolution. During the CAP process, an ONC–ACB instructs the developer to submit a proposed CAP, or a revised proposed CAP, to remedy the non-conformity. The ONC–ACB also verifies the attestation by the developer that it has completed all elements of the approved CAP (§ 170.556(d)(3)(i)(C)). We believe requiring developers to identify affected customers during the CAP approval process as part of the element in § 170.556(d)(3)(ii)(C) is helpful for several reasons, most notably that it aligns with the requirements in our enforcement mechanisms in § 170.580. It would also be useful information when we need to verify communications with a customer(s), as well as aid with Federal agency coordination by identifying the names and the number of affected customers who participate in other HHS programs. We welcome comment on our expectations and whether we should consider codifying this element as two separate requirements.

Recognizing the diversity of non-conformities, we propose, in § 170.556(d)(3)(iii), different required minimum elements for CAPs submitted for addressing non-compliance with Maintenance of Certification requirements specified in subpart D. We propose to require that an ONC–ACB verify that the proposed minimum required elements in § 170.556(d)(3)(i)(A), (B), and (C) are included in a CAP pertaining to Maintenance of Certification requirements. Additionally, to better address the variations in types of non-conformities to Program requirements, we propose in § 170.556(d)(3)(iii)(A) and (B) to implement specific required elements for each identified non-conformity with respect to any Program requirement codified in subpart D of this part for which the ONC–ACB has responsibilities under § 170.523 of this part (we refer readers to section III.D.2.b for a list of these proposed responsibilities in § 170.523). Thus, for all Maintenance of Certification requirement non-conformities, an ONC–ACB must verify that a CAP includes the proposed elements identified in § 170.556(d)(3)(iii)(A) and (B), in addition to the three minimum required elements identified in § 170.556(d)(3)(i)(A), (B), and (C).

The proposed required elements identified in § 170.556(d)(3)(iii)(A) and (B) would require ONC–ACBs to confirm how the developer will address and resolve identified non-conformities with Maintenance of Certification requirements for which the ONC–ACBs have responsibilities under proposed § 170.523. We propose to set forth different elements in § 170.556(d)(3)(iii)(A) and (B) for CAPs addressing non-conformities with certain Maintenance of Certification requirements because of the administrative nature of these requirements compared to, for example, the certification requirements of subparts A, B, C. The elements in § 170.556(d)(3)(iii)(A) and (B) enhance the process for developers to regain compliance with the Maintenance of Certification requirements in several ways. The proposal in § 170.556(d)(3)(iii)(A) would require a developer to outline the actions needed to address non-conformities related to Maintenance of Certification requirements, providing clarity in addressing the non-conformity; while the requirement in § 170.556(d)(3)(iii)(B) underscores the importance of ensuring comprehensive resolution for all identified non-conformities specific to the Maintenance of Certification requirements. These elements will aid developers in crafting CAPs tailored to the distinct challenges posed by Maintenance of Certification requirements, contributing to a clearer regulatory framework. By specifying actions related to Maintenance of Certification requirements, the elements offer explicit requirements, reduce ambiguity, and align requirements with the regulatory intent of maintaining industry-wide compliance and quality standards. This specificity supports ONC–ACBs' effective oversight, allowing them to assess the adequacy and thoroughness of CAPs and ensuring ongoing compliance with certification requirements. We welcome comments on these proposals.

iii. Additional Optional Elements

The proposed minimum CAP elements in § 170.556(d)(3)(i)—(iii) should be seen as a starting point and represent a minimum, and not a limit, on the elements that may be required by the ONC–ACBs. In other words, with the proposed changes to CAP minimum element specifications, an ONC–ACB may require that a developer include additional elements in any given CAP beyond those that would be the minimum required under § 170.556(d)(3), as proposed. This flexibility is consistent with prior surveillance requirements, and we would continue to give ONC–ACBs substantial flexibility and discretion to decide how to implement these requirements as part of their overall approach to surveillance (80 FR 16880). Such flexibility is important for minimizing the burden of surveillance on all interested parties, while ensuring that an ONC–ACB can approach surveillance in a way that effectively encourages and supports developers' successful correction of non-conformities with Program requirements. Accordingly, we also propose to revise § 170.556(d) by adding § 170.556(d)(3)(iv) to allow an ONC–ACB to require that the CAP include elements beyond those specified in proposed § 170.556(d) as the minimum.

Table 1C below includes the proposed revised elements described in this rule that an ONC–ACB would be required to verify in a CAP.

Table 1C. List of Proposed Required and Optional Elements of Corrective Action Plans

Program requirement implicated by the identified non-conformity:	The Corrective Action Plan must have the following elements included and verified by the ONC-ACB	Optional Elements
Subpart A, B, C, or E	§ 170.556(d)(3)(i)(A), (B), and (C)*; § 170.556(d)(3)(ii)(A), (B), and (C)*	§ 170.556(d)(3)(iv)
Subpart D	§ 170.556(d)(3)(i)(A), (B), and (C)*; § 170.556(d)(3)(iii)(A) and (B)**	§ 170.556(d)(3)(ii)(A), (B), and (C)*; § 170.556(d)(3)(iv)

Notes: * Elements that are currently codified in § 170.556(d)(3). We propose to move § 170.556(d)(3)(i) through (iii) to paragraphs (d)(3)(i)(A) through (C) and move § 170.556(d)(3)(iv) through (vi) to paragraphs (d)(3)(ii)(A) through (C), respectively.** Proposed § 170.556(d)(3)(iii)(A) and (B) are specific to non-compliances related to Maintenance of Certification requirements codified in subpart D.

To aid readers, we offer the following scenario to illustrate the required elements in a CAP that an ONC–ACB must verify based on the specific Program requirements implicated by each identified non-conformity. We note that this scenario is merely illustrative, and the outcomes provided in this scenario are hypothetical. The outcome of this scenario should not be construed as legal precedent for similarly situated fact patterns.

Scenario

The ONC–ACB receives signals indicating a potential non-conformity, sourced from user complaints, adverse event reports, or routine surveillance activities. Upon detecting possible certification criteria non-conformities within the certified Health IT Module of a developer, the ONC–ACB initiates surveillance to address the § 170.315(b) requirements. During this surveillance, the ONC–ACB receives information indicating the developer may have failed to submit a real world testing plan that demonstrates compliance to the full scope of the applicable certification criteria and functions requirements, including § 170.315(b). A certified Health IT Module that fails to successfully demonstrate full compliance of certification capabilities is treated as any other observation of a failure to meet specific Program requirements. As a result, the ONC–ACB also initiates a second surveillance, this time to address the § 170.405(b)(1) real world testing plan.

Once the surveillance activities substantiate non-conformity(ies), the ONC–ACB notifies the developer of its findings and requires the developer to produce a proposed CAP addressing the identified issues, such as interoperability challenges, ineffective decision support, delayed updates, and outdated documentation.

Because the ONC–ACB has identified a non-conformity pertaining to Maintenance of Certification requirements in § 170.405(b), the ONC–ACB must verify the CAP includes the proposed required elements identified in § 170.556(d)(3)(i)(A), (B), (C), and § 170.556(d)(3)(iii)(A) and (B). The CAP outlines a step-by-step approach and timeline for the developer to address the non-conformities. The ONC–ACB would require, under the proposed elements in § 170.556(d)(3), that the CAP address the non-conformity with § 170.315(b) and include the required elements in § 170.556(d)(3)(i)(A) through (C); and § 170.556(d)(3)(ii)(A) through (C) as it pertains to a non-conformity for subparts A, B, C, or E of this part. The ONC–ACB may also require the developer to include elements in the CAP beyond those specified in proposed § 170.556(d) as the minimum required elements, according to the proposed addition of § 170.556(d)(3)(iv).

With the ONC–ACBs guidance, the developer is able to provide an acceptable proposed CAP to the ONC–ACB addressing the two identified non-conformities, who verifies all the required elements to ensure effective resolution of the identified non-conformities and approves them. The CAP provides a roadmap for the developer to rectify real world testing Maintenance of Certification non-conformities, enhance interoperability, optimize decision support features, ensure timely updates, and update documentation and training materials.

The ONC–ACB continues its monitoring of the certified Health IT Module, including implementation of the CAP and progress towards resolution of the non-conformities. Follow-up assessments may be scheduled to confirm sustained compliance, aligning with the ONC–ACB's commitment to continuous improvement in the EHR system's reliability and adherence to certification criteria. The ONC–ACB ensures successful resolution of identified non-conformities and confirms that the Health IT Module now complies with all applicable certification criteria and Maintenance of Certification requirements for real world testing.

iv. Suspension, Withdrawals, and Notification Procedures

In some circumstances, despite an ONC–ACB's effort to engage and encourage the developer, a developer's non-conformity with Maintenance of Certification or other Program requirements may not be successfully addressed. Under existing regulations, ONC–ACBs shall initiate suspension procedures for a Health IT Module for the following reasons: a developer does not submit a proposed CAP in the

allotted time (§ 170.556(d)(5)(i)); a developer does not submit a revised proposed CAP within the allotted time resulting in the ONC–ACB being unable to approve a CAP (§ 170.556(d)(5)(ii)); and, if the developer does not complete the corrective actions specified in the approved CAP (§ 170.556(d)(5)(iii)). We propose to revise § 170.556(d)(5) to require that an ONC–ACB to initiate suspension procedures where a developer fails to propose a CAP, fails to propose an acceptable CAP, or fails to successfully complete an approved CAP for identified non-conformities with respect to those Maintenance of Certification requirements for which an ONC–ACB would have PoPC and surveillance responsibilities. This proposal would be a parallel complement to the existing requirement for an ONC–ACB to initiate suspension procedures for analogous failures of corrective action procedures to successfully resolve non-conformities of a Health IT Module to the requirements of its certification.

We note that under current requirements in § 170.556(d)(6), which we do not propose to substantively revise in this proposed rule, if a certified Health IT Module's certification has been suspended, then an ONC–ACB is permitted to initiate certification withdrawal procedures for the Health IT Module (consistent with its accreditation to ISO/IEC 17065 and procedures for withdrawing a certification) when the health IT developer has not completed the actions necessary to reinstate the suspended certification. Therefore, if an ONC–ACB initiates suspension procedures in accordance with proposed § 170.556(d)(5) with respect to an identified non-conformity for a Program requirement codified in subpart D for which the ONC–ACB has responsibilities under § 170.523, it may initiate certification withdrawal procedures in accordance with § 170.556(d)(6).

While the Maintenance of Certification requirements pertain to developer behaviors, we consider the specific Maintenance of Certification requirements that an ONC–ACB would have for PoPC and surveillance responsibilities to be entirely administrative in nature. The ONC–ACBs would not make a determination to suspend or withdraw certification based on developer behavior, such as non-compliance with information blocking requirements as specified in § 170.401. Instead, the ONC–ACB would carry out its obligations specified in § 170.556(d)(5) and (6) in response to a developer's failure to meet the CAP related to administrative and routine activities such as submitting a real world testing plan on time. Furthermore, ONC–ACBs and developers have experience with initiating suspensions and withdrawals for developers who fail to engage in the CAP process pertaining to certification non-conformities, and we anticipate that the ONC–ACBs could transition to applying § 170.556(d)(5) and (6) procedures to the proposed CAP procedures for Maintenance of Certification non-conformities without much additional effort. Developers too are also familiar with the process so we expect engaging in the suspension and withdrawal processes for Maintenance of Certification non-conformities would not place much additional burden on them.

We note that delegating suspensions and withdrawal responsibilities to ONC–ACBs for Maintenance of Certification non-conformities would not mean the National Coordinator does not have authority to review ONC–ACB action(s). As discussed in detail in the section III.D.2.b, we propose to revise the PoPCs to add a requirement in § 170.523(iii)(4) that ONC–ACBs must notify the National Coordinator prior to initiating a suspension or withdrawal as specified in § 170.556 for a non-conformity pertaining to a Maintenance of Certification requirement for which the ONC–ACBs have responsibilities. We also note in § 170.580(a)(3)(ii) that ONC may assert exclusive review of certified health IT as to any matters under review by ONC, and any similar matters under surveillance by an ONC–ACB.

While we believe that ONC–ACBs are well suited to conducting surveillance and coordinating with developers of certified health IT to resolve certain Maintenance of Certification requirement non-conformities, we also acknowledge that there may be instances when a developer fails to timely submit an acceptable proposed CAP or complete an approved CAP, despite an ONC–ACBs efforts to gather and verify this information. In these instances, we believe it is necessary for an ONC–ACB to notify the National Coordinator that a developer failed to submit or complete a CAP addressing these specific Maintenance of Certification non-conformities so that the National Coordinator may review the information and proceed accordingly. Therefore, we propose to add, as paragraph (d)(7) of § 170.556, new requirements for an ONC–ACB to report specific information to ONC when a developer fails to timely submit or complete an approved CAP. This proposal would apply to an identified non-conformity with respect to any Program requirement codified in subpart D for which the ONC–ACB has responsibilities under § 170.523.

Under the proposal in § 170.556(d)(7), we would require an ONC–ACB to notify the National Coordinator when the ONC–ACB's requirement to initiate suspension procedures is triggered by the developer's failure to engage (successfully or failure to engage at all, as applicable) with the CAP process for a non-conformity to a Maintenance of Certification requirement. Specifically, we propose in § 170.556(d)(7)(i) that an ONC–ACB must immediately notify the National Coordinator if one or more of the following occurs: 1) the developer has not submitted a proposed CAP; 2) the ONC–ACB cannot approve a CAP because the developer has not submitted a revised proposed CAP; or 3) the developer has not completed the corrective actions specified by an approved CAP within the time specified therein. We propose this requirement to strengthen transparency within the Program as well as encourage developer compliance with the Program. Additionally, this information would inform the National Coordinator whether the ONC–ACB met its obligations to notify the developer of the surveillance activity, if there was an identified non-conformity, and how to remediate the non-conformity, including guidance on the required elements in the CAP, as well as the developer's response and level of engagement with the CAP process.

To further accomplish our goal of increased transparency and encouraging developer compliance, we propose in § 170.556(d)(7)(ii) that an ONC–ACB must report certain information to ONC when a developer fails to submit a proposed CAP that can be approved, or complete an approved CAP with respect to any Program requirement codified in subpart D for which an ONC–ACB has responsibilities under § 170.523. We propose to add the requirement that an ONC–ACBs shall report the information specified in § 170.523(x) (discussed in section III.D.2.b above) to the National Coordinator pursuant to the requirements specified in § 170.556(d)(7)(i), and we propose to add the requirement in § 170.556(d)(7)(ii)(A) that an ONC–ACBs must notify the developer immediately when an ONC–ACB begins the notification procedures in § 170.556(d)(7)(i).

Lastly, we propose to revise 45 CFR 170.556 to correct regulatory text errors. First, we propose to revise § 170.556(d)(6) by removing the ''or''

within the description of ''Withdrawal'' because this was a typographical error. We also propose to revise § 170.556(e)(3) by removing the reference to § 170.523(f)(2)(xi). In the ONC Cures Act Final Rule, § 170.523(f)(2) was removed and reserved. Therefore, we propose to remove this reference from § 170.556(e)(3) to correct this technical error.

We welcome comment on these proposals.

3. Updates to Principles of Proper Conduct for API Discovery Details

In the ONC HTI–1 Final Rule, we finalized requirements in § 170.404(b)(2) for Certified API Developers to publish certain service base URLs and related organization details in a standardized FHIR® format (89 FR 1287). This included a requirement, in § 170.404(b)(2)(iii)(B), that Certified API Developers review this information quarterly and update it as necessary.

We propose a conforming policy, applicable to ONC–ACBs beginning January 1, 2027, to support the regular reporting of API discovery details including service base URLs and related organization details according to our proposed requirements in § 170.404(b)(2) and (3) (see elsewhere in this preamble at III.B.2, III.B.3, III.B.15, and III.B.20.d our proposals for revising § 170.404(b)(2)). Specifically, we propose to add a new paragraph in § 170.523(m)(6) to require ONC–ACBs to obtain a record of all updates to API discovery details for § 170.404(b)(2) and (3) on a quarterly basis each calendar year. This would ensure that ONC is aware of the latest API Discovery Details published on a quarterly basis by Certified API Developers meeting the requirements in § 170.404(b)(2) and (3) and would support ONC in hosting a link to developers' API discovery details on the Certified Health IT Product List (CHPL) or another website hosted by ONC. Our proposed requirement for § 170.523(m)(6) is consistent with similar existing requirements for adaptations and updates in § 170.523(m), which require ONC–ACBs to obtain records on a quarterly basis. Further, this same requirement is already in place for a related certification criterion, § 170.315(d)(13), which requires health IT developers to publish information and has a corresponding requirement for ONC–ACBs to obtain a record on a quarterly basis in § 170.523(m)(3).

4. New ONC–ACB Principle of Proper Conduct for Notice of Program Withdrawal

To date, we have handled the infrequent occurrence of an ONC–ACB withdrawing from the Program by working collaboratively with that departing ONC–ACB and the other remaining ONC–ACBs to enable an orderly transition of certifications administered by the departing ONC–ACBs. However, as the Program has matured and the scope of an ONC–ACB's responsibilities has increased (including proposals in this proposed rule), a requirement for an ONC–ACB to provide notice to the National Coordinator when it intends to withdraw from the Program would further support an orderly transition. Accordingly, we propose in § 170.523(y) a new Principle of Proper Conduct for ONC–ACBs requiring an ONC–ACB to give the National Coordinator sufficient notice of its intent to withdraw its authorization under the Program. We believe that notice provided 180 days (day is defined in § 170.102 as a calendar day or calendar days) prior to the ONC–ACB's withdraw from the Program would be sufficient time for ONC to work with the ONC–ACB to ensure the ONC–ACB's planned withdrawal does not interrupt Program operations and activities, put its clients at risk of losing their certification(s) under the Program, and/or impact end users' ability to meet their business needs and requirements for participation in other Federal and/or state programs that require the use of certified health IT.

When an ONC–ACB withdraws its authorization from the Program, ONC must work with that ONC–ACB to ensure the ONC–ACB's clients are able to transition to another ONC–ACB and maintain their certified status. For an ONC–ACB to onboard a new client and issue a new certificate based on the evidence supporting a certificate previously issued by another ONC–ACB, it must possess the evidence that supports the prior ONC–ACB's decision. The transition requires the transfer of test records and other documented evidence supporting the certification. Consistent with § 170.523(g)(1), ONC–ACBs are required to retain all records related to the certificates they issue, and per § 170.523(g)(2) make such records available to HHS upon request during the specified retention period. Therefore, to maintain the integrity of the certifications impacted by the ONC–ACB withdrawal, ONC will request records (per § 170.523(g)(2)) from the withdrawing ONC–ACB. These records will provide evidence of conformity with certification requirements to support the remaining ONC–ACBs that take on the withdrawing ONC–ACB's clients. These steps are important because, once an ONC–ACB withdraws from the Program, ONC no longer has authority over the actions of that organization. Furthermore, the influx of incoming business for the ONC–ACBs accepting requests from the withdrawing ONC–ACB's clients must be managed along with their existing workload.

Specifically, we propose to add two paragraphs in § 170.523(y). In § 170.523(y)(1), we propose to require the withdrawing ONC–ACB to provide ONC with notice of its intent to withdraw from the Program 180 days before its actual withdrawal. In § 170.523(y)(2), we propose to require the withdrawing ONC–ACB to submit all of its certification records to ONC pursuant to the retention requirements it followed in § 170.523(g). We believe the combination of these two proposals will give all parties involved (*i.e.,* ONC, the withdrawing ONC–ACB, and remaining ONC–ACBs) sufficient time to manage transition activities with minimal interruption to Program activities.

5. Updates to ONC Direct Review Procedures

In the EOA Final Rule, we created a regulatory framework for ONC's ''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 such health IT (81 FR 72404). The EOA Final Rule established bases on which ONC would initiate direct review, and procedures for ONC to follow in the event ONC's direct review of certified health IT substantiated a non-conformity. Under the framework established in the EOA Final Rule, inquiry into certified health IT's conformance with Program requirements may be conducted by ONC or a third party on ONC's behalf, and the term ''direct review'' is used to distinguish inquiries and enforcement actions taken under the 45 CFR 170.580 framework from ONC–ACBs' assessments and reviews as part of the ONC–ACB's surveillance and other responsibilities under the Program (85 FR 25738).

In the ONC Cures Act Final Rule (85 FR 25642), we finalized use of substantially the same processes established in the EOA Final Rule (81 FR 72404) for the enforcement of the

Conditions and Maintenance of Certification requirements for four stated reasons (85 FR 25783). 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 were already familiar with the ONC direct review framework that had been put in place by the EOA Final Rule. Third, 45 CFR 170.580 provides thorough and transparent processes for identifying, notifying, and addressing non-conformities in the Program through coordination with health IT developers to craft a CAP that will remedy Program non-conformities. Fourth, the updated direct review framework provides equitable opportunities for health IT developers to respond to ONC actions and appeal certain ONC determinations. We confirmed in the ONC Cures Act Final Rule that we would continue to use the term ''direct review'' to describe activities of ONC (or a third party on ONC's behalf) under the 45 CFR 170.580 framework and to differentiate them from ONC–ACBs' reviews of certified health IT under their surveillance responsibilities outlined in 45 CFR 170.556 (85 FR 25783).

In this proposed rule, we propose to revise parts of the ONC direct review regulatory framework in 45 CFR 170.580, including:

- 45 CFR 170.580(b) and (c) requirements for timeliness and content of health IT developers' CAPs in response to a notice that ONC has confirmed a non-conformity with Program requirements (discussed below in section III.D.3.a);
- 45 CFR 170.580(d) and (f) provisions for suspension and termination of certification for failure of certified health IT products or a Program-participating health IT developer to meet Program requirements (discussed below in section III.D.5.b); and
- 45 CFR 170.580(g) opportunity and procedures for heath IT developer appeals of ONC enforcement actions under § 170.580(d) or (f) and § 170.581 (discussed below in section III.D.5.b of this proposed rule).

a. Health IT Developers' Response to Notices of Non-conformity and Corrective Action Plan Requirements

We propose to revise regulatory provisions specific to the timing and content of health IT developers' responses to notices of non-conformity, as well as the mandatory minimum content of developers' CAPs, to improve efficiency for both ONC and developers under direct review.

We propose to revise paragraph § 170.580(b)(2)(ii)(A)(*3*) to require that, where multiple responses are provided pursuant to this paragraph, information provided in earlier responses be labeled as previously submitted. The intent of this proposed revision is to increase efficiency for ONC by making it clear that repeated submission of the same information in response to the same Notice of Non-Conformity should generally be avoided.

We propose to leave in place the flexibility that health IT developers currently have to re-submit the same information in multiple communications in response to any particular Notice of Non-Conformity. Because the information that a developer may need to provide in response to a Notice of Non-Conformity can include detailed technical or business practices data, we propose to balance this developer flexibility with a requirement that if a developer does elect to resubmit the same data or information, that it must label such data or information as having been previously submitted in response to the same Notice of Non-Conformity. The labeling of any resubmitted materials would promote efficiency by enabling ONC reviewers to immediately focus on updates, addenda, or refreshed discussion of the resubmitted data.

As discussed in section III.D.2.c above, we now have some experience evaluating non-conformities associated with developers failing to comply with administrative Maintenance of Certification requirements in 45 CFR 170 subpart D. We have learned from this experience that some of the mandatory minimum elements that § 170.580(c)(2) currently requires for all CAPs are not equally valuable with respect to all non-conformities. For example, an assessment and description of the nature, severity, and extent of the non-conformity (the element specified in § 170.580(c)(2)(i)) would likely be necessary where the ONC-substantiated non-conformity is that a certified Health IT Module is causing or contributing to a serious risk to public health or safety. The § 170.580(c)(2)(i) element would also likely be necessary in cases where a certified Health IT Module is found to be non-conforming by virtue of failing to satisfy the requirements of all 45 CFR 170 subpart C certification criteria to which it is certified. By contrast, the § 170.580(c)(2)(i) element is not likely to be necessary in many instances where the non-conformity is a failure to meet an administrative requirement under subpart D, such as to timely submit real world testing documentation pursuant to § 170.405(b), or to submit required attestations pursuant to § 170.406. Timely submission of attestations is a pass/fail, readily observed non-conformity for which inclusion of the § 170.580(c)(2)(i) element would not provide helpful or additional information. Similarly, where the resolution of the non-conformity amounts to submitting the overdue attestations or real world testing documentation, the successful resolution is self-documenting, so a detailed description of supporting documentation a developer would provide *to demonstrate* the identified non-conformity is resolved (as specified in § 170.580(c)(2)(vi), emphasis added) generally would not be necessary or add value to the direct review process.

We propose to revise paragraph (c)(2) of § 170.580 to establish flexibility for ONC to identify, for any particular non-conformity, the subset of the elements listed in subparagraphs (i) through (viii) relevant to demonstrating the resolution to each non-conformity. We propose the National Coordinator may explicitly waive any of the subset of elements listed in subparagraphs (i) through (viii). ONC would continue to provide direction to the health IT developer as to the required elements of the CAP for each identified non-conformity.

b. Suspension, Termination, and Appeals

We propose modifications to our suspension, termination, and appeals regulations for several reasons. Some proposed revisions would simply ensure clarity as to who makes, and where ultimate accountability lies with respect to, certain decisions. Other proposed revisions would update procedures to reflect other Program changes proposed elsewhere in this rule or update regulatory text to remove now-obsolete terminology.

Suspension, Termination, and Appeals Decisions

We propose to clarify in our regulatory text that our procedures for decisions to terminate the certification of Health IT Modules or issue certification bans under § 170.581 are made by the National Coordinator, whom the Secretary appoints to head ONC pursuant to 42. U.S.C. 300jj–11. We also propose to revise § 170.580 and § 170.581 to explicitly provide for the Secretary to have an opportunity to exercise direct oversight of these

determinations as well as for hearing officer determinations under 45 CFR 170.580(g). Specifically, we propose to revise paragraphs (d), (f), and (g) of § 170.580 (and to revise § 170.581, as discussed in section III.D below).

We propose to modify § 170.580(d) and § 170.580(f) to reflect that the National Coordinator makes determinations to suspend or terminate a certification, and to cancel a suspension or to rescind a termination determination. But, to ensure that it is clear, notwithstanding the decision of the National Coordinator, that the Secretary, a principal officer of the United States, retains ultimate responsibility for such decision-making, we propose that the Secretary may, at the Secretary's discretion, review a determination of the National Coordinator. The Secretary may direct the National Coordinator to cancel a suspension (paragraph (d)(6)(ii)) or review a termination determination made by the National Coordinator before such suspension or the termination would become effective (paragraph (f)(5)). We propose in § 170.580(f)(5) that, should the Secretary direct the National Coordinator to rescind a termination, ONC may resume (§ 170.580(f)(5)(i)) or end (§ 170.580(f)(5)(ii)) all or part of its review of certified health IT or a health IT developer's actions or practices under this section unless the Secretary specifically directs otherwise.

Updates to Align with Other Proposals in This Proposed Rule

We propose to modify paragraph (f) of § 170.580 to align with proposed added responsibilities of ONC–ACBs for confirming and encouraging compliance with certain Maintenance of Certification requirements codified in subpart D of 45 CFR part 170 (discussed in section III.D.2 of this proposed rule, above). Specifically, we propose in § 170.580(f)(1)(iv) to provide for the National Coordinator to terminate a certification based on ONC review of the information and documentation reported by the ONC–ACB pursuant to the principles of proper conduct (PoPC) proposed in paragraph (x) of § 170.523 (discussed in section III.D.2.b) that the developer did not fulfill its obligation under a CAP. This would explicitly establish that the National Coordinator may make a termination determination without ONC being required to engage in duplicative fact-finding in applicable non-conformity cases. Applicable cases would be those where the information and documentation provided in the ONC–ACB's § 170.523(x) report is, in the National Coordinator's view, sufficient to substantiate that a developer has failed to resolve a Program non-conformity related to a Maintenance of Certification requirement within the required timeframe of the CAP verified and approved by the ONC–ACB. The National Coordinator's consideration of the record submitted by the ONC–ACB pursuant to § 170.523(x) would include assessing whether the ONC–ACB had met its obligations to notify the developer of the non-conformity and initiate corrective action procedures under §§ 170.523 and 170.556.

We also propose revisions to § 170.580(a)(3)(iii), (a)(3)(v), and (a)(4)(ii) to clarify that the: (1) National Coordinator's determination on matters under ONC direct review is controlling and supersedes any determination by an ONC–ACB; (2) National Coordinator may end all or any part of ONC's review of certified health IT or a health IT developer's actions at any time; and (3) National Coordinator may rely on HHS Office of Inspector General (OIG) findings to form the basis of a direct review action. We also propose revisions to § 170.580(b)(2)(ii)(B) and § 170.580(b)(2)(iii) clarifying that the National Coordinator may adjust the 30-day timeline under § 170.580(b)(2)(ii)(A)(*3*) and that the National Coordinator makes a determination under § 170.580(b)(2)(iii) after receiving the health IT developer's written explanation and supporting documentation. We propose to revise § 170.580(c)(1) clarifying that if the National Coordinator determines that certified health IT or a health IT developer's action or practice does not conform to requirements of the Program, ONC will notify the health IT developer of its determination and require the health IT developer to submit a proposed CAP. In § 170.580(c)(2), we propose that the CAP shall include such required elements that the National Coordinator determines necessary. The CAP shall include, for each specific non-conformity, all the elements in § 170.580(c)(2) except when the elements are explicitly waived by the National Coordinator. We also propose to update § 170.580(c)(7) to provide that a CAP may be reinstituted by ONC if the National Coordinator later determines that a health IT developer has not yet fulfilled all its obligations under the CAP.

We also propose revisions to § 170.580(e)(1), (e)(1)(vii), (e)(2), and (e)(4) clarifying the actions that the National Coordinator can take with a proposed termination and updating the existing language to clarify that certain decisions are made by the National Coordinator, with ultimate accountability for the National Coordinator's decisions vested in the Secretary as discussed above. More specifically, we propose that: (1) excluding situations of noncompliance with a Condition or Maintenance of Certification requirement under subpart D of this part, the National Coordinator may propose to terminate a certification issued to a Health IT Module when a health IT developer fails to respond timely to a communication from ONC, fails to provide sufficient access or information to ONC, or the National Coordinator concludes that a certified health IT's non-conformity(ies) cannot be cured (§ 170.580(e)(1) and (e)(1)(vii)); (2) ONC will notify the health IT developer of the proposed termination through a notice of proposed termination when the National Coordinator decides to propose to terminate a certification (§ 170.580(e)(2)); and, (3) upon receipt of the health IT 'developer's written response to a notice of proposed termination, the National Coordinator has up to 30 days to make a determination based on ONC's review of the information submitted by the health IT developer and the National Coordinator may extend this timeframe if the complexity of the case requires additional time for ONC review (§ 170.580(4)).

c. Appeals

The ONC direct review regulatory framework established in the EOA Final Rule (81 FR 72404) included (in § 170.580(g)) procedural provisions for developers to appeal certification termination determinations made by the National Coordinator under § 170.580(f) as well as Program bans issued under § 170.581. In the ONC Cures Act Final Rule, we established that we would use the processes previously put in place for ONC direct review of certified health IT in the enforcement of the Conditions and Maintenance of Certification requirements. In doing so, we finalized modifications to § 170.580(g) provisions to address the inclusion of Condition and Maintenance of Certification requirements under § 170.580(f) and § 170.581 (85 FR 25649 and 25787).

We propose to rename § 170.580(g)(5) to ''Assignment of a hearing officer'' and clarify the text to explain that the National Coordinator will arrange for assignment of the case to a hearing officer to adjudicate the appeal on the National Coordinator's behalf, and add subparagraph (iii) that the hearing officer must be an officer properly appointed by the Secretary of Health and Human Services.

We propose to explicitly provide in § 170.580(g)(7)(ii) for the Secretary, at the Secretary's discretion, to review and revise or rescind hearing officer decisions before these decisions become the final decision of HHS. This proposed change would ensure the regulatory text is explicit that the Secretary, as a principal officer of the United States, holds appropriate oversight and accountability for the hearing officer's decisions.

We welcome comments on these proposals.

6. Certification Ban

We propose to update paragraphs (a) and (b) of the certification ban provisions in § 170.581 to explicitly provide for the Secretary to review, at the Secretary's discretion, the National Coordinator's determination to impose a ban before the ban becomes effective. We further propose updates to § 170.581(a)(2) and (d)(4) to indicate that the National Coordinator as a duly appointed officer of the United States, rather than ONC as an organization, would make any determination to impose a certification ban on a developer. These proposed revisions are similar to those we discussed above for suspension and termination.

We propose to update the wording of § 170.581(a)(1)(i) to replace a reference to termination of a Health IT Module ''under the ONC Health IT Certification Program'' to cross-reference the paragraph within § 170.580 specific to termination of a certification in the context of ONC direct review. We believe the specific cross-reference would make it easier for developers, ONC–ACBs, and other interested parties to read and understand § 170.581(a)(1)(i).

In parallel to our proposed addition of PoPCs and surveillance responsibilities for ONC–ACBs specific to certain Maintenance of Certification requirements in subpart D of 45 CFR part 170 (both in § 170.523), we propose to explicitly establish in § 170.581(a)(2) that the National Coordinator would have the option of determining a certification ban is appropriate based on the information and documentation provided in an ONC–ACB's § 170.523(x) report. We believe this is important to ensure that the National Coordinator can take prompt action, without duplicative data gathering or fact finding, where the information and record submitted by the ONC–ACB indicates to the National Coordinator that a program ban is appropriate.

We welcome comment on these proposals.

7. Updates Pursuant to 2014 Edition Removal

We propose to remove the ''Complete EHR'' and ''EHR Module'' terms from certain sections within subpart E of 45 CFR 170. By the time we would finalize any proposal in this proposed rule, the terms would no longer be relevant, as described below, due to the amount of time that will have elapsed since the June 30, 2020, effective date of the ONC Cures Act Final Rule's removal of the 2014 Edition from subparts A, B, and C of part 170. We believe removing obsolete terms as the Program evolves over time maintains clarity of the regulatory text and Program provisions, particularly for regulated entities and interested parties.

a. Removal of ''Complete EHR'' References

The ONC Cures Act Final Rule removed the 2014 Edition certification criteria in § 170.314 from the Program regulations in 45 CFR part 170 (85 FR 25656). The rule also finalized our proposals (84 FR 7434 through 7435) to remove 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. In conjunction with the removal of the 2014 Edition, we also removed references to ''Complete EHR'' from § 170.545 and removed the standards and implementation specifications found in §§ 170.200, 170.202, 170.204, 170.205, 170.207, 170.210, and 170.299 that were referenced only in the 2014 Edition certification criteria (85 FR 25656). In the HTI–1 Final Rule, we removed the ''Complete EHR'' language from all reference points in §§ 170.523 and 170.524 (89 FR 1209 through 1210).

Although we removed terms, standards, and certification criteria that were applicable only to the 2014 Edition in the ONC Cures Act Final Rule, we have retained until now reference to ''Complete EHRs'' in certain provisions within subpart E of 45 CFR part 170:

- The definition of ''gap certification'' (§ 170.502);
- Authorization scope for ONC–ATL status (§ 170.511);
- Requirements for ONC–ACBs to refund fees to developers seeking certification under certain circumstances (§ 170.523(j)(3)); and
- Applicability of a newer version of a minimum standard (§ 170.555(b)(2)).

Retaining reference to ''Complete EHRs'' in these part 170 subpart E requirements has supported continuity following the removal of the 2014 Edition's standards and certification criteria from 45 CFR part 170. For example, in the update of ONC–ACB record retention requirements in §§ 170.523 and 170.524 to align with the transition of the Program's structure and terminology away from annual themed ''editions,'' the ''Complete EHR'' concept remained relevant to these provisions at that time because the 2014 Edition was not removed from the CFR until the ONC Cures Act Final Rule (85 FR 25655). The ONC Cures Act Final Rule became effective on June 30, 2020, and records for the 2014 Edition were required to be retained (including Complete EHRs) until June 30, 2023, under 45 CFR 170.523(g)(1).

Beginning with the 2015 Edition, Complete EHR certifications could no longer be issued and December 31, 2023, has passed. Thus, we now propose to remove references to ''Complete EHRs'' from §§ 170.502,170.511, 170.523(j)(3), and 170.555(b)(2) as of the effective date of a subsequent final rule for this rulemaking.

b. Removal of ''EHR Modules'' References

In the 2011 ''Establishment of the Permanent Certification Program for Health Information Technology'' Final Rule (76 FR 1261), we used the Complete EHR and EHR Module terms and phrasing ''Complete EHRs and/or EHR Modules.'' In the rule, we stated our initial focus would be on EHR technology and supporting the EHR Incentive Programs, which at the time, focused on the ambulatory and inpatient settings (76 FR 1294).

As we explained in the 2015 Edition Final Rule (80 FR 62601), we changed the name of the ONC HIT Certification Program to the ''ONC Health IT Certification Program'' (Program). We also modified the Program in ways that 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 (80 FR 62604). These modifications also served to support other public and private programs that may reference the use of health IT certified under the Program (80 FR 62604).

Consistent with the three-year records retention requirement for ONC–ACBs (45 CFR 170.523(g)(1), June 30, 2023, marked the end of a three-year minimum retention period (36 calendar months) since we finalized, in the ONC Cures Act Final Rule, the removal of the 2014 Edition from 45 CFR subparts A,

B, and C (85 FR 25656). Similarly, December 31, 2023, marked the end of the third calendar year following the calendar year in which the ONC Cures Act Final Rule became effective. Because we have now passed both rules' three-year retention requirements for ONC–ACBs and the term ''EHR Module'' is no longer relevant, we propose to remove from § 170.523(f) reference to ''EHR Modules.''

8. Definition of Serious Risk to Public Health or Safety

We propose to revise 45 CFR 170.102 to include a definition of *serious risk to public health or safety.* The purpose of this proposed definition is to enhance understanding among developers and users of certified health IT of the types of conditions, events, or phenomena that would constitute egregiously dangerous non-conformities with Program requirements. Such events could be caused or contributed to by health IT certified as a Health IT Module or as part of a certified Health IT Module even if the certified Health IT Module(s) continued to pass lab testing procedures, in-the-field surveillance testing, or both with respect to the technical standards and certification criteria adopted in subparts B and C of part 170. Within the proposed regulation text for this proposed definition of serious risk to public health or safety, we have included fact patterns in (1) through (6) that would always meet the definition of *serious risk to public health or safety.* For purposes of these examples, a ''user'' of a certified Health IT Module would be any human being or any software application, process, or service that is authorized, intended, and enabled to create, read, update, or delete (CRUD) or to command the certified Health IT Module to execute specific CRUD functions on specific data entries. We request public comment on this definition, including but not limited to the illustrative examples.

We would continue to expect, as we reiterated in the EOA Final Rule, that ONC direct review on the bases of risk to public safety or where ONC–ACBs may be unable to respond effectively would occur relatively infrequently (*cf., e.g.,* 81 FR 72404 at 72415 or 74216). As we explained in the EOA Final Rule, we do not believe every risk to public health or safety necessitates ONC's direct review. We also recognize the need to prioritize ONC's limited resources by focusing on the kinds of problems and other issues that, if not addressed through ONC's direct review, are most likely to lead to harm to patients or the public and undermine confidence in health IT and the integrity of the Program (81 FR 72419). This proposed definition would not change this need to prioritize ONC's resources.

9. Removal of Time-Limited Criteria

In the ONC Cures Act Final Rule, we finalized § 170.550(m) ''time-limited certification and certification status for certain 2015 Edition certification criteria'' which provided that for five specific certification criteria, an ONC–ACB may only issue a certification to a Health IT Module and permit continued certified status for a specified time period (85 FR 25952). The five criteria with time-limited certification and certification status are found in § 170.315(a)(10), (a)(13), (b)(6), (e)(2), and (g)(8). Because the specified time periods for certification to these criteria have elapsed, we propose to remove all of the certification criteria referenced in § 170.550(m) in one action by removing and reserving § 170.550(m) in its entirety. We also propose to remove and reserve these aforementioned certification criteria from the specific CFR locations in which they are adopted. In the ONC Cures Act Final Rule, we also finalized revisions in § 170.315(b)(7)(ii) and (b)(8)(i)(B) to allow security tagging of Consolidated-Clinical Document Architecture (C–CDA) documents at the document level only for the period until 24 months after publication date of the final rule (85 FR 25667). Because that time period has elapsed, we propose to revise § 170.315(b)(7) and (8) to remove § 170.315(b)(7)(ii) and (b)(8)(i)(B). We describe our detailed proposals below.

The requirements finalized in the ONC Cures Act Final Rule in § 170.550(m)(1) permit ONC–ACBs to issue certificates for the ''drug-formulary and preferred drug list checks'' certification criterion in § 170.315(a)(10) up until January 1, 2022 (85 FR 25661). We stated in the ONC Cures Act Final Rule that we believed the functionality in § 170.315(a)(10) was ubiquitous due to widespread adoption of health IT certified to the 2014 Edition and that we did not believe it was necessary to continue to require certification to it under the Program in order to ensure it remains widely available (85 FR 25661). We also stated that because the certification criterion did not require use of standards or directly drive interoperability, we did not believe its continued inclusion in the Program would provide sufficient value to providers or patients to justify the burden on developers and providers (85 FR 25661). We propose to remove and reserve § 170.315(a)(10).

In the ONC Cures Act Final Rule, we finalized requirements in § 170.550(m)(1) permitting ONC–ACBs to issue certificates for the ''patient-specific education resources'' certification criterion in § 170.315(a)(13) up until January 1, 2022 (85 FR 25661). We stated that we believed that health IT's capabilities to identify appropriate patient education materials was widespread among health IT developers and their customers, and noted innovation had occurred for these capabilities, including the use of automation and algorithms to provide appropriate education materials to patients in a timely manner (85 FR 25661). We also stated that we believed this certification criterion was no longer the best way to encourage innovation and advancement in the capabilities of health IT to support clinician-patient interactions and relationships (85 FR 25661). We propose to remove and reserve § 170.315(a)(13).

The requirements finalized in the ONC Cures Act Final Rule in § 170.550(m)(1) permitted ONC–ACBs to issue certificates for the ''secure messaging'' certification criterion in § 170.315(e)(2) up until January 1, 2022 (85 FR 25662). In the ONC Cures Act Final Rule, while we did not finalize removal of the requirements in § 170.315(e)(2), we stated that we no longer believed that a separate certification criterion focused on a health IT's capabilities to send and receive secure messages between health care providers and patients was necessary and that the certification criterion would also no longer be associated with an objective or measure under the CMS PI Programs (85 FR 25662). We propose to remove and reserve § 170.315(e)(2).

In the ONC Cures Act Final Rule, we finalized requirements in § 170.550(m)(2) permitting ONC–ACBs to issue certificates for the ''data export'' certification criterion in § 170.315(b)(6) up until May 1, 2023 (85 FR 25662). This date was later extended to December 31, 2023, in the Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency Interim Final Rule (85 FR 70070). We noted in the ONC Cures Act Final Rule that § 170.315(b)(6) was replaced by the ''EHI export'' certification criterion in § 170.315(b)(10) and removed from the 2015 Edition Base EHR definition in § 170.102, and that this would encourage movement toward the interoperability opportunities afforded by new criteria

(85 FR 25699). We propose to remove and reserve § 170.315(b)(6).

The requirements finalized in the ONC Cures Act Final Rule in § 170.550(m)(2) permit ONC–ACBs to issue certificates for the certification criterion in § 170.315(g)(8) ''application access—data category request'' up until May 2, 2022 (85 FR 25666). This date was later extended to December 31, 2022, in the Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency Interim Final Rule (85 FR 70070). We noted in the ONC Cures Act Final Rule that we had adopted a new API certification criterion in § 170.315(g)(10) to replace the certification criterion in § 170.315(g)(8) and added the new certification criterion to the updated 2015 Edition Base EHR definition (85 FR 25645). We propose to remove and reserve § 170.315(g)(8).

In the ONC Cures Act Final Rule, we finalized revisions in § 170.315(b)(7)(ii) and (b)(8)(i)(B) to allow certification of health IT to demonstrate security tagging of Consolidated-Clinical Document Architecture (C–CDA) documents at the document level only for the period until 24 months after publication date of the final rule (85 FR 25707). This date was later extended to December 31, 2022, in the Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency Interim Final Rule (85 FR 70070). We noted in the ONC Cures Act Final Rule that only requiring 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 (85 FR 25645). We now propose to revise § 170.315(b)(7) and (b)(8) to remove § 170.315(b)(7)(ii) and (b)(8)(i)(B).

10. Privacy and Security Framework Incorporation of DSI Criterion

In the ONC HTI–1 Final Rule, we established a revised certification criterion (''decision support interventions'' (§ 170.315(b)(11)) to replace the ''clinical decision support'' certification criterion (§ 170.315(a)(9)) effective January 1, 2025 (89 FR 1196 through 1197). When finalizing the ''decision support interventions'' certification criterion, we did so by adopting a substantially similar structure to the structure of the ''clinical decision support'' certification criterion. However, we neither proposed nor finalized corresponding privacy and security certification requirements for Health IT Modules certifying to the ''decision support interventions'' certification criterion. This omission was an oversight. We now propose to add the ''decision support interventions'' certification criterion (§ 170.315(b)(11)) to the list of certification criteria in § 170.550(h)(3)(ii). This proposal would ensure that the same privacy and security certification requirements that apply to the ''clinical decision support'' certification criterion (§ 170.315(a)(9)) also apply to Health IT Modules certified to the ''decision support interventions'' certification criterion.

To provide developers of certified health IT time to comply with these proposed requirements, we specifically propose to require, in § 170.550(h)(3)(ii), that Health IT Modules certified to the ''decision support interventions'' (§ 170.315(b)(11)) must also be certified to the specific privacy and security certification criteria on and after January 1, 2028. These specific privacy and security certification criteria are: ''authentication, access control, and authorization'' in § 170.315(d)(1); ''auditable events and tamper-resistance'' in § 170.315(d)(2); ''audit report(s)'' in § 170.315(d)(3); ''automatic access time-out'' in § 170.315(d)(5); ''end-user device encryption'' in § 170.315(d)(7); ''encrypt authentication credentials'' in § 170.315(d)(12); and ''multi-factor authentication'' in § 170.315(d)(13).

We note that should we finalize our proposed revisions to ''encrypt authentication credentials'' in § 170.315(d)(12) (as discussed in section III.B.12) and finalize our proposal to revise § 170.550(h)(3)(ii) as described above, those revised requirements would apply to Health IT Modules certified to the ''decision support interventions'' certification criterion (§ 170.315(b)(11)). However, we further note that should we finalize our proposed revisions to the ''multi-factor authentication'' certification criterion in § 170.315(d)(13) as described in section III.B.17, and should we finalize our proposal to revise § 170.550(h)(3)(ii) as described above, Health IT Modules certified to the ''decision support interventions'' certification criterion would not be required to support the new multi-factor authentication requirements, due to the timing included in our proposed updates in § 170.550(h)(3)(ii), unless those Health IT Modules are also certified to § 170.315(b)(3), § 170.315(e)(1), § 170.315(g)(10), or § 170.315(g)(30) and required to meet the multi-factor authentication requirements in those certification criteria in § 170.315(b)(3)(ii)(G), § 170.315(e)(1)(iii), § 170.315(g)(10)(ii)(A)(1)(iii), or § 170.315(g)(30)(ii)(c) respectively.

E. Correction—Privacy and Security Certification Framework

We propose to make a correction to the Privacy and Security Certification Framework in § 170.550(h). We revised § 170.550(h) in the ONC Cures Act Final Rule but intended for § 170.550(h)(4) to remain unchanged. However, when we drafted the amendatory instructions, we erroneously included the instruction to revise all of paragraph (h) (85 FR 25952). Therefore, when the Code of Federal Regulations (CFR) was updated, § 170.550(h)(4) was removed. We now propose to add back to the CFR 170.550(h)(4) [45 CFR 170.550(h)(4) (Jan. 1, 2020)] as it existed prior to the ONC Cures Act Final Rule. The language in § 170.550(h) to be added to paragraph (4) is, ''*Methods to demonstrate compliance with each privacy and security criterion.* One of the following methods must be used to meet each applicable privacy and security certification criterion listed in paragraph (h)(3) of this section: (i) Directly, by demonstrating a technical capability to satisfy the applicable certification criterion or certification criteria; or (ii) Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

IV. Information Blocking Enhancements

A. Defined Terms

1. Health Care Provider

Health care provider, as defined in 45 CFR 171.102 for purposes of the information blocking regulations, has the same meaning as 'health care provider' in 42 U.S.C. 300jj. As finalized in the ONC Cures Act Final Rule (85 FR 25642), this definition cites to the entirety of 42 U.S.C. 300jj (section 3000 of the Public Health Service Act (PHSA)). We now propose to provide additional regulatory clarity for the ''health care provider'' definition and for certain types of health care providers referenced by the ''health care provider'' definition. We propose to revise § 171.102 to explicitly reference the ''health care provider'' definition in 42 U.S.C. 300jj(3) and the definitions of

''laboratory'' in 42 U.S.C. 300jj(10) and ''pharmacist'' in 42 U.S.C. 300jj(12).

In the ONC Cures Act Final Rule (85 FR 25794), we adopted a definition of ''health care provider'' citing 42 U.S.C. 300jj, indicating we had noted in the ONC Cures Act Proposed Rule (84 FR 7510) that the PHSA section 3000(3) definition is different from the definition of ''health care provider'' in 45 CFR 160.103 for purposes of the HIPAA Privacy and Security Rules. We now propose to revise the definition of ''health care provider'' in § 171.102 to explicitly cite 42 U.S.C. 300jj(3).

In addition, we propose to explicitly incorporate the PHSA section 3000 definitions of ''laboratory'' and ''pharmacist.'' The ''health care provider'' definition in paragraph (3) of PHSA section 3000 (cited in the regulatory text as 42 U.S.C. 300jj(3)) references these types of health care providers without further definition. While our interpretation of these types of health care providers has always relied on the 42 U.S.C. 300jj(10) and (12) definitions of ''laboratory'' and ''pharmacist,'' we now propose to formally incorporate these definitions into the health care provider definition codified in § 171.102. Specifically, we propose to add to the § 171.102 definition of ''health care provider'' subparagraphs designated as (1) and (2) and citing, respectively, paragraphs (10) and (12) of 42 U.S.C. 300jj. In 42 U.S.C. 300jj(10), ''laboratory'' has the meaning given such term in 42 U.S.C. 263a(a) (PHSA section 353(a)). In 42 U.S.C. 300jj(12), ''pharmacist'' has the meaning given such term in 21 U.S.C 384(a)(2). For ease of reference, we provide in the following paragraphs of this preamble the laboratory and pharmacist definitions cross-referenced by 42 U.S.C. 300jj(10) and (12).

As stated in 42 U.S.C. 263a(a): ''laboratory'' or ''clinical laboratory'' means ''a facility for the biological, microbiological, serological, chemical, immuno-hematological, hematological, biophysical, cytological, pathological, or other examination of materials derived from the human body for the purpose of providing information for the diagnosis, prevention, or treatment of any disease or impairment of, or the assessment of the health of, human beings.'' In addition to having been cited by 42 U.S.C. 300jj since the HITECH Act added Title XXX to the PHSA in 2009, this definition of ''laboratory'' or ''clinical laboratory'' has stood since the Clinical Laboratory Improvement Amendments of 1988 amended section 353 of the PHSA (42 U.S.C. 263a(a)) to include this definition.[227]

As stated in 21 U.S.C. 384(a)(2), the term ''pharmacist'' means ''a person licensed by a State to practice pharmacy, including the dispensing and selling of prescription drugs.'' While the text of 42 U.S.C. 300jj(12) cites ''the meaning given such term in section 384(2) of title 21'' the only definition of ''pharmacist'' appearing in 21 U.S.C. 384 is found in paragraph (a)(2).[228]

We welcome comment on this proposal.

2. Health Information Technology or Health IT

We propose to codify in § 171.102 that, for purposes of the information blocking regulations in 45 CFR part 171, both ''health information technology'' and its shorter form, ''health IT,'' have the same meaning as ''health information technology'' in 42 U.S.C. 300jj(5). The health information technology definition was added to the Public Health Service Act (PHSA) (section 3000(5)) by the HITECH Act (see Title XIII, Subtitle A, section 13101 of the American Recovery and Reinvestment Act of 2009, Pub. L. 111–5). 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.''

Because the 21st Century Cures Act added the information blocking statute to Title XXX of the PHSA as section 3022 (42 U.S.C. 300jj–52), we believe the most applicable definition of the term ''health information technology'' in the context of PHSA section 3022 and our regulations in 45 CFR part 171 is the definition found at 42 U.S.C. 300jj(5). We believe that codifying this interpretation will increase certainty for actors [229] and other interested parties that when we refer to ''health information technology'' or ''health IT'' in 45 CFR part 171, we mean the 42 U.S.C. 300jj(5) definition unless otherwise specified in or for a specific subpart or section.

We leveraged the definition of ''health information technology'' from Title XXX of the PHSA (specifically, section 3000(5) of the PHSA) in finalizing the definition of ''interoperability element'' in § 171.102, but we did not use it in its entirety and did not explicitly cite it, in the ''interoperability element'' definition (85 FR 25956, see also preamble discussion at 85 FR 25807). This proposal to adopt a definition for ''health information technology'' in § 171.102 would not change the definition of ''interoperability element'' in § 171.102. Our definitions of ''health IT developer of certified health IT'' and ''offer health IT'' as they are currently codified in § 171.102 explicitly reference the definition of ''health information technology'' in 42 U.S.C. 300jj(5). Thus, this proposal would not change the meaning of either of those definitions.

We welcome comments on this proposal.

3. ''Interfere With'' or ''Interference''

The 21st Century Cures Act defined information blocking in part as a practice that ''is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information'' (42 U.S.C. 300jj–52(a)(1)). In the definitions section of the information blocking regulations (§ 171.102), we define *interfere with* or *interference* to mean ''to prevent, materially discourage, or otherwise inhibit.'' We propose to add a new section (45 CFR 171.104) to codify certain practices that constitute ''interference'' and ''interfere with'' (as defined in § 171.102) for purposes of the information blocking definition in § 171.103. Although these practices constitute an interference, we note that the list is not exhaustive and other practices not described in this proposed new section will also constitute an interference for purposes of the information blocking definition.

We emphasize that these proposed provisions are practices that constitute an interference. We do not attempt to establish facts and circumstances in this proposed rule that would specify practices that are information blocking

[227] *See* section 2 of the Clinical Laboratory Improvement Amendments of 1988 (Pub. L. 100–578,102 Stat. 2903). *See also* 42 U.S.C. 263a(a) authority citations (available online at *https://uscode.house.gov/view.xhtml?req=granuleid:U.S.C.-prelim-title42-section263a&num=0&edition=prelim*).

[228] Note 3 to 42 U.S.C. 300jj as it appears in the U.S. Code as maintained by the Office of law Revision Counsel of the U.S. House of Representatives reads: So in original. Probably should be ''(a)(2)''. (Available online at: *https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title42-chapter6A-subchapter28&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGU0Mi1zZWN0aW9uMzAwamotNTI%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim#300jj_3_target*.)

[229] Throughout Section IV of this proposed rule, we use ''actor'' as it is defined in § 171.102. (We do not propose in this rule to revise that codified definition.)

as the term is defined in § 171.103. For a practice to be information blocking, all elements of the definition must be met. This means that the individual or entity that engages in the practice must be an actor under the information blocking regulations; that the practice must be likely to interfere with the access, exchange, or use of EHI; and that the actor engaging in the practice meets the requisite knowledge standard. Further, ''information blocking'' does not include practices required by law or that meet an exception.

In the ONC Cures Act Proposed Rule (84 FR 7424), we noted that the information blocking provision and its enforcement subsection in the 21st Century Cures Act do not define the terms ''interfere with,'' ''prevent,'' and ''materially discourage.'' Based on our interpretation of the information blocking provision, as discussed in the Cures Act Proposed Rule, we proposed to define ''interfere with'' and ''interference'' as preventing, materially discouraging or otherwise inhibiting access, exchange, or use of electronic health information (84 FR 7516, 7601). We finalized the definition in the ONC Cures Act Final Rule as proposed, but with a modification to remove the phrase ''access, exchange, or use of electronic health information'' as unnecessary and duplicative of the information blocking definition (85 FR 25642, 25809; see also 45 CFR 171.102). The preamble discussion of the definition of ''interfere with'' or ''interference'' in the ONC Cures Act Final Rule provides guidance explaining the meaning of these terms.

In the ONC Cures Act Proposed Rule, to further clarify the scope of the information blocking provision, we provided several examples of practices that would constitute interference. We refer readers to the ONC Cures Act Proposed Rule (84 FR 7518 through 7521) for discussion of those examples, which we also cited in the ONC Cures Act Final Rule (85 FR 25811). We refer readers to the ONC Cures Act Final Rule (85 FR 25811 through 25818) for additional examples of practices likely to interfere with access, exchange, or use of electronic health information (EHI) and additional discussion, including responses to public comments received on the ONC Cures Act Proposed Rule.

Since publication of the ONC Cures Act Final Rule (May 1, 2020), we have provided additional guidance in the form of information blocking Frequently Asked Questions (FAQs). As of the time of publication of this proposed rule, we have posted 12 FAQs in the ''Interference'' category. Links to all categories of FAQs within the information blocking topic are available under the ''Resources'' heading of this page of ONC's website: *https://www.healthit.gov/topic/information-blocking.*[230]

Certain practices have been brought to our attention through submissions to the Report Information Blocking Portal, questions we have received through the *Health IT.gov* Feedback and Inquiry Portal, and other interactions (including interactions with parties interested in learning more about seeking or providing access, exchange, or use of EHI).[231] Often, the party will present a hypothetical scenario and inquire if the practice constitutes information blocking. For a variety of reasons, ONC does not opine on whether a given practice constitutes information blocking. First, ONC does not have authority to offer binding advisory opinions.[232] Second, ONC cannot readily determine whether a scenario focused on a specific action or inaction generally constitutes information blocking because whether a practice meets the § 171.103 information blocking definition will involve an assessment of all the elements of the information blocking definition, as discussed above, and will be based on the facts and circumstances of each unique situation.

Informed by the concerns and questions that interested parties have brought to our attention, we propose to add § 171.104 to 45 CFR part 171 to codify that certain practices will constitute interferences for purposes of the information blocking definition.

As previously noted, the practices we propose to codify are not an exhaustive list of all practices that constitute interferences. The practices in the proposed § 171.104 are intended to help regulated entities and other interested parties by codifying certain practices that constitute *interferences* for purposes of the information blocking definition. The practices we propose to codify include affirmative acts as well as omissions, because a practice, under the information blocking definition, can be ''an act or omission committed by an actor.''

The practices we propose to codify generally relate to:

- Actions taken by an actor to impose delays on other persons' access, exchange, or use of EHI;
- Non-standard implementation of health IT and other acts to limit interoperability of EHI or the manner in which EHI is accessed, exchanged, or used by other persons;
- Improper inducements or discriminatory contract provisions; and
- Omissions (failures to act). Some omissions which constitute interferences in the proposed § 171.104 include failures to publish (or make available for publication) technical information such as service base URLs for Certified API Technology. Other types of omissions include an actor's failure to fulfill requests for access, exchange, or use of EHI that is required by law, or failure to fulfill requests for access, exchange, or use of EHI when it is permitted by law and not inconsistent with any additional restrictions on access to the individual's EHI that the individual (patient) or their personal representative may have requested and that an actor agreed to honor.

In the proposed § 171.104(a)(3), we describe ''delaying the access, exchange, or use of EHI to or by a third-party app designated and authorized by the patient when there is a deployed application programming interface (API) able to support the access, exchange, or use of the EHI.'' In this paragraph and corresponding regulatory text (§ 171.104(a)(3)), the term ''app,'' as used in ''third-party app,'' describes any number of ''applications'' (or types of applications) a patient could use to access, exchange, or use their EHI—on their smart phone, computer, or smart watch, for example. These ''apps'' are able to communicate with other health information technology through an API (such as a Health IT Module certified to § 170.315(g)(10)) that permits EHI to be accessed and exchanged at the patient's direction.

In the proposed § 171.104(a)(6), we note that certain non-compete clauses can implicate the information blocking definition. In the ONC Cures Act Proposed Rule, we stated that one means by which actors may restrict access, exchange, or use of EHI is through formal, contractual restrictions (84 FR 7518). We provided several examples of restrictive contractual clauses in that proposed rule (84 FR 7518). In the ONC Cures Act Final Rule, we acknowledged that many

[230] The link to the *interference* category of FAQs directs to this URL: *https://www.healthit.gov/faqs?f%5B0%5D=subtopic%3A7031.* (Retrieved Apr. 9, 2024.)

[231] Report Information Blocking Portal URL: *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/6Health* IT Feedback and Inquiry Portal URL: *https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/2* Other interactions with interested parties include, for example, interactive discussion in various public venues, such as the ''Ask Us About Information Sharing'' sessions ONC has hosted since May 2020. (*https://www.healthit.gov/newsroom/past-events*)

[232] ONC requested but did not receive advisory opinion authority via the Congressional Appropriations Committee in fiscal years 2023 and 2024.

commenters stated that EHR developers place onerous contract terms on developers of applications that enable patient access to EHI through APIs (88 FR 25811). Regulated entities, software developers, and patient advocates have continued to express concerns to ONC about restrictive contractual clauses.

Actors are placing conditions on access to EHI in the actor's health IT that are unrelated to security or privacy laws, and function as anti-competitive clauses that effectively prevent certain employees or contractors from accessing, exchanging, or using EHI in other health IT. Therefore, we propose to identify a particular type of contractual clause as an interference: negotiating or enforcing a clause in any agreement that prevents or restricts an employee (other than the actor's employees), contractor, or contractor's employee who accesses, exchanges, or uses the EHI in the actor's health IT from accessing, exchanging, or using EHI in other health IT in order to participate in the design, development, or upgrade of such other health IT. This proposal is intended specifically to make clear that it is an interference to prevent employees of an individual or entity (other than the actor's employees) from working on software development and design for both Company A (actor's company) and Company B, even if the companies are competitors or potential competitors, and even if the work is being conducted simultaneously. We note that this interference could be found in ''any agreement,'' even an agreement to which the actor is not a party, provided that the actor requires another party to include such a clause in that party's contracts with its employees or contractors. In addition, it is an interference for the actor to negotiate or enforce such a clause—again, in any agreement.

Recently, the Federal Trade Commission (FTC) finalized a nationwide ban on most non-compete clauses in any employment contract (89 FR 38342). The FTC noted that non-compete clauses have many deleterious effects, including on earnings, job creation, innovation, consumer prices, and new business formation (80 FR 38343). Although the FTC's rule would not cover the types of restrictions that are covered by our proposal, we believe such clauses have the same effects on health information technology by restricting the ability of developers to work on different software and to enter into new contracts at the same time that they are contracted to work with an actor's software. Although the contractual language at issue may occasionally be couched in language claiming to protect intellectual property, the clauses function as anti-competitive clauses and not as clauses protecting intellectual property from infringement or misappropriation. We note that in some cases, there are applicable laws that prevent employees and contractors from misusing intellectual property. Our proposal would not impact legally permissible intellectual property protections. In addition, we note that the Licensing Exception in § 171.303 acknowledges intellectual property rights, including the administration of a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets.

We solicit comment on all aspects of our proposed description of the interference in § 171.104(a)(6). We specifically ask if we should add ''including health IT for a competitor or potential competitor'' at the end of the paragraph. We solicit comment on whether it is necessary to say ''access, exchange, or use'' or if ''access or use'' of EHI is sufficient. We specifically used the term ''agreement'' instead of ''contract'' because we recognize that such clauses can also be found in licensing agreements and other agreements that are not typically referred to as a contract. We also ask, more broadly, whether there are other types of agreements that should specifically be identified in the text of § 171.104(a)(6), such as those specified in the Cures Act rulemaking (84 FR 7518 and 88 FR 25811). Because we recognize that sometimes the actor induces a contractor to include the language in the agreement the contractor has with its employees, we use the phrase ''negotiating or enforcing'' to ensure that an actor inducing or forcing a customer, business associate, or any other entity to include such restrictions would also be considered an interference. We ask commenters to opine on whether ''negotiating or enforcing'' is broad enough to cover the situations intended to be covered by the description in § 171.104(a)(6), and whether any terms should be added to the definitions section of the regulation as a result of this or other descriptions of interferences in § 171.104.

We also solicit comments on the rest of the descriptions of interferences in the proposed § 171.104. Are the descriptions clear enough for regulated entities and those whose access, exchange, or use of EHI that might be adversely affected by the conduct to understand the intended policy? Are there other practices that interested parties believe should be explicitly identified in regulatory text as constituting interference? Would codification of more or fewer interferences be more helpful? In considering these questions, we remind readers that ''interference'' or ''interfere with'' includes practices that prevent, materially discourage, or otherwise inhibit the access, exchange, and use of EHI.

Finally, we reiterate and emphasize that the descriptions in the proposed § 171.104 are of conduct constituting ''interference.'' The facts and circumstances of an actor's engaging in any of these practices, or any other practice likely to interfere with access, exchange, or use of EHI, would determine whether the practice constitutes ''information blocking.'' OIG has the statutory authority to investigate allegations of information blocking and to determine whether information blocking has occurred.

a. Application of ''Interference'' to TEFCA™ Requirements

Having discussed practices that would be considered interferences, we want to take this opportunity to identify certain practices that we believe would be unlikely to interfere with the access, exchange, and use of EHI under the information blocking definition. Specifically, it would be unlikely to be an interference for Qualified Health Information Networks™ (QHINs), Participants, or Subparticipants to comply with required provisions of the Common Agreement and the incorporated terms of participation and standard operating procedures, respectively. In the ONC Cures Act Final Rule, we took a similar approach and identified certain practices that we believed would be unlikely to interfere with the access, exchange, and use of EHI. Specifically, we explained that an actor's practice that focused on educating individuals about the privacy and security risks posed by certain applications would be unlikely to rise to the level of an interference when certain conditions were met, and therefore would be unlikely to meet the definition of information blocking (85 FR 25815).

Many interested parties, directly and through responses to proposed rules and requests for information, have inquired about the implications of following requirements of the Trusted Exchange Framework and Common Agreement™ (TEFCA™), including the related terms of participation and standard operating procedures, with respect to the information blocking definition. In light of the concerns and questions that interested parties have brought to our attention with respect to TEFCA, we believe it is important to provide

guidance to actors who are QHINS™, Participants, or Subparticipants that practices they must undertake to comply with TEFCA requirements would be unlikely to rise to the level of an interference under the information blocking definition. We believe providing such guidance with respect to TEFCA requirements is important because when actors choose to access, exchange, and use EHI through TEFCA, their compliance with TEFCA requirements supports the policy goals of the Cures Act and information blocking regulations more broadly, such as to promote confidence in health IT infrastructure and interoperability (see 85 FR 25649, 25794, 25804, 25805, and 25806) by advancing interoperability and expanding secure access, exchange, and use of EHI. We also believe that because the proposed § 171.104 does not describe the full universe of practices that could constitute an interference, it is important to clarify that compliance with TEFCA requirements, in the context of TEFCA participation by a QHIN, Participant, or Subparticipant, is unlikely to constitute an interference under the information blocking definition.

Actors who are QHINs, Participants, or Subparticipants have documents relevant to their participation in TEFCA, including documents such as the Common Agreement, terms of participation, and standard operating procedures. These documents may for example, establish certain standards to ensure the security of EHI, or on the manner of exchange of EHI.

In certain cases, QHINs, Participants, or Subparticipants may engage in practices not specifically required by the Common Agreement, terms of participation, and standard operating procedures. Our guidance does not extend to such permissible or optional practices. To this point, not complying with a request for access, exchange, or use of EHI via the standards adopted in 45 CFR 170.215, including version(s) of those standards approved pursuant to 45 CFR 170.405(b)(8), *could* be an interference, *could* implicate the information blocking definition, and would not be covered by the TEFCA Manner Exception (§ 171.403). Further, in general and for clarity, any practice (act or omission) between TEFCA entities that is not one specifically required by the Common Agreement, including its terms of participation and standard operating procedures, as well as any practice involving or affecting non-participants in TEFCA *could* also be an interference. For practices that are not required under TEFCA and/or that affect non-participants in TEFCA, which could constitute an interference, all of the other voluntary exceptions in part 171 would be available, as appropriate.

We seek comments on our discussion. Does this discussion sufficiently reassure actors interested in participating in TEFCA that complying with the requirements of TEFCA as a QHIN, Participant, or Subparticipant would be unlikely to constitute ''interference'' under the information blocking definition? We also welcome comment on the desirability of further Federal guidance or education materials on the interaction between the information blocking regulations and the Common Agreement, including terms of participation and standard operating procedures.

B. Exceptions

1. Privacy Exception

a. Privacy Exception—Definition of Individual

For purposes of the Privacy Exception, the term ''individual'' is defined in § 171.202(a)(2). When the Privacy Exception in § 171.202 and paragraph (a)(2) were initially established by the ONC Cures Act Final Rule, the codified text included a typographical error that was not identified until after publication. In the ONC Cures Act Final Rule (at 85 FR 25957) and the current *Code of Federal Regulations,* the text of § 171.202(a)(2)(iii), (iv), and (v) cross-references paragraphs (a)(1) and (2) of § 171.202 instead of paragraphs (a)(2)(i) and (ii) when referencing a person who is the subject of EHI in defining the term ''individual.'' We now propose to make a technical correction to cross-references within the text of § 171.202(a)(2)(iii), (iv), and (v) to accurately cross-reference paragraph (a)(2)(i), (a)(2)(ii), or both, as applicable.

Paragraph (a)(2) of the current § 171.202 defines the term ''individual'' in part by referring to its definition in 45 CFR 160.103. In § 171.202(a)(2)(i), we cross-reference to the definition of ''individual'' as defined in the HIPAA Privacy Rule at 45 CFR 160.103. In (a)(2)(ii), we provide a second definition: ''any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.'' [233] Then, in (a)(2)(iii), (iv), and (v), we expand on those two definitions in order to include persons legally acting on behalf of such individuals or their estates in certain circumstances. However, the current text of § 171.202(a)(2)(iii), (iv), and (v) incorrectly references a ''person described in paragraph (a)(1) or (2) of this section'' instead of referencing a ''person described in paragraph (a)(2)(i) or (ii) of this section.''

The ONC Cures Act Final Rule preamble demonstrates our intent for the definition of ''individual'' in paragraph (a)(2) of § 171.202. Citing the ONC Cures Act Proposed Rule at 84 FR 7526, we stated in the ONC Cures Act Final Rule preamble (85 FR 25846 through 25847) that ''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.'' Further, still referencing the ONC Cures Act Proposed Rule preamble, we wrote at 85 FR 25845 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.'' The paragraph designated as ''(a)(3)'' in the Proposed Rule at 84 FR 7602 and referenced simply as ''(3)'' in the discussion at 85 FR 25845 was designated as (a)(2)(iii) in § 171.202 as finalized at 85 FR 25957 and currently codified.

The quotes from the ONC Cures Act Final Rule preamble above demonstrate a consistent intention across the ONC Cures Act Proposed and Final Rules to cross-reference in the paragraphs finalized (at 85 FR 25957) and codified in § 171.202 as (a)(2)(iii), (iv), and (v) the paragraphs finalized and codified in § 171.202(a)(2)(i) and (ii). Accordingly, we propose the technical correction in the revised text of 45 CFR 171.202 to reflect the correct reading and intent.

In drafting our proposed technical correction to § 171.202(a)(2), we determined that the cross-reference to (a)(2)(ii), a natural person who is the subject of the EHI being exchanged *other than* an individual as defined in

[233] The definition of ''person'' for purposes of 45 CFR part 171 is codified in § 171.102 and is, by cross-reference to 45 CFR 160.103, the same definition used for purposes of the HIPAA Privacy Rule (45 CFR part 160 and subpart E of 45 CFR part 164). The § 160.103 definition of ''person'' clarifies the meaning of ''natural person'' within it. We use ''natural person'' with that same meaning in § 171.202(a)(2) and throughout this discussion of § 171.202(a)(2).

45 CFR 160.103, is not needed in describing (in (a)(2)(iii)) a person acting as a personal representative in making decisions related to health care specifically in accordance with 45 CFR 164.502(g). This is because 45 CFR 164.502(g) pertains personal representatives of individuals as defined in 45 CFR 160.103 (persons who are the subject of PHI) under the HIPAA Privacy Rule. A person described in (a)(2)(i) is an individual as defined in 45 CFR 170.103 for purposes of the HIPAA Privacy Rule. However, (a)(2)(ii) describes ''any *other* natural person who is the subject of the EHI being accessed, exchanged, or used'' (emphasis added) rather than an ''individual'' who is the subject of PHI under the HIPAA Privacy Rule. Such *other* person (described in (a)(2)(ii)) would not have a person who is a ''personal representative'' specifically in accordance with the 45 CFR 164.502(g) provisions pertaining to ''personal representatives'' under the HIPAA Privacy Rule. Therefore, we propose to strike the unnecessary reference to § 171.202(a)(2)(ii) (a subject of EHI who does *not* meet the 45 CFR 160.103 (HIPAA Privacy Rule) definition of ''individual'') from the § 171.202(a)(2)(iii) description of a person who acts as a personal representative specifically in accordance with the HIPAA Privacy Rule provisions in 45 CFR 164.502(g). By striking an unnecessary cross-reference, this proposal would simplify the regulatory text without changing what the § 171.202(a)(2) definition of ''individual'' means or how it applies in practice.

b. Privacy Sub-Exception—Interfering With Individual Access Based on Unreviewable Grounds

In the ONC Cures Act Final Rule (85 FR 25856), we finalized in § 171.202(d) a sub-exception to the Privacy exception applicable to the denial of an individual's request for electronic health information consistent with ''unreviewable grounds'' for denial of access under 45 CFR 164.524. As we explained in the ONC Cures Act Final Rule, 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 (85 FR 25856). (See 45 CFR 164.524(a)(2) for the full listing of circumstances in which individual may be denied access under 45 CFR 164.524 without the individual being provided an opportunity for review of the denial.)

The current text of § 171.202(d) is explicitly applicable when an individual requests EHI under the HIPAA individual right of access standard (45 CFR 164.524(a)(1)) from an actor who must comply with this HIPAA Privacy Rule provision. Thus, the sub-exception is available only to actors who are also HIPAA covered entities or business associates.[234]

We explained how the sub-exception currently operates in the ONC Cures Act Final Rule preamble (see 85 FR 25856 through 25857). The current text of § 171.202(d) states that the actor's practice ''must be consistent with 45 CFR 164.524(a)(2).'' The preamble discussion of this sub-exception explains that an actor who chooses to deny the request must, to satisfy the § 171.202(d) sub-exception, meet the actor's obligations [235] under the HIPAA Privacy Rule. Thus, if an actor who also must comply with 45 CFR 164.524(a)(1) denies, on unreviewable grounds, access to some or all of the protected health information (PHI) that is also EHI [236] requested by the individual in compliance with the HIPAA Privacy Rule requirements, the denial is covered under the § 171.202(d) sub-exception as currently codified.

We propose to broaden the applicability of the sub-exception so that it is available to any actor responding to a request for EHI where the circumstances set out in 45 CFR 164.524(a)(2)(i) through (v) apply, and not just for actors who are also HIPAA covered entities or business associates. Allowing the same information blocking sub-exception to cover a practice regardless of whether the actor engaging in the practice is also required to comply with the HIPAA Privacy Rule does not create a misalignment for actors who *are* subject to both the information blocking regulations and the HIPAA Privacy Rule. Instead, making this sub-exception available to all actors under the same conditions in which the sub-exception is available to HIPAA covered entities should reduce unnecessary variation across actors, improve compliance efficiency, and provide additional certainty as it relates to the applicability of this exception.

We believe that broadening the applicability of the unreviewable grounds sub-exception (§ 171.202(d)) to practices by actors who are not required to comply with the HIPAA Privacy Rules will provide greater benefit to actors than creating unique requirements for the application of § 171.202(d) to such actors' practices in the circumstances set forth in § 164.524(a)(2). Actors who are not required to comply with the HIPAA Privacy Rule would need to familiarize themselves with up-to-date 45 CFR 164.524 implementation specifications that would apply to the actor's denial of access to the EHI in question in the circumstances set forth in § 164.524(a)(2) if the actor were a HIPAA covered entity or business associate. This is similar to such actors needing to familiarize themselves with the HIPAA Privacy Rule definitions for ''ePHI'' and ''designated record set'' (in §§ 160.103 and 164.501) for purposes of understanding the EHI definition in § 171.102. Actors who are not HIPAA covered entities or business associates and who want to obtain help in learning about denials of individual access in the circumstances specified in § 164.524(a)(2) could find a variety of educational sources to choose from. However, most health care providers, HIN/HIEs, health information management professionals, and health IT developers of certified health IT throughout the United States have experience complying with the HIPAA Privacy Rule.

To clearly establish coverage of the § 171.202(d) sub-exception for all actors' practices under the same requirements, we propose to change the name of the sub-exception to: ''interfering with individual access based on unreviewable grounds.'' This proposed change to the header text is intended to express the expansion of the sub-exceptions' availability to all actors. Additionally, the proposed regulatory text would remove the current text's reference applying the sub-exception only to actors required to comply with the HIPAA right of access standards and only where the individual is making a request ''under the right of access provision under 45 CFR 164.524(a)(1).'' Instead, the proposed text would provide that the sub-exception applies where an individual requests their EHI from any actor in circumstances set

[234] *See* the definitions of ''covered entity'' and ''business associate'' at 45 CFR 160.103.

[235] At 85 FR 25856, we referred to the actor's HIPAA Privacy Rule compliance obligations in this situation as ''its requirements.'' We use more precise wording here for clarity.

[236] As defined in § 171.102 and excluding certain information as specified in subparagraphs (1) and (2) of this definition, EHI is electronic protected health information (ePHI) (defined in 45 CFR 160.103) that is or would be in the designated record set (defined in 45 CFR 164.501). It may be helpful for purposes of this discussion to think of EHI as a subset of PHI. The HIPAA right of access standard (45 CFR 164.524) applies to PHI that is not ePHI (*e.g.,* paper records), but § 171.202 would be moot with respect to PHI that is not ePHI and therefore does not meet the EHI definition in § 171.102.

forth in 45 CFR 164.524(a)(2). The proposed revision would, further, cross-reference the implementation specifications set out in 45 CFR 164.524 (access of individuals to protected health information) that HIPAA covered entities and business associates must already meet to comply with the HIPAA Privacy Rule when denying individual access on ''unreviewable grounds'' (45 CFR 164.524(a)(2)).

We seek comments on this proposal.

c. Privacy Sub-Exception—Individual's Request Not To Share EHI

We propose to slightly modify the header of § 171.202(e) for ease of reference to ''individual's request not to share EHI.'' More importantly, we propose to revise the sub-exception to remove the existing limitation that applies the exception only to individual-requested restrictions on EHI sharing that are permitted by other applicable law. The proposal would extend the availability of the § 171.202(e) sub-exception to an actor's practice of implementing restrictions the individual has requested on the access, exchange, or use of an individual's EHI even when the actor may have concern that another law or instrument could attempt to compel the actor to fulfill access, exchange, or use of EHI contrary to the individual's expressed wishes.

The existing text and scope of 45 CFR 171.202(e) was established in 2020 by the ONC Cures Act Final Rule (85 FR 25642). When the sub-exception was finalized, health care providers and other actors did not raise explicit concerns regarding when they must comply with statutes, regulations, or instruments (such as subpoenas) issued under the laws of states in which they are not licensed, do not reside, and do not furnish care. In 2022, the Supreme Court decision in *Dobbs* v. *Jackson Women's Health Organization* overturned precedent that protected a constitutional right to abortion and altered the legal and health care landscape.[237] Since the Court's decision, across the United States, a variety of states have newly enacted or are newly enforcing restrictions on access to reproductive health care. The Court's ruling—and subsequent state restrictions—have had far-reaching implications for health care beyond the effects on access to abortion.[238]

In light of the changing landscape, we are concerned that actors might deny or terminate an individual's requested restrictions on sharing their EHI specifically due to uncertainty about whether the actor is aware of and can account for any and all laws that might override the individual's requested restrictions. An actor who might otherwise be inclined to agree to an individual's request not to share their EHI could be concerned about potential information blocking implications of honoring those individual requests in the face of demands for disclosure that *might* ultimately be enforced in a court of competent jurisdiction. In particular, we are concerned that actors may be unwilling to consider granting individuals' requests for restrictions, or may prematurely terminate some or all requested restrictions, based on uncertainty as to whether information blocking penalties or disincentives might be imposed in addition to costs the actor may incur to confirm whether the actor is, by other authority, compelled to provide access, exchange, or use of EHI despite the individual's wishes. For example, we understand actors are concerned about potentially implicating the information blocking definition by delaying a disclosure of EHI pursuant to a court order that the actor is aware is being contested, so that the actor can wait to see if the order will, in fact, compel the actor to make EHI available for access, exchange, or use contrary to the individual's request for restrictions to which the actor had agreed consistent with § 171.202(e). Accordingly, the removal of ''unless otherwise required by law'' from § 171.202(e) would be a useful complement to the existing Precondition Not Satisfied sub-exception (§ 171.202(b)) to help address actors' uncertainty about various state laws' applicability as they relate to information blocking. As currently codified, § 171.202(b) sub-exception of the Privacy Exception outlines a framework for actors to follow so that the actors' practices of not fulfilling requests to access, exchange, or use EHI would not constitute information blocking when one or more preconditions has not been satisfied for the access, exchange, or use to be permitted under applicable Federal and State, or Tribal laws.

To be clear, the proposed revision to § 171.202(e) would not operate to override other law compelling disclosure against the individual's wishes. It would, however, offer actors who elect to honor individual requested restrictions certainty that applying those restrictions will not be considered information blocking so long as the actor's practices in doing so satisfy the requirements of the § 171.202(e) sub-exception. Whether the courts will or should apply any particular Federal, state, or Tribal law to any actor (or enforce orders issued under such laws to any actor in any particular circumstances) is beyond the scope of this proposal. If or where there may be a law that is enforced by a court with jurisdiction over the actor and subject matter and that requires a particular actor to fulfill access, exchange, or use of EHI without the individual's authorization, permission, or consent, the actor might be compelled to comply with that law independent of the information blocking statute and 45 CFR part 171. This would continue to be the case even if we were to finalize the proposed revision to § 171.202(e).

We also remind HIPAA covered entities and business associates that they must comply with the HIPAA Privacy Rule, including privacy protections in the HIPAA Privacy Rule to Support Reproductive Health Care Privacy Final Rule and any other applicable Federal laws that limit access, exchange, or use of EHI in particular circumstances. For example, an actor's practice likely to interfere with an individual's access, exchange, or use of EHI (as defined in 45 CFR 171.102) might satisfy an information blocking exception without fully satisfying the actor's separate obligations under 45 CFR 164.524 (HIPAA Privacy Rule's individual right of access). In such cases, an actor that is a HIPAA covered entity or business associate would be subject to penalties for violating the HIPAA Privacy Rule.

We welcome comments on this proposal.

2. Infeasibility Exception

In the ONC Cures Act Final Rule, ONC established the Infeasibility Exception (§ 171.204) (85 FR 25865 through 25870, and 85 FR 25958). Under the Infeasibility Exception, it is not considered information blocking if an actor, as defined in § 171.102, does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided the actor satisfies at least two conditions: the § 171.204(b) *responding to requests* condition and

[237] *See* 142 S. Ct. 2228.

[238] *See* Melissa Suran, ''Treating Cancer in Pregnant Patients After *Roe* v *Wade* Overturned,'' JAMA (Sept. 29, 2022), (available at *https://jamanetwork.com/journals/jama/fullarticle/2797062#:~:text=The%20US%20Supreme%20Court,before%20cancer%20treatment%20can%20begin),* and Rita Rubin, ''How Abortion Bans Could Affect Care for Miscarriage and Infertility,'' JAMA (June 28, 2022), (available at *https://jamanetwork-com.hhsnih.idm.oclc.org/journals/jama/fullarticle/2793921?resultClick=1).* (URLs retrieved May 23, 2024.)

any one of the conditions in § 171.204(a).

In the HTI–1 Final Rule (89 FR 1436, see preamble at 89 FR 1373 through 1387), we finalized the following revisions to § 171.204:

- clarification of the § 171.204(a)(1) *uncontrollable events* condition requirement that the uncontrollable event must have an actual negative impact on an actor's ability to fulfill EHI access, exchange, or use in order for *uncontrollable events* condition to apply;
- addition of two new conditions (*third party seeking modification use* and *manner exception exhausted,* respectively subparagraphs (3) and (4)) under paragraph (a); and
- renumbering the *infeasible under the circumstances* condition from § 171.204(a)(3) to § 171.204(a)(5).

However, in the HTI–1 rulemaking, we did not change the substance of the *infeasible under the circumstances* condition (now codified in § 171.204(a)(5)) or the § 171.204(a)(2) *segmentation* condition, and we did not make any changes to § 171.204(b). In this rule, we propose to modify:

- the § 171.204(a)(2) *segmentation* condition as described in section IV.B.2.a;
- the § 171.204(a)(3) *third party seeking modification use* conditions as described in section IV.B.2.b; and
- the § 171.204(b) *responding to requests* condition as discussed in section IV.B.2.c (of this proposed rule).

a. Segmentation Condition Modifications

The § 171.204(a)(2) *segmentation* condition currently applies where the actor is not able to fulfill a request for access, exchange, or use of EHI specifically because the actor cannot unambiguously segment from other requested EHI the EHI that cannot be made available by law or due to an individual's preference, or that may be withheld in accordance with § 171.201. In practice, ''by law or due to an individual's preference'' would include situations where: an actor has chosen to honor an individual's request for restrictions on sharing of some of their EHI; an individual's authorization or consent is a pre-requisite for a particular use or disclosure of their EHI to be lawful and the individual has not provided such authorization or consent; or law applicable in the circumstances of the request restricts sharing of the EHI.

We propose updates to the *segmentation* condition to enhance clarity and certainty, and to provide for its application to additional situations. We propose to update how the regulation text describes why certain EHI cannot or will not be made available, including more specific cross-references to relevant provisions within 45 CFR part 171.

Currently, the *segmentation* condition references (in subparagraph (i) of § 171.204(a)(2)) EHI that cannot be made available due to an individual's preference or by law, and (in subparagraph (ii) of § 171.204(a)(2)) EHI that the actor may choose to withhold in accordance with the Preventing Harm Exception. We propose to revise the condition (§ 171.204(a)(2)) as follows: to focus subparagraph (i) on EHI that is not permitted by applicable law to be made available, and to explicitly cross-reference in subparagraph (ii) the proposed Protecting Care Access Exception (§ 171.206) and the existing Privacy Exception (§ 171.202) in addition to the existing Preventing Harm Exception (§ 171.201) (which currently has an explicit cross-reference).

We believe that focusing § 171.204(a)(2)(i) solely on EHI that is not permitted by applicable law to be made available for a requested access, exchange, or use will reinforce for actors and other interested persons that actors cannot make EHI available when applicable law, such as the HIPAA Privacy Rule or 42 CFR part 2, does not permit covered information to be made available. Under our proposed revision of § 171.204(a)(2)(i), the *segmentation* condition would continue to apply as it does today when an actor cannot unambiguously segment EHI that, under applicable law, is permitted to be available to a particular person for a particular purpose from EHI that is not permitted to be available to that person for that purpose. This would include situations where the actor cannot unambiguously segment EHI for which preconditions for permitting use or disclosure under the HIPAA Privacy Rule (or other applicable law) have not been met from EHI for which such preconditions have been met, as well as scenarios where use or disclosure of specific EHI for a particular purpose is prohibited by applicable law.

The proposed revision to § 171.204(a)(2) would retain in subparagraph (ii) explicit reference to the Preventing Harm Exception (§ 171.201). Thus, the Infeasibility Exception's revised *segmentation* condition would continue to apply where the actor cannot unambiguously segment other EHI from EHI that the actor has chosen to withhold in accordance with the Preventing Harm Exception (§ 171.201).

We propose to explicitly add reference to § 171.202 in our revision to subparagraph (ii) of § 171.204(a)(2). This would ensure that the *segmentation* condition would continue to apply where the actor cannot unambiguously segment other EHI they could lawfully make available from EHI for which the actor has chosen to honor the individual's request not to share the EHI (consistent with § 171.202(e) sub-exception). In addition, citing § 171.202 in the proposed revision to subparagraph (ii) of § 171.204(a)(2) would expand explicit application of the § 171.204(a)(2) *segmentation* condition to certain situations where an actor subject to multiple laws with inconsistent preconditions adopts uniform privacy policies and procedures to adopt the more restrictive preconditions (as provided for under the Privacy sub-exception Precondition Not Satisfied, see § 171.202(b)(3) as currently codified). By referencing all of the Privacy Exception (§ 171.202), the proposed revised § 171.204(a)(2)(ii) would allow the Infeasibility Exception's *segmentation* condition to apply where an actor (who has adopted the more restrictive of multiple laws' preconditions for sharing of some information about an individual's health or care consistent with § 171.202(b)) cannot unambiguously segment EHI for which a more restrictive precondition has not been met from other EHI that the actor could lawfully share in the jurisdictions with less restrictive preconditions.

By referencing all of the Privacy Exception (§ 171.202), the proposed revision would also extend the *segmentation* condition's coverage to situations where the actor is unable to unambiguously segment EHI that could be made available from specific EHI that the actor may choose to withhold from the individual or their (personal or legal) representative consistent with the § 171.202(d) Privacy sub-exception ''denial of individual access based on unreviewable grounds.''

We have identified a possibility that individuals and interested parties could be concerned that extending the *segmentation* condition's coverage could affect the speed with which actors move to adopt or improve segmentation capabilities. Segmentation capabilities may need to be improved to sequester the EHI that may be withheld from an individual on certain unreviewable grounds from *other* EHI an actor may have for that individual. For instance, in comparison to health information that may need to be sequestered for other reasons, different or additional segmentation functionality may be

needed to sequester from other EHI only that information created or obtained in the course of research that includes treatment and only for as long as the research is in progress.[239] While the actor that is a HIPAA covered entity would still need to satisfy the individual's right of access to other PHI to the extent possible (see 45 CFR 164.524(d)(1)), the form and format in which the PHI is readily producible (see 45 CFR 164.524(c)(2)) may not be supported by the same electronic manner of access, exchange, or use that the individual would prefer. Therefore, we invite commenters to share any concerns or other perspectives they may wish to share relevant to this issue. We also propose in the alternative to reference only Privacy Exception sub-exceptions *other than* denial of access based on unreviewable grounds (§ 171.202(d)) in the revised § 171.204(a)(2) *segmentation* condition. Including this alternative proposal in this proposed rule means we could decide to finalize the revision to the § 171.204(a)(2) *segmentation* condition with or without cross-reference to (or that would include) ''denial of access based on unreviewable grounds'' (§ 171.202(d)).

For an actor's practice to be consistent with the § 171.202 Privacy Exception, the practice must meet the requirements set forth in any one of the sub-exceptions enumerated in § 171.202 (b) through (e). Referencing the entirety of § 171.202 in § 171.204(a)(2)(ii) would, therefore, also extend application of the Infeasibility Exception's *segmentation* condition to situations where a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule may withhold EHI they could otherwise lawfully make available based on an organizational privacy policy consistent with the § 171.202(c) sub-exception. (As used in § 171.202, ''HIPAA Privacy Rule'' means 45 CFR parts 160 and 164 (§ 171.202(a)(1).)

Because the § 171.202(c) sub-exception is applicable only where a health IT developer of certified health IT is not required to comply with the HIPAA Privacy Rule, it would apply in situations where the health IT developer of certified health IT is not required to comply with the individual right of access in 45 CFR 164.524. We believe it is possible that some individuals might seek health care or other services from such developers' customers (including health care providers) who are not HIPAA covered entities. In such situations, a State, or Tribal law may operate to provide the individual rights to access their health information that the actor has. (Determining what other laws may operate, or how, in specific circumstances is beyond the scope of this proposed rule.) Although the number of such situations may be relatively small, we do recognize it is possible for some individuals to find themselves in situations where no other law explicitly guarantees them a right to access EHI of which the individual is the subject (or the legal representative of the subject). In such situations, the individual may rely solely on the information blocking statute to ensure actors will not unreasonably and unnecessarily interfere with the individual's EHI access, exchange, or use. We are, therefore, interested in whether commenters may be concerned about potential unintended consequences of extending the (§ 171.204(a)(2)) *segmentation* condition to situations where a health IT developer is not required to comply with HIPAA and cannot segment EHI they have *chosen* to withhold consistent with the actor's own organizational privacy policies from other EHI. Would extending the *segmentation* condition to situations where a health IT developer has chosen to withhold EHI consistent with the Privacy sub-exception ''health IT developer of certified health IT not covered by HIPAA'' (§ 171.202(c)) pose too much risk of such developers avoiding individuals' EHI requests by choosing not to develop segmentation capabilities in the health IT they provide their customers who are not HIPAA covered entities? We welcome commenters' thoughts on this question. We also propose in the alternative to reference in the revised § 171.204(a)(2)(ii) *segmentation* condition only Privacy Exception sub-exceptions *other than* § 171.202(c) ''health IT developer of certified health IT not covered by HIPAA'' sub-exception. Including this alternative proposal in this proposed rule means we could decide to finalize the revision to the § 171.204(a)(2)(ii) *segmentation* condition with or without cross-reference to (or that would include) § 171.202(c) ''health IT developer of certified health IT not covered by HIPAA.''

As discussed in section IV.B.3 of this preamble, the § 171.206 Protecting Care Access Exception would apply to practices that an actor chooses to implement that are likely to interfere with access, exchange, or use of specific EHI (including, but not limited to, withholding such EHI) when relevant conditions are met. We propose to reference § 171.206 in the proposed revised § 171.204(a)(2)(ii) because the proposed § 171.206(a) *threshold* condition's requirements include (among others) a requirement that the actor's practice be no broader than necessary to reduce the risk of potential exposure of any person(s) to legal action that the actor believes could arise from the particular access, exchange, or use of the specific EHI. The actor's lack of technical capability to sequester only the EHI for which relevant conditions of § 171.206 have been satisfied would not render § 171.206 applicable to interference with the lawful access, exchange, or use of other EHI pertaining to the same individual(s). Therefore, the proposed reference to § 171.206 in the proposed revised § 171.204(a)(2)(ii) would accommodate circumstances where an actor lacks the technical capability to unambiguously segment the EHI the actor has chosen to withhold consistent with the Protecting Care Access Exception (§ 171.206, if finalized) from other EHI that they could lawfully make available. The requirements for an actor's practice to satisfy the proposed new § 171.206 exception, including the § 171.206(a) *threshold* condition that would be relevant to any practice to which § 171.206 could apply as well as when the § 171.206(b) *patient protection* or § 171.206(c) *care access* conditions are relevant, are discussed in detail in section IV.B.3, below in this preamble.

We solicit comments on these proposals.

b. Third Party Seeking Modification Use Condition Modifications

In the HTI–1 Final Rule (89 FR 1436) we excluded from applicability of the *third party seeking modification use* condition of the Infeasibility Exception (§ 171.204(a)(3)) a health care provider's requests for modification use from an actor that is its business associate. In the HTI–1 Final Rule, we noted that, for reasons stated in response to comments suggesting the condition's applicability exclusion may not be broad enough and in consideration of all comments on our discrete proposal, we did not expand the finalized exclusion from applicability of the condition as some commenters had requested (89 FR 1379). We also noted that we may consider amending the *third party seeking modification use* condition in the future if doing so may be appropriate (89 FR 1379). Upon further consideration, we now propose in § 171.204(a)(3)(ii) to extend the

[239] Please *see* 45 CFR 164.524(a)(2)(iii) for the HIPAA Privacy Rule's full ''unreviewable grounds for denial'' circumstances to which this example alludes.

exclusion from applicability of the condition.

We now propose to revise the *third party seeking modification use* condition to designate the existing exclusion from the applicability of this condition as subparagraph (i) of § 171.204(a)(3), and within it change the words ''health care provider'' to ''covered entity as defined in 45 CFR 160.103.'' We propose this change because the HIPAA Privacy and Security Rules require that all covered entities and their business associates safeguard the privacy, security, and integrity of EHI, not just health care providers. As we noted in the HTI–1 Proposed Rule (88 FR 23866), covered entities and business associates often have a level of trust and contractual protections that reduce certain concerns, such as security and data provenance, that led us to propose the *third party seeking modification use* condition. In addition, as we noted in the HTI–1 Proposed Rule discussion of the limitation of this condition, covered entities and their business associates (as permitted by their business associate agreements) need to access and modify relevant EHI held by other business associates of those covered entities on a regular basis (88 FR 23866). Therefore, we believe the exclusion from applicability of this condition should encompass requests from all covered entities to their business associates.

We also propose to exclude from applicability of the condition requests from any health care provider (as defined in § 171.102), who is not a HIPAA covered entity (as defined in 45 CFR 160.103) but who is requesting modification use from an actor whose activities would make the actor a business associate of that same health care provider if that health care provider were a HIPAA covered entity. Even if a health care provider is not a HIPAA covered entity, a health care provider likely has obligations and responsibilities under State law [240] and according to accreditation organizations' requirements [241] and payers' requirements [242] to keep and maintain medical records. Those responsibilities will likely require a health care provider to be able to regularly access and modify EHI held by entities who perform the functions of a business associate (as defined in 45 CFR 160.103) and would be considered a business associate of the health care provider if the health care provider were a covered entity. Further, it is our expectation that even if a health care provider is not a HIPAA covered entity and, therefore, does not have a HIPAA business associate agreement with an actor who maintains EHI or health IT system(s) or application(s) for the health care provider, the health care provider likely would have a pre-existing relationship with the actor similar to the relationship that a covered entity health care provider would have with their business associate, in terms of the existing level of trust, responsibilities, and obligations to handle EHI safely and securely. The health care provider who is not a HIPAA covered entity may be asking for modification use of EHI from an actor for the same purpose(s) that a health care provider who is a covered entity would be. We, therefore, propose to revise the *third party seeking modification use* condition by adding subparagraph (ii) of § 171.204(a)(3) that would exclude from applicability of the condition requests from health care providers (as defined in § 171.102) who are not HIPAA covered entities, requesting modification use from actors who would be considered the health care provider's business associate if the health care provider were a covered entity as defined in 45 CFR 160.103.

We welcome comments on these proposals.

c. Responding to Requests Condition Modifications

The Infeasibility Exception currently includes as paragraph (b) of § 171.204 a *responding to requests* condition. To satisfy the Infeasibility Exception as a whole, an actor's practice must meet the requirements of the § 171.204(b) *responding to requests* condition in addition to meeting at least one of the conditions in § 171.204(a). To meet the § 171.204(b) *responding to requests* condition, if an actor does not fulfill a request for access, exchange, or use of EHI consistent with any of the conditions in paragraph (a) of § 171.204, then the actor must provide, within ten business days of receipt of the request, to the requestor a written reason(s) why the request is infeasible.

We propose to modify the § 171.204(b) *responding to requests* condition by establishing different timeframes for sending written responses to the requestor based on the § 171.204(a) condition under which fulfilling the requested access, exchange, or use of EHI is infeasible. The proposed revision to § 171.204(b) would retain the requirement that actors communicate to requestors ''in writing the reason(s) why the request is infeasible'' that we finalized in the ONC Cures Act Final Rule (85 FR 25958, preamble discussion at 85 FR 25869). Under this proposed revision, the condition would also continue to provide actors wishing to avail themselves of the Infeasibility Exception with discretion to decide the appropriate level of detail to include in their written responses (see 85 FR 25869). In addition, we do not propose to specify the format of the written response or a specific delivery mechanism (such as paper mail versus email). Therefore, the proposed revision would retain the condition's existing flexibility specific to the format of the written response. As is the case under the current text of § 171.204(b), meeting the proposed modified § 171.204(b) would be required in conjunction with meeting a condition in § 171.204(a) in order for an actor's practice to satisfy the § 171.204 Infeasibility Exception.

We did not propose to modify the *responding to requests* condition in the HTI–1 Proposed Rule, but we received comments on the proposed rule indicating that ten business days may not allow actors sufficient time to engage with requestors and fully evaluate all factors relevant to meeting certain conditions in § 171.204(a). We discussed such comments in reference to the *manner exception exhausted* condition (§ 171.204(a)(4)) in the HTI–1 Final Rule preamble (89 FR 1387). We noted in the preamble that we did not propose changes to the ten-day timeframe in the HTI–1 Proposed Rule and did not finalize any changes to paragraph (b) of § 171.204 in the HTI–1 Final Rule, but we stated that we may consider those comments in relation to future regulatory action. The concern that ten business days may not allow actors sufficient time to engage with requestors and fully evaluate all factors relevant to meeting certain conditions in § 171.204(a) has also been raised by various actors in both written informal correspondence and real-time interactions since the publication of the ONC Cures Act Final Rule (85 FR 25642). We have also received inquiries from these same actors as to what constitutes a ''request'' for purposes of the Infeasibility Exception. These inquiries specific to § 171.204(b) have generally centered on how we would

[240] *See, e.g., https://www.healthit.gov/sites/default/files/appa7-1.pdf* (accessed Feb 26, 2024), and *http://www.healthinfolaw.org/comparative-analysis/medical-record-retention-required-health-care-providers-50-state-comparison* (accessed Feb 26, 2024).

[241] *See, e.g., https://www.jointcommission.org/standards/standard-faqs/home-care/leadership-ld/000001197/* (accessed Feb 26, 2024).

[242] *See, e.g., https://www.cms.gov/files/document/mln4840534-medical-record-maintenance-and-access-requirements.pdf* (accessed Feb 27, 2024), and *https://www.healthdatamanagement.com/articles/how-to-craft-an-effective-record-retention-policy* (accessed Feb 28, 2024).

determine when the ten-day ''clock'' for providing a written response begins.

We believe defining in regulation what constitutes a ''request'' or ''actionable request'' is unnecessary and could have more undesirable effects than desirable effects. We believe it would be difficult to define a single set of characteristics that every person's communication or conduct would need to satisfy before their communication to an actor, or other interaction with an actor or with health IT maintained or deployed by the actor, indicating the person seeks EHI access, exchange, or use would be considered a ''request'' for purposes of the information blocking regulations. Such specifications would increase complexity of the regulations and risk increasing rather than decreasing barriers to requestors' obtaining access, exchange, or use of EHI permitted under applicable law and, where applicable, consistent with patients' expressed individual preferences for privacy-protective restrictions beyond those required by law. In light of both experience over the four years since the ONC Cures Act Final Rule was published and the revisions that were finalized to the § 171.204(a) conditions in the HTI–1 Final Rule (89 FR 1436 through 1437, preamble discussion at 89 FR 1373 through 1387), we believe it remains appropriate to include as a condition of the Infeasibility Exception that the actor provide written responses within timeframes specified by the § 171.204(b) *responding to requests* condition. However, we have determined that the optimal timeframes to specify in § 171.204 going forward may vary based on the specific condition in § 171.204(a) that is satisfied.

We propose to retain, as new subparagraph (1) of § 171.204(b), the current § 171.204(b) requirement for a written response within ten business days of the actor receiving a request where the infeasibility of fulfilling requested access, exchange, or use of EHI satisfies the § 171.204(a)(1) *uncontrollable events* condition, § 171.204(a)(2) *segmentation* condition, or the § 171.204(a)(3) *third party seeking modification use* condition. We believe ten business days should be adequate time for an actor to recognize that a request that the actor has received, and that the actor might otherwise be able to fulfill, is not feasible in specific circumstances where an uncontrollable event has adversely impacted the actor's ability to fulfill the requested access, exchange, or use of EHI. Ten business days should also be sufficient for an actor to recognize that they cannot fulfill a request for EHI access, exchange, or use for reasons consistent with § 171.204(a)(2) *segmentation* condition or where a third party is seeking modification use in circumstances where § 171.204(a)(3) applies. However, we propose to revise the wording of the requirement from ''receipt of'' to ''the actor receiving'' to address what we believe some actors may experience as uncertainty regarding when one would start counting the ten business days in circumstances where fulfilling a request is infeasible for reasons consistent with § 171.204(a)(1).

We recognize that there is significant variation in how people make requests and for what purposes, as well as the manners in which they seek to achieve access, exchange, or use of EHI. We also recognize that mechanisms and workflows for receiving and reviewing requests may vary, even within a single actor's operations, based on characteristics of the request. For example, fulfillment of patient requests for EHI access, exchange, or use that can be received and supported automatically via a cloud-based patient portal unaffected by a particular uncontrollable event would continue to be feasible even while the impact of an uncontrollable event on the actor's systems or operational status has rendered the actor unable to receive other requests from, for example, payers or health care providers.

An uncontrollable event's impact on a particular actor's systems or operational status may render it infeasible for the actor to receive some requests until a time when restoration or recovery efforts have progressed far enough that the actor's staff are able to access and use the actor's systems. For example, for some types of request and actor workflows, it may be necessary that: (1) application(s) involved in receiving and responding to requests for EHI access, exchange, and use are operational; and (2) appropriate staff are able to safely and securely log into and use the application(s). Once those two things are true again following an uncontrollable event, we would expect the actor's staff to resume receiving and appropriately dispositioning requests. By revising the wording to focus explicitly on the actor receiving the request, we hope the proposed revised wording will make it easier for actors to consider the distinction between requests that can be received and processed using only automated means and requests that require a human to do something—such as log into a system or obtain and open a piece of paper mail—in order for the actor to, in fact, receive the request.

Similarly, we believe revising the wording to focus on the actor receiving the request clarifies when the ten-day clock starts in scenarios where third parties seek modification use. From the point the actor receives the request, we believe ten business days is sufficient time for an actor to both determine and respond in writing to the requestor that the request is infeasible consistent with § 171.204(a)(3).

In this proposed rule, we propose to define ''business day'' or ''business days'' in § 170.102 for purposes of the ONC Health IT Certification Program. For preamble discussion of this proposed definition of ''business day'' or ''business days,'' please see section III.D.1 of this proposed rule. We propose to adopt this same definition in § 171.102 for purposes of 45 CFR part 171. This proposal that is specific to the definition of ''business day'' or ''business days'' for purposes of 45 CFR part 171 is aligned with but is independent of the proposal to adopt the proposed definition of ''business day'' or ''business days'' discussed in section III.D.1 of this proposed rule for purposes of 45 CFR part 170. Therefore, commenters should be aware that we could choose to adopt the full proposed definition in § 171.102, instead of a cross-reference to § 170.102, for purposes of 45 CFR part 171 if we do not also adopt the definition for purposes of 45 CFR part 170. We welcome comment on this proposal specific to adoption of the definition (discussed in section III.D.1 and shown in the proposed revisions to § 170.102 in this proposed rule) for purposes of 45 CFR part 171 in general and as it would apply to the *responding to requests* condition of the Infeasibility Exception (§ 171.204(b)).

A proposed new subparagraph (2) in the proposed revised § 171.204(b) would apply where fulfilling a request is infeasible under the *manner exception exhausted* condition (§ 171.204(a)(4)) or the *infeasible under the circumstances* condition (§ 171.204(a)(5)). Under this proposal, the ten-day clock would start after the actor determines, without unnecessary delay and based on a reasonable assessment of the facts, that the requested access, exchange, or use of EHI cannot be provided consistent with § 171.301 or that fulfilling the request is infeasible under the circumstances. We expect that any actors who find themselves attempting to fulfill a request consistent with § 171.301 will be aware that the attempt to fulfill the request could instead result in infeasibility consistent with the § 171.204(a)(4) *manner exception exhausted* condition. Therefore, we

expect that any such actor would, in good faith and without unnecessary delay, interact with the requestor to ascertain the scope and requested manner of EHI access, exchange, or use and negotiate any necessary fees and licensing consistent with § 171.301. Similarly, we expect that any actor who embarks on the consideration of factors in paragraph (i) of the *infeasible under the circumstances* condition (§ 171.204(a)(5)) will be aware that their consideration of these factors could lead to either a successful fulfilment of requested access, exchange, or use of EHI or a determination that complying with the request would be infeasible under the circumstances. Therefore, we expect the actor would, in good faith and without unnecessary delay, interact with the requestor to ascertain the scope and requested manner of EHI access, exchange, or use and obtain any additional information needed to support the actor's prompt consideration of the § 171.204(a)(5) factors.

We welcome comments on this proposal.

We also propose in the alternative to enhance the revisions to § 171.204(b) by adopting either or both of the following requirements specific to the circumstances where § 171.204(b)(2) would be applicable.

- We propose an additional requirement for a specific maximum timeframe for the § 171.204(b)(2)(i) determination of infeasibility related to § 171.301. Under this additional requirement, the maximum timeframe would be one of the following: three, five, ten, twenty, or thirty business days.
- We propose an additional requirement that for § 171.204(b)(2) to be met, the determination and communication of infeasibility (for reasons consistent with § 171.204(a)(4) or (5)) would have to be made within the timeframe permitted under 45 CFR 164.524 for providing access to PHI where a request for EHI access, exchange, or use is one that implicates the HIPAA Privacy Rule's provisions for individual access to PHI (45 CFR 164.524) in addition to implicating the information blocking regulations in 45 CFR part 171.

We welcome comments on the possible additional requirements proposed above.

Please note, if ONC adopts the alternative proposal above that specifically references 45 CFR 164.524 for purposes of § 171.204(b)(2), we intend to apply the timeframes required under that section when a request for individual EHI access, exchange, or use is received by the actor. Thus, under the alternative proposal's requirements that would limit maximum available response time under the *responding to requests* condition where the request for EHI implicates 45 CFR 164.524(a)(1) the timeframe would be limited to the timeframe required under 45 CFR 164.524. We also highlight for readers' awareness that HHS has proposed to revise 45 CFR 164.524(b)(2) to shorten the timeframes allowed to respond to individual requests for access to PHI (see 86 FR 6459 through 6460 and 86 FR 6535). In the event that changes to the 45 CFR 164.524 timeframes were to be finalized in a future HIPAA rule, the shorter timeframes would (upon becoming effective) apply to the alternative proposed additional requirement for responding to requestors where paragraph (b)(2) of the Infeasibility Exception would apply.

3. Protecting Care Access Exception

a. Background and Purpose

As we explained in the ONC Cures Act Final Rule, the information blocking provision in PHSA section 3022 was enacted in response to concerns about practices that ''unreasonably limit the availability and use of electronic health information (EHI) for authorized and permitted purposes'' because such practices ''undermine public and private sector investments in the nation's health IT infrastructure, and frustrate efforts to use modern technologies to improve healthcare quality and efficiency, accelerate research and innovation, and provide greater value and choice to healthcare consumers'' (85 FR 25790). We also noted in the ONC Cures Act Final Rule that research suggests that information blocking practices ''weaken competition among health care providers by limiting patient mobility'' and ''unnecessarily impede the flow of EHI or its use to improve health and the delivery of care'' (85 FR 25791). As required by section 3022(a)(3) of the PHSA, we recognized that certain reasonable and necessary activities that could otherwise meet the definition of information blocking should not be considered information blocking, and therefore, established the initial eight ''exceptions'' to the definition of information blocking (see 45 CFR 171 Subpart B and C; a ninth exception was established by the HTI–1 Final Rule in Subpart D). Each reasonable and necessary activity identified as an exception to the information blocking definition does not constitute information blocking for purposes of section 3022(a)(1) of the PHSA if the conditions of the exception are met (85 FR 25649).

Since the first eight regulatory exceptions to the information blocking definition were finalized in 2020 (see ONC Cures Act Final Rule, 85 FR 25642), the legal landscape has changed significantly for many patients seeking, and for health care providers providing, reproductive health care. In the wake of the decision in *Dobbs* v. *Jackson Women's Health Organization,* 597 U.S. 215 (2022) decision, some States have newly enacted or are newly enforcing restrictions on access to reproductive health care. Uncertainties and other concerns that people who seek reproductive health care and people who provide or facilitate that care have about the legal landscape in the wake of the Supreme Court's ruling—and subsequent State restrictions on reproductive health care—have had far-reaching implications for health care beyond access to abortion. This changing legal landscape increases the likelihood that a patient's EHI may be disclosed in ways that erode trust in health care providers and the health care system, ultimately chilling an individual's willingness to seek, or other persons' willingness to provide or facilitate, lawful health care as well as individuals' willingness to provide full information to their health care providers.

As a practical matter, a person's ability to access care of any kind depends on a variety of factors including whether the care is available. For health care to be available, licensed health care professionals and health care facilities must be willing to provide it—and people other than the licensed health care professionals must be willing to take on various roles essential to delivering care in this modern, technology-enabled environment. Also, patients' access to care may rely in some part on services or supports from other persons, such as a spouse or partner.

In the current environment, various jurisdictions might enact legislation or attempt to enforce law that purports to authorize administrative, civil, or criminal legal action against persons who engage in reproductive health care that is required or authorized by Federal law or that is permitted by the law of the jurisdiction where the care is provided. Fear of being investigated or of having to defend themselves against potential legal liability under such laws, even where the health care provider or other person has reasonable confidence the defense will be successful, may impact people's willingness to provide or assist in reproductive health care that is lawful under the circumstances in which such health care is provided.

On April 26, 2024, the HHS Office for Civil Rights (OCR) issued the ''HIPAA Privacy Rule to Support Reproductive Health Care Privacy'' final rule (89 FR 32976) (2024 HIPAA Privacy Rule) to adopt a prohibition on the use or disclosure of PHI by an entity regulated under the HIPAA Privacy Rule, in certain circumstances, for the following purposes:

- To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.
- To identify any person for any purpose described above.

As noted in the National Coordinator's ONC Health IT blog post titled ''Supporting Information Privacy for Patients, Now and Always: Four Reminders of How HHS Information Blocking Regulations Recognize Privacy Rules,'' on and after the 2024 HIPAA Privacy Rule's effective date, a HIPAA covered entity's or business associate's practice of refusing to make a use or disclosure of PHI that is prohibited under that rule is excluded from the information blocking definition (45 CFR 171.103) because that refusal is required by law. Therefore, the practice does not need to be covered by any information blocking exception because it is not considered information blocking to begin with.

The 2024 HIPAA Privacy Rule also establishes a requirement for HIPAA covered entities and business associates to obtain attestations prior to using or disclosing PHI potentially related to reproductive health care for certain purposes (see 45 CFR 164.509 at 89 FR 33063). The Precondition Not Satisfied (45 CFR 171.202(b)) sub-exception of the information blocking Privacy Exception outlines a framework actors can follow so that the actors' practices of not fulfilling requests to access, exchange, or use EHI would not be considered information blocking when a precondition of applicable law has not been satisfied. By meeting the Precondition Not Satisfied sub-exception's requirements, the actor can have confidence that their practices of not sharing EHI because they have not obtained the required attestation will not be considered information blocking.

The 2024 HIPAA Privacy Rule's new protections do not prohibit use or disclosure of PHI for various purposes other than those specified in 45 CFR 164.502(a)(5)(iii), though the protections include additional preconditions or limitations on disclosures for certain purposes (for more information, please see the 2024 HIPAA Privacy Rule (89 FR 32976) and consider visiting the HHS.gov Health Information Privacy section's HIPAA and Reproductive Health page: *https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/index.html*). The 2024 HIPAA Privacy Rule does not require a HIPAA covered entity or business associate to obtain the attestations specified in 45 CFR 164.509 before disclosing PHI (including PHI potentially related to reproductive health care) for permissible purposes other than those specified in 45 CFR 164.512(d), (e), (f), or (g)(1). For example, the HIPAA Privacy Rule continues to provide for uses and disclosures of PHI for treatment, payment or health care operations purposes (see 45 CFR 164.506) that do not meet any of the prohibitions set out in 45 CFR 164.524(a)(5)(iii). Thus, an actor choosing to deny requests for access, exchange, or use of EHI for a purpose permitted under HIPAA is not making a denial that is ''required by law'' specifically under HIPAA. As a result, the information blocking definition could be implicated unless another applicable law requires the denial or a regulatory exception applies. Similarly, an actor conditioning fulfilment of such requests on preconditions that an actor chooses to set (such as that the requestor provides an attestation that is not required by any privacy law that applies in the circumstances) could implicate the information blocking definition unless an exception applies to that practice.

It may be helpful to pause here for a brief review of how the information blocking regulations, which are based on statutory authority separate from HIPAA, operate (independently of regulations promulgated under HIPAA). This background information may help readers understand how and why an actor may be concerned about potentially implicating the information blocking definition (and penalties or disincentives for information blocking authorized by the information blocking statute) if the actor engages in practices that the HIPAA Privacy Rule would require of a HIPAA covered entity or business associate when the actor is not required to comply with the HIPAA Privacy Rule.

First, information blocking regulations apply to health care providers, health IT developers of certified health IT, and health information networks (HIN) and health information exchanges (HIE), as each is defined in 45 CFR 171.102. Any individual or entity that meets one of these definitions is an ''actor'' and subject to the information blocking regulations in 45 CFR part 171, regardless of whether they are also a HIPAA covered entity (CE) or business associate (BA) as those terms are defined in 45 CFR 160.103. Second, for purposes of the information blocking regulations, the definition of ''EHI'' applies to information ''*regardless* of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103'' (§ 171.102, emphasis added). Therefore, it is possible for an information blocking actor that is not required to comply with the HIPAA Privacy Rule to have EHI that is not also PHI. It is also possible for an actor (such as a HIN/HIE) to not be a HIPAA covered entity itself and to exchange, maintain, or otherwise handle EHI on behalf of network participants that are not required to comply with the HIPAA Privacy Rule.

Where an actor that is not a HIPAA covered entity has EHI that is not maintained on behalf of a HIPAA covered entity, the actor may be concerned about potential information blocking consequences if the actor were to engage in a practice such as denying requests for access, exchange, or use of EHI that indicates or potentially relates to reproductive health care for purposes for which the 2024 HIPAA Privacy Rule would prohibit use or disclosure of PHI or would require an attestation as a precondition for permitting disclosure of PHI.

There is a sub-exception within the Privacy Exception currently codified in § 171.202(c) that is available to a health IT developer of certified health IT ''not covered by HIPAA.'' The sub-exception is available ''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'' (§ 171.202(c), please see § 171.202(c) for the requirements to meet the exception.) However, this exception represents a departure from our general approach of designing each information blocking exception to be available to all actors (regardless of whether they must comply with the HIPAA Privacy Rule). The § 171.202(c) sub-exception is also not available to actors who meet the § 171.102 definition of ''health care provider'' or ''HIN/HIE'' even if they are not required to comply with the HIPAA Privacy Rule. (We refer actors and other persons interested in learning more about how the information blocking regulations, and particularly the

exceptions, work in concert with the HIPAA Rules and other privacy laws to support health information privacy, to the discussion of this topic in the HTI–1 Final Rule at 89 FR 1351 through 1354.)

We have come to understand that some health care providers and other actors may have concerns about the risk of potential exposure to legal action flowing from the uses and disclosures of EHI indicating or (in the case of patient health concern(s) or history) potentially relating to reproductive health care that remains permissible under applicable law. For example, the HIPAA Privacy Rule permits a HIPAA covered entity to disclose an individual's PHI to a health care provider who is not a HIPAA covered entity for treatment activities. Once PHI is in the possession, custody, or control of an entity that is not regulated under the HIPAA Privacy Rule, the information is no longer protected by the HIPAA Privacy Rule.

Thus, the HIPAA Privacy Rule's strengthened protections for PHI would not preclude a health care provider (or other recipient of PHI for other permissible purposes) who is not a HIPAA covered entity or business associate from further disclosing individually identifiable health information to someone who might then use the information to potentially impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care (or any other care) that was lawful under the circumstances in which it was provided.

We reiterate that the information blocking statute is separate from the HIPAA statute and that the information blocking regulations operate both separately and differently from the HIPAA regulations. One point of such difference that is key to understanding why we propose a new ''Protecting Care Access Exception'' (§ 171.206) is that a HIPAA covered entity or business associate is not required by the HIPAA Privacy Rule to make a use or disclosure that the rule merely permits. (The HIPAA Privacy Rule does require certain uses and disclosures of PHI but merely permit various other uses and disclosures.) Persons subject to the information blocking regulations, however, could implicate the information blocking definition if they ''interfere with'' any access, exchange, or use of EHI except as required by law or covered by an exception. It is the implication of the ''information blocking'' definition (and the potential to incur penalties or disincentives for engaging in information blocking) that would cause an actor to be concerned about, for instance, refusing to disclose EHI indicating reproductive health care for permissible purposes to an entity not required to comply with the HIPAA Privacy Rule and whom the actor has reason to believe does not safeguard the privacy or security of individuals' health information in compliance with the same standards as would be required of a HIPAA covered entity or business associate.

In a variety of situations where a patient or an actor may be concerned that an access, exchange, or use of EHI may implicate any person's physical safety interests or the individual's privacy interests, other exceptions (such as the Preventing Harm Exception in § 171.201 or three of the four sub-exceptions of the Privacy Exception in § 171.202) are available to any actor who wants to engage in practices that are likely to interfere with EHI access, exchange, or use consistent with the conditions of the applicable exception.

Currently, however, there are no exceptions in 45 CFR part 171 that are designed to accommodate concerns an actor may have about a patient's, health care provider's, or other person's risk of potential exposure to legal action (investigation, action in court, or imposition of liability) that could arise from [243] the access, exchange, or use for permissible purposes specific EHI (that is, one or more data points)that indicates reproductive health care was sought, obtained, provided, or facilitated. None of the current exceptions are designed to accommodate similar concerns an actor may have about risk of patients' potential exposure to legal action that could arise from the sharing for permissible purposes of EHI that indicates health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated.[244] Thus, where preconditions (under the HIPAA Privacy Rule or other applicable law—or both, where applicable) to the provision of access, exchange, or use of EHI have been met, and another exception (such as Privacy (§ 171.202) or Preventing Harm (§ 171.201)) does not apply, attempts to limit the disclosure of EHI for the purposes addressed in the *patient protection* or *care access* condition of the proposed Protecting Care Access Exception (§ 171.206(b) or (c)) could currently constitute information blocking. (An actor's practice will only meet the statutory or regulatory definition of information blocking if it meets all of the definition's elements, including the knowledge standard applicable to the actor engaged in the practice.)

Even for actors to whom the HIPAA Privacy Rule does not apply, other laws (Federal, State, or Tribal) may apply preconditions that must be satisfied in order for EHI to be shared without violating these laws. For any actor, compliance with such other applicable law does not implicate the information blocking definition, as ONC has discussed in the HTI–1 Final Rule preamble (see 89 FR 1351 through 1354) and in information resources available on ONC's official website (*HealthIT.gov*). However, where the preconditions under such other applicable law are met, any practice by an actor that is likely to interfere with access, exchange, or use of EHI could implicate the information blocking definition (§ 171.103) unless the actor's practice is covered by an exception set forth in 45 CFR part 171.

The proposed new Protecting Care Access Exception (§ 171.206) would be available to any actor, regardless of whether the actor is also a HIPAA covered entity or business associate. The proposed exception would apply regardless of whether another exception could also apply to an actor's practice(s) in relevant scenarios. Other exceptions would continue to be available in circumstances where the conditions of the Protecting Care Access cannot be met but the other exception(s) can be met. Each information blocking exception and each provision of each exception is designed to stand independent of any and every other exception unless any specific provision of an exception might explicitly reference another exception (even then the dependency is limited to the exact provision or function of such provision that relies upon the cross-reference).

Thus, the proposed Protecting Care Access Exception would also operate independently of any provision of any other exception in part 171 and any provision in 45 CFR 171 that does not reference it. It is our intent that if any provision in § 171.206 were, if or when finalized, held to be invalid or unenforceable facially, or as applied to

[243] For purposes of this discussion and of the proposed Protecting Care Access Exception, a risk need not be one that is certain to occur, or that is likely to occur immediately following, an access, exchange, or use of EHI in order to be one that could arise from the access, exchange, or use.

[244] In this preamble, we at some points use for brevity and readability ''potentially related to reproductive health care'' as shorthand for EHI that shows or would carry a substantial risk of supporting an inference that (as described in proposed § 171.206(b)(1)(iii)) the patient has health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated.

any person, plaintiff, or stayed pending further judicial or agency action, such provision shall be severable from other provisions of § 171.206 that do not rely upon it and from any other provision codified in 45 CFR part 171 that does not explicitly reference § 171.206 even if such provisions were to be established or modified through this same rulemaking action.

A patient's ability to access care can be adversely affected when a provider believes they could be exposed to legal action based on the mere fact that care is provided. Given the demonstrated chilling effect of some States' laws on the availability of medically appropriate care, it is reasonable and necessary for actors to mitigate risks of potential exposure of health care professionals and other persons who provide or facilitate, as well as those who seek or obtain, reproductive health care that is lawful under the circumstances in which the care is provided to legal action based on the mere fact that such care was sought, obtained, provided, or facilitated. Thus, a new exception is needed to address actors' concerns about potentially implicating the information blocking definition (§ 171.103) if they choose not to share applicable EHI in the circumstances where the Protecting Care Access Exception (§ 171.206) would apply. This new proposed exception (§ 171.206) is important in order to ensure health care providers do not feel the need to adopt paper or hybrid recordkeeping methods in place of fully electronic, interoperable formats. Thus, we believe it is reasonable and necessary for an actor to restrict access, exchange, or use of specific EHI that indicates or (under § 171.206(b)) is potentially related to reproductive health care so that health care providers continue to use modern, interoperable health IT that better promotes patient safety than would paper or hybrid recordkeeping methods. Restricting EHI sharing under the conditions of the proposed new Protecting Care Access Exception (§ 171.206) is also necessary to preserve and promote public trust in health care professionals, health care, and the health information infrastructure.

We propose the Protecting Care Access Exception to address actors' concerns about potentially implicating the information blocking definition if they choose not to share EHI in an EHI sharing scenario that an actor believes in good faith could risk exposing a patient, provider, or facilitator of lawful reproductive health care to potential legal action based on what care was sought, obtained, provided, facilitated, or (specific to the *patient protection* condition) is often sought, obtained, or medically indicated for the patient's health condition(s) or history.

The HIPAA Privacy Rule does not prohibit the use or disclosure of PHI that indicates or is potentially related to ''reproductive health care'' as it is now defined in 45 CFR 160.103 (see 89 FR 32976 for definition effective June 25, 2024; see also 89 FR 33005 through 33007 for the 2024 HIPAA Privacy Rule's preamble discussion of that definition) where the use or disclosure is not for a purpose described at 45 CFR 164.502(a)(5)(iii) and where the use or disclosure is otherwise required or permitted by the HIPAA Privacy Rule. Therefore, within the information blocking regulations, the proposed new Protecting Care Access Exception is needed where an information blocking actor (whether or not that actor is required to comply with the HIPAA Privacy Rule) is concerned about the risk of potential exposure to legal action (as we propose in § 171.206(e) to define ''legal action'') flowing from an access, exchange, or use of such EHI for a permissible purpose.

We recognize that no information blocking exception can address all of the concerns a person may have about potential legal action for the mere act of seeking, obtaining, providing, or facilitating reproductive health care. However, to the extent such concerns may be mitigated by actors' withholding relevant EHI from access, exchange, or use that all other applicable law would permit and where no other existing information blocking exception applies, we believe such withholding of EHI is reasonable and necessary. We are concerned that actors' uncertainty about whether such withholding of EHI could implicate the information blocking definition could prevent actors from withholding EHI unless an exception applies. Thus, we believe the Protecting Care Access Exception is needed to address actors' concerns specific to information blocking related to the risk of providers changing or limiting what care they are willing to offer (such as when a professional changes practice specialty or a hospital closes a service or department).

When providers limit what care they are willing to offer or what new patients they are willing to accept, it may be more difficult for those who seek care to get access to care they need. When patients' needs are not being met, they lose trust in the health care system and in their physicians. Trust in one's own physician, in general, correlates with better care satisfaction and outcomes. This could also be true of other types of health care providers. Thus, we believe that addressing actors' uncertainty specific to information blocking with the proposed Protecting Care Access Exception would promote better patient satisfaction and health outcomes as well as continued development, public trust in, and effective nationwide use of health information technology infrastructure to improve health and care.

Moreover, actors' uncertainty about the potential information blocking implications of not sharing all of the EHI that applicable laws would permit them to share could undermine health care professionals' (and other health care providers') confidence in their ability to protect the privacy and confidentiality of their patients' EHI. Such a lack of confidence on the part of health care providers can in turn erode a patient's trust.

Patient trust in physician confidentiality and competence is associated with patients being less likely to withhold information from doctors and more likely to agree it is important for health care providers to share information with each other. Thus, actors' narrowly tailored restrictions on (otherwise lawful) sharing of specific EHI in the circumstances addressed by the proposed exception in § 171.206 would be reasonable and necessary to preserve patient trust in the health IT infrastructure and information sharing, not just to protect the availability and safety of care and to promote better care outcomes.

One of the goals of the information blocking exceptions is ''to accommodate practices that, while they may inhibit access, exchange, or use of EHI, are reasonable and necessary to advance other compelling policy interests . . .'' including ''[p]romoting public confidence in the health IT infrastructure by supporting the privacy and security of EHI and protecting patient safety,'' as we explained in the ONC Cures Act Final Rule (85 FR 25791). In the absence of an information blocking exception applicable to risks of legal actions that actors believe could arise from the sharing EHI for permissible purposes (for instance, with entities not required to comply with the HIPAA Privacy Rule), we are concerned actors may be unwilling to engage in these practices that—for example—advance public confidence in health IT infrastructure and protect patient safety.

If actors are unwilling to engage in such practices, health care providers may convey to patients an inability to withhold EHI even when they believe withholding the EHI could mitigate the potential risks cognizable under the

Protecting Care Access Exception. If patients are aware that health care providers believe that they are unable to avoid sharing EHI to mitigate risks of potentially exposing care providers, recipients, or facilitators to legal action then patients may be less willing to be candid with their providers about their health history, conditions, or other information relevant to the patient's care. Without that candor, health care providers may be unable to provide care that will best meet the patient's needs.

In addition, a care provider's lack of confidence or competence in their ability to adequately safeguard the privacy of information that care recipients share with them could erode the mutual trust that contributes to better care outcomes by promoting more effective relationships between care providers (including clinicians) and the individuals receiving care.

In the absence of an exception applicable to practices that the proposed Protecting Care Access Exception would cover, we are concerned that health IT developers of certified health IT and HINs/HIEs may be unwilling to take the actions necessary to address their own, or their customer health care provider's, good faith belief that particular sharing of specific EHI could create the risk of potential exposure of a health care provider (or persons seeking, obtaining, providing, or facilitating care) to legal action regarding health care items and services that are lawful under the circumstances in which such health care is provided. Thus, health care providers in these situations may believe they are faced with a choice between changing what care they offer (such as when a hospital closes a department) or switching at least some portions of their clinical records from electronic to paper formats specifically to avoid concerns that they may be engaged in information blocking.

For health care professionals in reproductive health care specialties or whose practice necessarily includes patients who need reproductive health care, a partial or complete switch to paper-based recordkeeping for that care may seem like their only option. (Because the information blocking definition references ''electronic health information'' rather than all ''protected health information,'' the information blocking regulations do not apply to health information maintained only in paper format.)

A reversal to paper-based methods of keeping even a relatively small portion of the records currently managed using modern health IT would have an adverse effect on interoperability and on the development of a nationwide health IT infrastructure that does the things identified in section 3001(b) of the PHSA. Thus, such a reversal to paper-based recordkeeping methods would impede the goals of promoting public confidence in the electronic health information infrastructure and of advancing patient safety through the use of interoperable health IT and EHI. For example, information kept only on paper is not available to support tools that help clinicians avoid adverse drug events by automatically checking for potential drug-drug or drug-allergy interactions.

For the reasons discussed above, we believe actors' practices of limiting EHI sharing under the conditions of the proposed § 171.206 exception are reasonable and necessary to preserve advances in digitization, interoperability, and public confidence in the nationwide health information technology infrastructure. Actors selectively withholding EHI that indicates or is potentially related to reproductive health care (as applicable) under the conditions of the proposed § 171.206 would also promote patient safety and improve outcomes by fostering trust between care providers and recipients. Maintaining advances and trust in the health information technology infrastructure fosters better care by continuing to make information available to more care providers and care recipients when and where the information can help them choose the right care for each patient (care recipient). Use of interoperable, electronic health IT and exchange of EHI also enables providers to use decision support tools, such as drug-drug interaction alerting, and to deliver better care.

The proposed Protecting Care Access Exception (§ 171.206) could apply in some circumstances where another exception (such as Preventing Harm (§ 171.201) or Privacy (§ 171.202)) would or could also apply. The proposed new exception is, however, intended to stand alone and independent of other. The proposed Protecting Care Access Exception would not affect if, how, or when any provision of any exception that does not explicitly reference § 171.206 applies to an actor's practice, or how any such provision operates. Moreover, where facts and circumstances were such that an actor could choose to shape their practice in withholding EHI to satisfy either the Protecting Care Access Exception (if finalized) or another exception, the actor would have discretion to choose which exception they wish to satisfy. An actor's practice in such situation(s) would not need to satisfy both exceptions in order for the practice to not be considered information blocking.

One of the existing information blocking exceptions applicable in some circumstances where the proposed Protecting Care Access Exception could also apply is the Privacy Exception. Of particular relevance to actors' confidence that they will not be ''information blocking'' if they withhold EHI based on the individual's preference that their EHI be closely held is the Privacy Exception's sub-exception ''respecting an individual's request not to share information'' (§ 171.202(e)).

This Privacy sub-exception is applicable where an actor agrees to honor an individual's request not to share their EHI even where it is permissible to share under all applicable law. We are proposing to strengthen and simplify that § 171.202(e) Privacy sub-exception as discussed in section IV.B.1.c of this proposed rule. The § 171.202(e) sub-exception offers actors certainty that they can, if they so choose, honor an individual's preference for restrictions on the sharing of EHI about the individual without subjecting the actor to an information blocking penalty or disincentive for not sharing such EHI. However, while the § 171.202(e) sub-exception does not rest on why the individual may prefer that some or all of their EHI not be shared, the § 171.202(e) sub-exception only applies to scenarios where the individual requests the restrictions. There may be circumstances where an individual does not request the restriction, but when it would be reasonable and necessary for actors to interfere with access, exchange, or use of EHI for the purpose of addressing individuals' (let alone providers' and others') risk of potential exposure to legal action that could discourage availability, access, and choice of medically appropriate reproductive health care.

We believe it would be burdensome to individuals, in the constantly changing legal landscape, to rely exclusively on them to make or update requests for restrictions on their EHI that indicates or is potentially related to reproductive health care. In such a complex and uncertain environment, any individual may experience difficulty in making timely requests for such restrictions. Moreover, some individuals may not have the resources—such as affordable, secure access to the internet—to update their providers on their information sharing preferences outside of the occasions that they interact with these providers to obtain health care. Thus, individuals may not be able to request

restrictions soon enough, or that are broad enough, to protect themselves or others from potential legal liability based on what care they have received.

An individual's request for restrictions on sharing their EHI is specific and limited to that individual's EHI, and (depending on what the individual chooses to request) may be specific to identified requestors of the individual's EHI. Thus, it is not as efficient for actors to implement such individual restrictions as it would be to implement restrictions based on an organizational policy that consistently addresses a concern common to sharing any individuals' EHI in a particular access, exchange, or use scenario—such as the actor's good faith belief that there is a concern regarding the risk of potential exposure to legal action that could be created or increased by propagating to a recipient not required to comply with the HIPAA Privacy Rule the specific EHI within a patient's record that indicates the receipt of reproductive health care.

For these reasons, we believe that health care providers and other actors must have available to them an information blocking exception designed to apply to practices that the actor believes could help to avoid creating—through sharing of EHI indicating or potentially related to reproductive health care in relevant scenarios—a risk of potential exposure to legal action based on the mere fact that lawful reproductive health care was sought, obtained, provided, or facilitated (or where the proposed *patient protection* condition would apply, because the EHI indicates patient health history or condition(s) for which reproductive health care is often sought, obtained, or medically indicated).

When an actor has a belief consistent with the proposed § 171.206(a)(1) belief requirement, we believe an exception should be available that is designed to cover practices likely to interfere with access, exchange, or use of EHI under certain conditions.[245] Therefore, we propose in § 171.206 a new Protecting Care Access Exception from the information blocking definition. When its conditions are met, the new exception would cover an actor's practices that interfere with access, exchange or use of EHI in order to reduce potential exposure of applicable persons to legal action (as defined in the exception). For the proposed exception to apply, the potential exposure to legal action that the actor believes could be created must be one that would arise from the fact that reproductive health care was (or may have been) sought, obtained, provided, or facilitated rather than because the care provided was (or is alleged to have been) clinically inappropriate or otherwise substandard.

We note here that the statutory authority in PHSA section 3022(a)(3) is to ''identify reasonable and necessary activities that do not constitute information blocking.'' Thus, practices that meet the applicable conditions of the proposed new Protecting Care Access Exception (§ 171.206) would not be considered information blocking (as defined in PHSA section 3022(a)(1) and 45 CFR 171.103), and, therefore, actors would not be subject to civil monetary penalties or disincentives under HHS information blocking regulations based specifically on those practices.

However, as is the case with exceptions already established in 45 CFR part 171, the proposed exception would not override an actor's obligation to comply with a mandate contained in law that requires disclosures that are enforceable in a court of law. For example, the proposed exception would not invalidate otherwise valid court-ordered disclosures, or disclosures (for example, infectious disease, or child or elder abuse case reports) mandated by a Federal, State, or Tribal law with which an actor is required to comply in relevant circumstances. The exception is also not intended to justify an attempt to limit the legally required production of (otherwise discoverable) EHI in a civil, criminal, or administrative action that is brought in the jurisdiction where a health care provider provided health care that a patient (or their representative) alleges was negligent, defective, substandard, or otherwise tortious. Similarly, the exception would not apply to, and is not intended to justify, attempts to avoid disclosing information where the actor's belief is that the information could be useful to a legal action against the actor or other person specific to alleged violations of Federal or other law against conduct other than merely seeking, receiving, providing, or facilitating reproductive health care. One example of such other conduct would be a physical assault of any natural person, even if the assault occurred in a health care setting.[246]

We emphasize that if the proposed Protecting Care Access Exception were to be finalized, actors would continue to be subject to other Federal laws, and to State and Tribal laws. This is consistent with how the information blocking exceptions in place today operate in harmony with, but separate from, requirements of other statutes and regulations—including, among others, the HIPAA Privacy Rule's individual right of access (45 CFR 164.524).

For example, an actor that is also a HIPAA covered entity may receive a request from an individual for access to EHI of which the individual is the subject, in a manner (form and format) specified by the individual. If the actor is technically unable to fulfill the request, or if the individual and actor cannot come to agreement on terms to fulfill the request in the manner requested or an alternative manner consistent with § 171.301(b), the actor may be able to satisfy the Infeasibility Exception by meeting that exception's manner exception exhausted (§ 171.204)(a)(4)) and the responding to requests (§ 171.204(b)) conditions. By satisfying the Infeasibility Exception, the actor's practice of failing to fulfill the request for access, exchange, or use of EHI will not be considered information blocking. However, the actor in this example is a HIPAA covered entity and, therefore, must comply with the HIPAA Privacy Rule's right of access at 45 CFR 164.524, even though the actor's practices in failing to provide access, exchange, or use of EHI met the requirements to be covered by the Infeasibility Exception (§ 171.204) for purposes of the information blocking regulations.

Consistent with our approach to establishing the initial eight information blocking exceptions, the conditions of the proposed Protecting Care Access Exception (§ 171.206) are intended to limit its application to the reasonable and necessary activities enumerated within the exception. Therefore, our proposed Protecting Care Access Exception would (for purposes of the information blocking definition in § 171.103) cover an actor's practice that is implemented to reduce potential exposure of persons meeting the § 171.202(a)(2)(i) or (ii) definition of ''individual,'' other persons referenced or identifiable from EHI as having sought or obtained reproductive health care, health care providers, or persons who facilitate access to or delivery of health care to potential threats of legal action based on the decision to seek, obtain, provide, or facilitate reproductive health care, or on patient health information potentially related to

[245] These conditions would be those specified in the exception.

[246] The definition of ''person'' for purposes of 45 CFR part 171 is codified in § 171.102 and is, by cross-reference to 45 CFR 160.103, the same definition used for purposes of the HIPAA Privacy Rule (45 CFR part 160 and subpart E of 45 CFR part 164). The § 160.103 definition of ''person'' clarifies the meaning of ''natural person'' within it. We use ''natural person'' with that same meaning in proposed § 171.206(b)(3) and throughout this discussion of proposed § 171.206.

reproductive health care, subject to the exception's conditions.

Because we propose in this rule an exception that relies on the ''reproductive health care'' definition in 45 CFR 160.103, we also propose to add to § 171.102 the following: ''Reproductive health care is defined as it is in 45 CFR 160.103.'' We refer readers to 45 CFR 160.103or 89 FR 32976 for that definition, which became effective for purposes of the HIPAA Privacy Rule on June 25, 2024.[247] We refer readers interested in learning more about this definition to 89 FR 33005 through 33007 for the 2024 HIPAA Privacy Rule's preamble discussion of the ''reproductive health care'' definition.

For this exception to apply to an actor's practice that is likely to interfere with EHI access, exchange, or use, the practice would have to satisfy the *threshold* condition in the proposed paragraph (a), and at least one of the other conditions (proposed paragraph (b) or (c)) of the proposed exception. These conditions are discussed in detail below. An actor's practice could satisfy both conditions (b) and (c) at the same time, but the minimum requirement for the exception to apply would be that the practice satisfy at least one of these two conditions in complement to the *threshold* condition in paragraph (a).

b. Threshold Condition and Structure of Exception

The § 171.206(a) *threshold* condition's requirements must be satisfied in order for any practice to be covered by the proposed exception. To meet the condition's subparagraph (a)(1) belief requirement, the practice must be undertaken based on a good faith belief that:

- the person(s) seeking, obtaining, providing, or facilitating reproductive health care are at risk of being potentially exposed to legal action that could arise as a consequence of particular access, exchange or use of specific EHI; and
- the practice could reduce that risk.

To satisfy the belief requirement (§ 171.206(a)(1)), the actor's belief need not be accurate, but must be held in good faith. We are also considering, and seek comment, on whether actors, patients, or other interested parties may view ''good faith belief'' as a standard that is unnecessarily stringent or that could make the Protecting Care Access Exception difficult for small actors with limited resources, such as small and safety net health care providers, to confidently use. We are also interested in any thoughts or concerns commenters may have about the ''good faith belief'' standard and how such concerns could be mitigated by the addition to § 171.206 of a presumption that an actor's belief is held in good faith.

To ensure we have flexibility to do so in case we determine it is the optimal approach after considering public comments on the proposed Protecting Care Access Exception, we propose in the alternative to do one or both of the following: (1) set ''belief'' or ''honest belief'' rather than ''good faith belief'' as the substantive standard in § 171.206(a); or (2) add to § 171.206 a provision for HHS to presume an actor's belief met the standard unless we have or find evidence that the actor's belief did not meet the standard at all relevant times (relevant times are those when the actor engaged in practices for which the actor seeks application of the exception).

Like ''good faith belief,'' ''belief'' or ''honest belief'' would be a subjective rather than an objective standard. Under either alternative, the actor's belief would not be required to be accurate but could not be falsely claimed. Unlike ''good faith,'' neither ''belief'' nor ''honest belief'' is a particularly long established and widely used legal standard. However, we are interested in actors' and other commenters' views on whether these standards might help to reduce potential misunderstanding of § 171.206(a) and what would be necessary for an actor to meet the proposed ''good faith belief'' standard.

Where an actor is a business associate of another actor or otherwise maintains EHI on behalf of another actor, this exception would (where its requirements are otherwise fully satisfied) apply to practices implemented by the actor who maintains EHI based on the good faith belief and organizational policy or case-by-case determinations of the actor on whose behalf relevant EHI is maintained. We propose in the alternative to require that each actor rely only on their own good faith belief in order to implement practices covered by the Protecting Care Access Exception, including when an actor maintains EHI on behalf of other actor(s) or any other person(s). We welcome comment on both of these approaches to the good faith belief requirement where the actor implementing the practice is doing so in relation to EHI maintained on behalf of another actor.

As discussed in section IV.B.3.e, we propose to define ''legal action'' for purposes of § 171.206 to include a broad array of criminal, civil, and administrative investigations, actions, and proceedings as specified in the proposed § 171.206(e)(1)–(3).

We emphasize that to satisfy the proposed Protecting Care Access Exception, an actor's practice that is likely to interfere with lawful access, exchange, or use of EHI would need to fully satisfy relevant requirements of the *threshold* condition in § 171.206(a) and at least one of the other two conditions (§ 171.206(b) or § 171.206(c)).[248] Thus, a practice could not satisfy the exception if implemented based on an actor's good faith belief about any access, exchange, or use (that is permitted under HIPAA Privacy Rule and any other applicable privacy law) that potentially creates or increases anyone's risk of facing any legal action that would not be based upon a person having merely sought, obtained, provided, or facilitated care that was lawful under the circumstances in which such health care was provided. The exception is not intended to apply to an actor's interference with access, exchange, or use of EHI based on an actor's belief that the practice would reduce any person's exposure to legal action or liability based on the conduct that was not the mere act of seeking, obtaining, providing, facilitating, or (where the *patient protection* condition applies, potentially needing) reproductive health care that was, under the circumstances in which the conduct occurred, unlawful.

The belief requirement (subparagraph (1)) of the *threshold* condition (§ 171.206(a)) would ensure that the exception is applicable only in situations where an actor has a good faith belief that their practice of interfering with the access, exchange, or use of EHI that indicates the seeking, obtaining, providing or facilitating of reproductive health care (not with EHI access, exchange, or use in general or universally) could reduce a risk of potential exposure to legal action against identifiable persons that could otherwise arise as a consequence of the

[247] The addition of the ''reproductive health care'' definition to 45 CFR 160.103 is reflected in the Electronic Code of Federal Regulations (eCFR) system at *https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103* at the time this proposed rule (HTI–2) is issued. The annual revision of the published Title 45 occurs on October 1. (The eCFR is a continuously updated online version of the CFR. Please *see* the following website for more information about the eCFR system: *https://www.ecfr.gov/reader-aids/using-ecfr/getting-started.*)

[248] In relevant circumstances, an actor's practice might meet *both* the § 171.206(b) *patient protection* and § 171.206(c) *care access* conditions simultaneously. But each of these conditions could also apply in circumstances where the other does not. Thus, the proposed exception is intended and designed to apply where either or both of the *patient protection* and *care access* conditions are met in complement to the § 171.206(a) *threshold condition.*

particular access, exchange or use of specific EHI that is affected by the practice. To satisfy the § 171.206(a)(1) requirement, the actor's good faith belief would need to be that persons seeking, obtaining, providing, or facilitating reproductive health care ''are at risk'' of being potentially exposed to legal action. This does not mean that the exception would apply only where the actor is confident that legal action will follow from access, exchange, or use of EHI related to reproductive health care. ''Are at risk'' would simply mean that the risk the actor believes might arise as a consequence of the affected access, exchange, or use of EHI is one that could, to the best of the actor's knowledge and understanding, arise under law that is in place at the time the practice(s) that is based on the belief are implemented. Thus, the proposed § 171.206 exception would not apply to practices undertaken based on a hypothetical risk of exposure to legal action, such as one the actor postulates could perhaps become possible if applicable law(s) were to change in the future. Similarly, where an actor may believe a risk exists that someone could potentially be exposed to legal action but does not believe that a particular practice could achieve some reduction in that risk, the § 171.206(a)(1) requirement would not be met by (and therefore the § 171.206 exception would not apply to) that practice.

The § 171.206(a) *threshold* condition's tailoring requirement (§ 171.206(a)(2)) is intended to further restrict the exception's coverage to practices that are no broader than necessary to reduce the risk of potential exposure to legal action that the actor has a good faith belief could arise from the particular access, exchange or use of the specific EHI.

Like similar provisions in other exceptions, this tailoring requirement ensures that the exception would not apply to an actor's practices likely to interfere with access, exchange, or use of all of an individual's EHI when it is only portions of the EHI that the actor believes could create the type of risk recognized by the exception. Where only portion(s) of the EHI an actor has pertaining to one or more patients pose a risk of potentially exposing some person(s) to legal action, the proposed Protecting Care Access Exception would apply only to practices affecting particular access, exchange, or use of the specific portion(s) of the EHI that pose the risk.

Data segmentation is important for exchanging sensitive health data (as noted in the ONC Cures Act Final Rule at 85 FR 25705) and for enabling access, exchange, and use of EHI (as noted in the HTI–1 Proposed Rule at 88 FR 23874). We are aware of external efforts to innovate and mature consensus technical standards, and we hope this will foster routine inclusion of increasingly advanced data segmentation capabilities in more EHR systems and other health IT over time.

However, we have received public feedback (both prior to and in response to the HTI–1 Proposed Rule request for information on health IT capabilities for data segmentation and user/patient access at 88 FR 23874 through 23875) indicating that there is currently significant variability in health IT products' capabilities to segment data, such as to enable differing levels of access to data based on the user and purpose. We recognize there is a potential that some actors who may wish to withhold specific EHI under the conditions specified in the proposed Protecting Care Access Exception (§ 171.206) may not yet have the technical capability needed to unambiguously segment the EHI for which § 171.206 would apply from other EHI that they could lawfully make available for a particular access, exchange, or use. Therefore, we propose elsewhere in this proposed rule to modify the Infeasibility Exception's *segmentation* condition (§ 171.204(a)(2)) to explicitly provide for circumstances where the actor cannot unambiguously segment EHI that may be withheld in accordance with Protecting Care Access Exception (§ 171.206) from the EHI for which this exception is not satisfied. (This and other proposed revisions to § 171.204(a)(2) are discussed in section IV.B.2.A of this proposed rule.)

The implementation requirement in subparagraph (a)(3) of the *threshold* condition is intended to ensure that practices are applied fairly and consistently while providing flexibility for actors to implement a variety of practices, and to do so through organizational policy or in response to specific situations, as best suits their needs. We propose that any given practice could satisfy this implementation requirement in either of two ways. First, an actor could undertake the practice consistent with an organizational policy that meets the requirements proposed in § 171.206(a)(3)(i). To satisfy the proposed requirement in this first way, the organization's policy would need to identify the connection between the particular access, exchange, or use of the specific EHI with which the practice interferes and the risk of potential exposure to legal action that the actor believes could be created by such access, exchange, or use. The policy would also need to be:

- in writing;
- based on relevant clinical, technical, or other appropriate expertise;
- implemented in a consistent and non-discriminatory manner; and
- structured to ensure each practice implemented pursuant to the policy satisfies paragraphs (a)(1) and (a)(2) as well as at least one of the conditions in paragraphs (b) or (c) of § 171.206 that is applicable to the prohibition of the access, exchange, or use of the EHI.

In order to ensure each practice implemented pursuant to the policy applies only to the particular access, exchange, or use scenario(s) to which at least one of the conditions in paragraphs (b) or (c) of § 171.206 is applicable, a policy would need to specify the facts and circumstances under which it would apply a practice. Such specifications need not be particularized to individual patients but would need to identify with sufficient clarity for the actor's employees and business associates (or other contractors, as applicable) to accurately apply the practice only to relevant access, exchange, or use scenarios. The types of facts or circumstances the policy might need to specify may vary, but we believe might often include such details as to what EHI (such as what value set(s) within what data element(s)) and to what scenario(s) of access, exchange, or use the policy will apply to a practice.

There may be value sets currently available or in development by various parties that may help an actor to identify what EHI within the actor's EHR or other health IT systems indicates care meeting the reproductive health care definition in 45 CFR 160.103. However, we do not propose to limit the application of the exception to any specific value set(s). Because version updates of such value sets, or new value sets, may develop more rapidly than adoption or reference of them in regulations could occur, we believe the intended operation of the exception will be best served by leaving actors flexibility to identify, document in their organizational policy or case-by-case determination(s), and then use whatever value set(s) comport with their belief that a risk of potential exposure to legal action (consistent with the exception's conditions) could be created or increased by sharing specific EHI indicating or (where the *patient protection* condition applies) potentially related to reproductive health care.

The proposed provision in paragraph (a)(3)(ii) offers actors the second of the two ways to satisfy subparagraph (a)(3):

by making determination(s) on a case-by-case basis. To satisfy paragraph (a)(3)(ii), any case-by-case determination would need to be made in the absence of an organizational policy applicable to the particular situation and be based on facts and circumstances known to, or believed in good faith by, the actor at the time of the determination. A practice implemented based on the determination must also be tailored to reduce the risk of legal action the actor has a good faith belief could result from access, exchange, or use of the EHI. And the practice must be no broader than necessary to reduce the risk of potential exposure to legal action (paragraphs (a)(1) and (a)(2)).

Finally, to meet paragraph (a)(3)(ii), the determination made on a case-by-case basis would need to be documented either before or contemporaneous with beginning to engage in any practice(s) based on the determination. The documentation of the determination must identify the connection or relationship between the interference with access, exchange, or use of EHI indicating or related to reproductive health care and the risk of potential exposure to legal action. By identifying the connection or relationship, this documentation would explain what risk the actor believes the practice(s) will mitigate.

The proposed § 171.206(a)(3) implementation requirement's optionality would support the actor's interest in having flexibility to address both relatively stable and more dynamic facts and circumstances. Each of the options is intended to balance this interest of the actor with the interests of others, including the actor's current and potential competitors, in ensuring that any information blocking exception does not apply to practices that are not necessary for the specific purpose(s) the exception is designed to serve. The subparagraph (a)(3)(i) organizational policy provision would allow actors to apply relevant expertise available at the time of creating and updating organizational policies to craft a policy that suits their circumstances (such as technological capabilities and staffing and the types of scenarios they have experienced or expect to experience, perhaps with some regularity). The case-by-case determination provision (subparagraph (a)(3)(ii)) ensures the proposed exception would be available for all actors across the full array of facts and circumstances they may encounter, including unanticipated ones.

We are considering adding to the § 171.206(a) *threshold* condition an additional requirement that the actor's practice must not have the effect of increasing any fee for accessing, exchanging, or using EHI that the actor chooses to seek from an individual (as defined in § 171.202(a)) or counsel representing the individual in an action or claim contemplated, filed, or in progress with a Federal agency, in Federal court, or a court in the jurisdiction where care was provided. We propose this requirement in the alternative. This alternative proposal would mean that the proposed exception would not be met by an actor's practice that had such effect even if any fee that the actor chooses to charge for access, exchange, or use of EHI would, after such increase, continue to satisfy the Fees Exception (§ 171.302). We seek comment on this potential additional requirement for an actor's practice to satisfy the proposed *threshold* condition (§ 171.206(a)).

c. Patient Protection Condition

The proposed *patient protection* condition in paragraph (b) of § 171.206 could be met by practices implemented for the purpose of reducing the patient's risk of potential exposure to legal action (as legal action would be defined in § 171.206(e)). Further narrowing the practices that could satisfy the condition, paragraph (b)(1) would require that the practice affect only specific EHI (the data point or points) that the actor in good faith believes demonstrates, indicates, or would carry a substantial risk of supporting a reasonable inference that the patient has: (1) obtained reproductive health care that was lawful under the circumstances in which such care was provided; (2) inquired about or expressed an interest in seeking reproductive health care; or (3) particular demographic characteristics or health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated.

For purposes of § 171.206, we would interpret ''lawful under the circumstances in which it was provided'' to mean that when, where, and under relevant circumstances (such as, for health care, the patient's clinical condition and a rendering health care provider's scope of practice) the care was:

- protected, required, or authorized by Federal law, including the United States Constitution, in the circumstances under which such health care is provided, regardless of the State in which it is provided; or
- not prohibited by Federal law and lawful under the law of the jurisdiction in which it was provided.

Where care is not prohibited by Federal law and permitted under the law of the jurisdiction in which it is provided, we would consider the care lawful regardless of whether the same care would, under otherwise identical circumstances, also be unlawful in other circumstances (for instance, if provided in another jurisdiction).

The *patient protection* condition proposed in § 171.206(b) would provide the actor discretion and flexibility over time to determine which EHI poses a risk of potential exposure to legal action. At the same time, the § 171.206(b)(1) requirement that the practice ''affect only the access, exchange, or use of specific electronic health information the actor believes could expose the patient to legal action'' because it shows or carries a substantial risk of supporting an inference of one of the things described in subparagraphs (i) through (iii) would preserve the expectation that the actor would share other EHI that the actor does not believe poses such a risk unless another exception applies, or sharing restriction(s) under other law apply, to that other EHI in relevant circumstances.

We propose that even when an actor has satisfied the requirements in paragraph (b)(1), the practice would be subject to nullification by the patient if the patient explicitly requests or directs that a particular access, exchange, or use of the specific EHI occur despite any risk(s) the actor has identified to the patient. This requirement (paragraph (b)(2)) is intended to respect patients' autonomy to choose whether and when to share their own EHI. The requirement would prevent the exception from applying where an actor is attempting to substitute their judgment or tolerance of risks to the patient for the patient's own judgment.[249]

[249] The *patient protection* condition in § 171.206(b) would apply to practices implemented for the purpose of reducing the patient's risk of potential exposure to legal action (as legal action would be defined in § 171.206(e). The *care access* condition in § 171.206(c) would apply to practices an actor implements to reduce potential exposure to legal action based on the mere fact that reproductive health care occurred for persons, other than the person seeking or receiving care, who provide care or are otherwise involved in facilitating the provision or receipt of reproductive health care that is lawful under the circumstances in which it is provided. In some circumstances, an actor's practice might meet both the § 171.206(b) *patient protection* and § 171.206(c) *care access* conditions simultaneously. But each of these conditions could also apply in circumstances where the other does not. Thus, the proposed exception is intended and designed to apply where either or both of the *patient protection* and c*are access* conditions are met in complement to the § 171.206(a) *threshold* condition.

We clarify in proposed paragraph (b)(3) that for purposes of the *patient protection* condition ''patient'' means the natural person who is the subject of the electronic health information or another natural person referenced in, or identifiable from, the EHI as a person who has sought or obtained reproductive health care. We propose to also recognize as ''patients,'' for purposes of this condition, natural persons other than the natural person who is the subject of the EHI because we are aware that in the field there may be times when information about a parent's reproductive health care is included in the EHI of a child. (A child's parent is often identified in or identifiable through the child's EHI.)

We note that the *patient protection* condition, and generally the exception, are not intended to permit any actor to avoid legal consequences resulting from malpractice or their own wrongdoing. The proposed exception is also not intended to have any effect on any obligation an actor has to comply with disclosure requirements under Federal, State, or Tribal law that applies to the actor. Even where an actor could deny any given access, exchange, or use of EHI for permissible purposes consistent with an information blocking exception, the actor who is a HIPAA covered entity or business associate would still have to comply with the 45 CFR 164.524 individual right of access, and any actor would still have to comply with other valid, applicable law compelling the actor to make the EHI available for permissible purposes.[250] For example, the actor would still need to comply with applicable legal discovery rules and judicial orders issued by a court of competent jurisdiction. Non-compliance with such other laws could subject the actor to sanctions under those other laws regardless of whether the actor's practice would also be considered information blocking or would instead be covered by an exception set forth in any subpart of 45 CFR part 171.

We are also considering, and propose in the alternative, adding one or more of the following explicit requirements to the *patient protection* (§ 171.206(b)), *care access* (§ 171.206(c)), or *threshold* (§ 171.206(a)) condition(s) so that to be covered by the exception the actor's practice must not:

- if undertaken by any actor that is also a HIPAA covered entity or business associate, delay beyond the time allowed under 45 CFR 164.524 or otherwise interfere with any request for access, exchange, or use of EHI that implicates the HIPAA Privacy Rule's individual right of access in a manner or to an extent that would constitute non-compliance with 45 CFR 164.524;
- deny the individual (as defined in § 171.202(a)(2)) or an attorney representing the individual access, exchange, or use of EHI for purposes of considering, bringing, or sustaining any claim for benefits under any Federal law or any action against the actor under administrative, civil, or criminal (including discovery and other procedural) law of the jurisdiction in which care indicated by the EHI was provided;
- interfere with any use or disclosure of EHI required by subpart C of 45 CFR part 160 as it applies to actions by the Secretary (or by any part of HHS) with respect to ascertaining compliance by covered entities and business associates with, and the enforcement of, applicable provisions of 45 CFR parts 160, 162, and 164; or
- prevent any EHI's use by or disclosure to a Federal agency or a State, or Tribal authority in the jurisdiction where health care indicated by the EHI was provided, to the extent such use or disclosure is permitted under 45 CFR parts 160 and 164.

Each (or any) of these requirements would function as a limit on the applicability of the exception and mean that practices not meeting the exception for those reasons could constitute information blocking in addition to potentially violating any other law. (Due to the substantial variation across individual actors' circumstances, it would be impossible to maintain in the text of 45 CFR part 171 an accurate, comprehensive catalog of all other laws that could be implicated by an actor's practices otherwise consistent with any exception set forth in subparts B, C, or D of 45 CFR part 171.)

We welcome comments on the proposed exception, including whether commenters would recommend we add to the exception (if finalized) any or all of the above potential additional limits on applicability of the proposed Protecting Care Access Exception (§ 171.206) that we propose in the alternative.

d. Care Access Condition

The proposed *care access* condition would apply as specified in paragraph (c) of § 171.206 under the ''Regulatory Text'' heading of this proposed rule. The condition could be met by practices an actor implements to reduce potential exposure to legal action based on the mere fact that reproductive health care occurred for persons, other than the person seeking or receiving care, who provide care or are otherwise involved in facilitating reproductive health care that is lawful under the circumstances in which it is provided. Such persons would include licensed health care professionals, other health care providers, and other persons involved in facilitating care that is lawful under the circumstances in which it is provided. Such persons would include persons (friends, family, community caregivers, and others) who help patients find, get to the site of or home from, and afford care. For purposes of the *care access* condition in § 171.206(c) and § 171.206(b)(1)(i) (within the *patient protection* condition), the reproductive health care must be ''lawful under the circumstances in which it is provided'' as explained above in section IV.B.3.c of this proposed rule.

To satisfy the *care access* condition in paragraph (c) of § 171.206 as proposed, the practice must affect only access, exchange, or use of specific EHI (one or more data points) that the actor believes could potentially expose a care provider(s) or facilitator(s) to legal action because that EHI shows or would carry a substantial risk of supporting a reasonable inference that such person(s) are currently providing or facilitating, have provided or facilitated, or both, reproductive health care that is (or was) lawful under the circumstances in which it is (or was) provided.[251]

We propose this requirement in order to ensure the § 171.206(c) *care access* condition would not apply to an actor's practice affecting access, exchange, or use of EHI that the actor does not believe could create a risk of potential exposure to legal action based on the mere fact that reproductive health care was provided or facilitated. Actors will often have additional EHI that applicable law would also permit them

[250] For purposes of the information blocking regulations, ''permissible purpose'' is defined in 45 CFR 171.102.

[251] The *patient protection* condition in § 171.206(b) would apply to practices implemented for the purpose of reducing the patient's risk of potential exposure to legal action (as legal action would be defined in § 171.206(e). The *care access* condition in § 171.206(c) would apply to practices an actor implements to reduce potential exposure to legal action based on the mere fact that reproductive health care occurred for persons, other than the person seeking or receiving care, who provide care or are otherwise involved in facilitating the provision or receipt of reproductive health care that is lawful under the circumstances in which it is provided. In some circumstances, an actor's practice might meet both the § 171.206(b) *patient protection* and § 171.206(c) *care access* conditions simultaneously. But each of these conditions could also apply in circumstances where the other does not. Thus, the proposed exception is intended and designed to apply where either or both of the *patient protection* and *care access* conditions are met in complement to the § 171.206(a) *threshold* condition.

to make available for permissible purposes, which could include information relevant to the safety, continuity, and quality of care, such as a patient's chronic condition(s) or a medically confirmed allergy to a substance that does not indicate or suggest reproductive health care has, or may have, occurred (and thus poses no risk of exposure to legal action as defined in § 171.206(e)). To the extent the actor has such other EHI that the actor can (both legally and technically) make available for any and all permissible purposes, we would expect the actor to do so. We recognize that in some circumstances the actor may need to make such other EHI available in an alternative manner rather than the manner requested by the requestor. (We use ''manner requested'' and ''alternative manner'' here in a sense consistent with paragraphs (a) and (b), respectively, of the Manner Exception as currently codified in § 171.301.)

We propose that when an actor's practice satisfies the *threshold* condition in § 171.206(a) and meets all the requirements of the *care access* condition in § 171.206(c), the actor's practice will not constitute information blocking. As with any of the existing exceptions, the proposed Protecting Care Access Exception would not supersede or override any other valid Federal, State, or Tribal laws that compel production of EHI for purposes of legal proceedings or that compel other disclosures in relevant circumstances. Therefore, actors and other interested persons will want to remember that satisfying an exception set forth in 45 CFR part 171 does not prevent other law that operates independently from the 45 CFR part 171 from potentially compelling an actor to provide access, exchange, or use of EHI in manners or for purposes the actor, or an individual, might prefer the EHI not be accessed, exchanged, or used. As actors are likely already aware, conduct that is not considered ''information blocking'' under 45 CFR part 171, whether on the basis of satisfying an exception or on the basis of not meeting an element of the definition of ''information blocking'' in the information blocking statute (42 U.S.C. 300jj–52) may nevertheless violate, and may subject the actor to consequences authorized by, laws separate from and operating independently of the information blocking statute and 45 CFR part 171.

The *care access* condition would apply where the risk of potential exposure to legal action is specific to the mere fact that reproductive health care (that was lawful under the circumstances in which it was provided) was provided or facilitated. The *care access* condition would not be met where the risk of potential exposure to legal action is based on care having been provided in circumstances where the care was not lawful. (We refer readers again to our explanation, in Section IV.B.3.c of this proposed rule, of how we would interpret ''lawful under the circumstances'' in which care was provided in context of the proposed § 171.206.)

The proposed exception would not apply to a practice that precludes the patient or an attorney representing the patient from obtaining access, exchange, or use of the patient's EHI for purposes of filing a benefit claim or a complaint against the actor with any agency of the U.S. Government. It would be unreasonable for an actor to withhold from a patient or a patient's attorney EHI that they need or seek to use in support of a claim for a benefit that is filed with any agency of the U.S. Government. It would also be unreasonable for the actor to attempt to withhold EHI access, exchange, or use to impede the patient or the patient's attorney filing, or the U.S. Government investigating, any complaint against the actor that the patient or the patient's attorney may file with any agency of the U.S. Government. Patients and their attorneys should have easy access to necessary information for considering, filing, or maintaining or pursuing such claims or complaints.

As we have noted several times in this proposed rule, an actor that is also required to comply with the HIPAA Privacy Rule must comply with the individual right of access as codified in 45 CFR 164.524 regardless of whether the actor may be able to satisfy any existing or proposed exceptions to the § 171.103 definition of ''information blocking.'' To ensure actors remain aware of this fact, we propose as the first of several (non-exclusive) alternatives, to include in the proposed *care access* condition (§ 171.206(c)) an additional explicit restriction of the condition to practices that do not violate 45 CFR 164.524. We might finalize this additional requirement even if we do not finalize any of the other additional requirements that we propose to potentially apply to the Protecting Care Access Exception as a whole or to the proposed *patient protection* condition (§ 171.206(b)) (as discussed in section IV.B.3.b, above).

The first requirement we propose in the alternative specific to the *care access* condition would provide for the *care access* condition (§ 171.206(c)) to be met by practices that could interfere with an individual's access to EHI only to the extent that the interference could otherwise implicate the ''information blocking'' definition in § 171.103 without also constituting non-compliance with 45 CFR 164.524 where 45 CFR 164.524 also applies. For example, under this first proposed potential added restriction on applicability of § 171.206(c), a delay of an individual's access, exchange, or use of EHI that would rise to the level of an ''interference'' for purposes of the ''information blocking'' definition in § 171.103 that satisfied all other requirements of § 171.206(a) and (c) would be covered by the § 171.206 exception only to the extent the delay of the individual's (or their personal representative's) access to EHI did not exceed the maximum time permitted, in the specific circumstances, for fulfillment of access to PHI under 45 CFR 164.524. (Coverage of an exception would be irrelevant for a delay not rising to the level of an ''interference'' because § 171.103 focuses on practices not required by law that are likely to ''interfere with'' access, exchange, or use of EHI.) This proposed restriction to practices not violating § 164.524 would also mean § 171.206 would apply where an actor's interference involved offering fewer manners of access, exchange, or use than would be feasible for the actor to support, but only to the extent that the actor's limiting the manners in which EHI is made available would not constitute a violation under 45 CFR 164.524. We welcome comment on this first additional potential limitation on the applicability of the proposed exception.

We propose as a second (again, non-exclusive) alternative to include in the proposed *care access* condition (§ 171.206(c)) an additional requirement that would be applicable specifically if an actor chooses to engage in a practice of delaying fulfillment of requests for EHI access, exchange, or use by individuals (as defined in § 171.202(a)(2)) because the actor wants to provide, in a non-discriminatory manner, information to the individual relevant to the actor's good faith belief that a risk of potential exposure to legal action could be created by the individual's choice of how to receive their EHI or to whom the individual wishes to direct their EHI. For example, an actor that is also a HIPAA covered entity would, under § 164.524, be required to fulfill an individual's request for access to PHI or to transmit to a third party an electronic copy of the individual's PHI in an EHR within the time period required under § 164.524.

Where the § 171.206 exception would apply and the third party is not a covered entity or business associate, the actor may wish to first provide the individual with information (that is, to the best of the actor's knowledge and belief, accurate and factual) about the HIPAA Privacy, Security, and Breach Notification Rules and differences in their applicability to EHI when it is not held by a HIPAA covered entity or business associate in comparison to when it is. Similarly, an actor might wish to communicate such information to an individual before enabling access, exchange, or use of EHI for a health care provider that is not a HIPAA covered entity or business associate. The actor might, for example, be concerned that the individual may not have previously obtained or been provided basic information about how the applicability of the HIPAA Privacy Rule to information held by or for a provider that is not a HIPAA covered entity may differ from the rule's application to the same information when it is held by or for entities regulated under HIPAA. The actor may wish to provide the individual such information so that the individual would have a fair opportunity to consider the possible privacy risks. In such situations, the actor may be concerned about potential information blocking implications of the delay that is necessary to provide the individual with information. Or the actor may be concerned with the delay that results when an individual (or their personal representative) is considering the information before confirming they want the actor to proceed with enabling the application the individual (or their personal representative) has chosen to receive the EHI of which the individual is a subject. Specifically, the actor may be concerned these delays could rise to the level of an ''interference'' and, therefore, implicate the information blocking definition even if the time required is less than the maximum time permitted to fulfill PHI access under 45 CFR 164.524 in the relevant circumstances.

Therefore, we are considering the second proposed additional a requirement for § 171.206. This second potential additional requirement would apply where an actor's practice delays making EHI available upon individual request or directive in order to provide individuals with non-biased general information about relevant laws or about the actor's belief that is consistent with § 171.206(a)(1)(i), the delay must be of no longer duration than is reasonably necessary to provide to the individual two things:

(1) honest information that is provided in a non-discriminatory manner and that is relevant to the actor's belief that a risk of potential exposure to legal action could be created by the particular access, exchange, and use of what specific EHI, such as general information about privacy laws or other laws that the actor believes may be relevant; and

(2) a reasonable opportunity to consider the information and seek additional information from other sources if the individual would like, before the individual is asked to either confirm or revise any specifics of their request for access, exchange, or use of their EHI.

Under this alternative proposal specific to delaying a response to a right of access request (including the right to direct a HIPAA covered entity to transmit to a third party an electronic copy of the individual's PHI in an EHR), delays longer than reasonably necessary to provide the individual with information relevant to the actor's belief that is consistent with § 171.206(a)(1) and allow the individual to consider the actor's information and seek information from additional source(s) (if the individual desires) would not satisfy the § 171.206(c) *care access* condition. This proposed restriction that is specific to delays for the purpose of informing individuals of an actor's belief that sharing specific EHI could create risk of potential exposure to legal action could be implemented regardless of whether we also implement a requirement that, for the *care access* condition or for the *threshold* condition to be met by an actor's practice, the practice must not constitute a violation of § 164.524. This potential additional requirement would limit the applicability of the condition in scenarios where an actor might choose to engage in delay to provide individuals with information about potential privacy consideration, but should not be construed as creating an affirmative requirement for any actor to delay fulfillment of individual access requests to provide individuals with information about potential privacy implications of the individual's request. We reiterate that information blocking exceptions are voluntary.

We reiterate that even in scenarios where an actor's denial of access, exchange, or use of EHI might not be ''information blocking'' because it satisfies an exception under and for purposes of part 171, an actor that is a HIPAA covered entity or business associate will still need to comply with 45 CFR 164.524 (individual right of access). (This is true of the exceptions codified in subparts B, C, and D of 45 CFR part 171 as of the date of publication of this proposed rule and would also be true of the new exceptions proposed in this rule in the event any of them are finalized.)

The additional requirement(s) we are considering, and as noted above propose in the alternative, would seek to more finely tune the exception's balance of the interests of actors and patients in protecting reproductive health care availability by mitigating legal risks for the people who provide that care, and for the people who facilitate the provision of such care, with the interests of individuals in being able to access, exchange, and use all of their EHI however and whenever they want, and to share all of their EHI however and with whomever they choose, at no cost for ''electronic access'' as defined in § 171.302(d). We seek comment on these proposals.

e. Clarifying Provisions: Presumption and Definition of ''Legal Action''

For purposes of determining whether an actor's practice meets paragraph § 171.206(b)(1)(i) or § 171.206(c), we propose in § 171.206(d) that care furnished by someone other than the actor would be presumed to be lawful unless the actor has actual knowledge that the care was not lawful under the circumstances in which it was provided. The presumption provision proposed in § 171.206(d) is similar to the presumption provision finalized (in 45 CFR 164.502(a)(5)(iii)(C)) by the 2024 HIPAA Privacy Rule, but is necessarily different because of differences in how the prohibition at 45 CFR 164.502(a)(5)(iii)(A) operates and how the proposed Protecting Care Access Exception (§ 171.206) is intended to operate.

First, the proposed Protecting Care Access Exception (§ 171.206) would be voluntary. It would offer those actors who may wish to engage in practices likely to interfere with EHI access, exchange, or use under the exception's conditions certainty that practices satisfying the exception will not be considered ''information blocking.'' Nothing in § 171.206 is intended to create an affirmative obligation for any actor to evaluate whether the Protecting Care Access Exception might apply to any access, exchange, or use of EHI for permissible purposes.

Second, the proposed Protecting Care Access Exception (§ 171.206) is based on statutory authority found in section 3022 of PHSA to identify reasonable and necessary activities that do not constitute information blocking for purposes of the PHSA 3022 definition of the term. We do not propose that

anything in § 171.206 would operate to override an actor's obligation to comply with another (applicable) law that requires the actor to make EHI available for any permissible purpose. Thus, an actor may still be compelled to disclose EHI in compliance with such other law even where the exception might mean an actor's failure to comply with such other law would not be considered ''information blocking'' under 45 CFR part 171 or PHSA 3022. (The exception would not be relevant where an actor is also a HIPAA covered entity or business associate would be required to comply with the prohibition at 45 CFR 164.502(a)(5)(iii) because a HIPAA covered entity's or business associate's practice of refusing to make a use or disclosure of PHI prohibited by the HIPAA Privacy Rule is ''required by law'' and therefore not information blocking to begin with.)

Finally, a policy goal of the proposed Protecting Care Access Exception is that it be easy for any actor to confidently and efficiently meet the conditions of the proposed exception. One way the exception's structure supports this goal is by providing (in § 171.206(a)(3)(i)) for the actor to implement practices per organizational policies that address particular types of EHI sharing scenarios where the actor believes the risk of potential exposure to legal action could be created even if the actor has not yet received a request for EHI for the activities specified in 45 CFR 164.502(a)(5)(iii)(A) or any of the purposes specified in 45 CFR 164.512(d), (e), (f), or (g)(1) for which the attestations specified in 45 CFR 164.509 would be required as a precondition for disclosing PHI potentially related to reproductive health care to be permitted under the 2024 HIPAA Privacy Rule.

As noted elsewhere, an actor's practice satisfying the new exception would mean the practice will not be considered information blocking. To the extent that EHI indicates or potentially relates to reproductive health care that was not lawful under the specific circumstances in which it was provided, we presume that the legal authority compelling disclosure of EHI for such purposes would have its own enforcement provisions independent of the penalties and disincentives authorized by PHSA 3022 for an actor determined by the HHS OIG to have committed information blocking. Because exception would not exempt the actor from their obligation to comply with such other law, we do not believe it is necessary to preserve the potential for information blocking penalties to apply in addition to any consequences that might attach under such other law to an actor's non-compliance with that law. On the other hand, we believe it is important to ensure that concern about information blocking consequences would not prevent the actor from, for example, delaying fulfillment of a demand for EHI in order to review factual information supplied by the requestor and determine whether that information ''demonstrates a substantial factual basis'' (as stated in 45 CFR 164.502(a)(5)(iii)(C)(2)) and, by extension, whether the 2024 HIPAA Privacy Rule or applicable State law permits, preempts, or conflicts with the law the requestor indicates compels the actor to make the EHI available to the requestor.[252]

We are, moreover, concerned that tying the proposed § 171.206(d) presumption provision to the requestor not supplying information demonstrating a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided would make the proposed Protecting Care Access Exception (§ 171.206) more difficult for actors to use and therefore could discourage actors from using it. We are concerned this difficulty could discourage use of the exception particularly by those actors—such as small and safety net health care providers or non-profit health information networks who serve them—who may have limited ability to divert resources to these types of legal analyses, especially in circumstances where this exception is intended to apply but the request for EHI access, exchange, or use may not be coming from a law enforcement entity and the access, exchange, or use of EHI sought may not be for a law enforcement purpose.

We propose in the alternative to add to § 171.206(d), if finalized, a provision that parallels the provision in 45 CFR 164.502(a)(5)(iii)(C)(2) and that would prevent the § 171.206(d) presumption from applying where factual information supplied by the person requesting access, exchange, or use of EHI demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided. We welcome comments on this alternative proposal. We are particularly interested in whether and why actors, patients, and other interested parties may believe § 171.206(d) would strike a better balance between actors' interests in a simpler, more easily usable exception and requestors' interests in obtaining EHI for permissible purposes with or without the additional limit on application of the presumption provision.

We propose in § 171.206(e) to define ''legal action'' for purposes of the Protecting Care Access Exception. Under the proposed definition, ''legal action'' would include any of the following when initiated or pursued against any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care: (1) civil, criminal, or administrative investigation; (2) a civil or criminal action brought in a court to impose criminal, civil, or administrative liability; or (3) an administrative action or proceeding against any person. We emphasize that the proposed Protecting Care Access Exception would apply where an actor's practice meets the § 171.206(a) *threshold* condition and at least one of the other two conditions in the exception, none of which would require the actor to quantify a degree, amount, or probability of the risk of potential exposure to legal action the actor believes in good faith exists and could be reduced by the practice to which § 171.206 applies.

We welcome comment on all aspects of the proposal for a new Protecting Care Access Exception to the information blocking definition.

4. Requestor Preferences Exception

We propose a new exception, ''Requestor Preferences,'' in § 171.304 to offer actors certainty that, under the conditions specified in this exception, it would not be considered ''information blocking'' to honor a requestor's preferences expressed or confirmed in writing for: (1) limitations on the scope of EHI made available to the requestor; (2) the conditions under which EHI is made available to the requestor; and (3) the timing of when EHI is made available to the requestor for access, exchange, or use.

Since publication of the ONC Cures Act Final Rule, actors have indicated a preference for greater certainty as to the conditions under which they would not be committing information blocking if they were to honor certain preferences expressed by a requestor seeking lawful

[252] We remind readers that the currently codified ''pre-condition not satisfied'' sub-exception of the Privacy Exception outlines a framework for actors to follow so that the actors' practices of not fulfilling requests to access, exchange, or use EHI would not constitute information blocking when one or more preconditions has not been satisfied for the access, exchange, or use to be permitted under applicable Federal and State, or Tribal laws. Please *see* § 171.202(b) and discussion in HTI–1 final rule (at 89 FR 1351 through 1354) of how information blocking exception work in concert with the HIPAA Rules and other privacy laws to support health information privacy.

access, exchange, or use of EHI. In some instances, this preference might be that some type(s) of new EHI are not made available as quickly as would be technically feasible or that a more limited scope of EHI is made available than would be permitted (or required) under applicable law based on whose EHI the requestor seeks and for what purpose(s). For example, actors have indicated that they are uncertain of the scenarios when honoring an individual's request for delay of EHI availability to the individual in the patient portal would not be information blocking. Actors have also indicated that they are unable to honor a health care provider's expressed preference to receive only some of the EHI that an actor has and could disclose to the provider under applicable law, because the actor is uncertain whether honoring the health care provider's preference would be considered information blocking. The proposed exception (new § 171.304) would address these concerns by providing certainty of the conditions under which we would not consider an actor to engage in information blocking when the actor honors a requestor's preference to: (1) receive only a subset of EHI (limitation on scope of EHI), (2) have the EHI be available to the requestor only under specific timing or other conditions, or (3) any combination of such preferences.

We recognize that, sometimes, a requestor who seeks access, exchange, or use of EHI may prefer to have less EHI available to the requestor than an actor has and would be permitted to make available under the HIPAA Privacy Rule (and any other applicable law(s) restricting uses and disclosures of an individual's health information to protect the individual's privacy). We also recognize that sometimes a requestor may not want particular EHI to be available to the requestor immediately, perhaps preferring the EHI not be available until a certain period of time has elapsed or until certain conditions are met. For example, an individual who uses a patient portal or app to access EHI of which they are the subject may not want certain test results to be available in that patient portal or app for a certain number of hours or until the next business day (timing preference). Similarly, an individual may not want the results of certain diagnostic tests performed on the individual to be available to the individual in a patient portal or app until the doctor who ordered the test(s) has seen the results or until a doctor, nurse, or other health care professional is available who can explain what the results mean (conditions for making EHI available preference). For a provider-to-provider example, a primary-care clinician office (requestor) may ask that for laboratory tests done more than once during a patient's stay at a hospital, the hospital (actor) only send the clinician office the results from the last time each test was done (scope of EHI preference), and only send that EHI to the clinician office upon the patient's discharge from the hospital stay (a preference for the conditions under which EHI becomes available). As another provider-to-provider example, a health care provider (requestor) might ask another health care provider (actor) to not send all of the medication history the responding actor has for a patient that the actor is legally permitted to share with the requesting health care provider. The requestor might ask the responding actor to send instead only the patient's current medications and known allergies. The proposed exception (to be codified in § 171.304) would address all of these examples and a variety of other situations. The proposed exception (§ 171.304) has four separate conditions: (a) *request;* (b) *implementation,* (c) *transparency;* and (d) *reduction or removal.* In order for an actor's practice(s) to satisfy the proposed Requestor Preferences Exception (§ 171.304), the practice(s) would have to meet all four of the conditions at all relevant times.

The *request* condition (paragraph (a)) of this proposed new exception would require that the requestor express their preferences in writing without the actor improperly encouraging or inducing the requestor to ask for restrictions on the scope of EHI that would be available to the requestor, the conditions for which the EHI would be available, or timing of when EHI would be available to the requestor. This condition is similar to our approach under the Privacy Exception (§ 171.202) for obtaining a patient's consent under sub-exception (b), which cannot be satisfied if the actor improperly encourages or induces the individual to withhold consent or authorization. It is also similar to a provision of the Privacy Exception's sub-exception (e), which can be satisfied only if the individual requests that the actor not provide such access, exchange, or use of EHI without any improper encouragement or inducement of the request by the actor. In addition to disqualifying an actor's practices in response to such requests from application of the proposed Requestor Preferences Exception, we remind actors that any improper inducement of a patient's or other person's request for delay or other restrictions on a requestor's access to EHI is a practice that, on its own, could constitute an interference that implicates the information blocking definition.

To reiterate, the *request* condition (§ 171.304(a)) requires the requestor to document in writing their preference (or ask) for tailoring of their access, exchange, or use of EHI. This requirement is intended to guard against the inappropriate citation of the exception to retroactively ''justify'' the actor's limitation of a requestor's access, exchange, and use of EHI to suit the *actor's* preferences. The documentation requirement parallels a similar requirement of the Privacy Exception sub-exception (§ 171.202(e)) applicable to honoring individuals' requests to restrict other people's access, exchange, or use of their EHI.[253] Subparagraphs (a)(1), (2), and (3) of the proposed § 171.304 *request* condition also specify, as discussed above, the three types of preferences that the exception would cover.

The *implementation* condition (§ 171.304(b)) would ensure that an actor's practice of limiting the scope of EHI, conditions or timing of EHI availability to the requestor, or any combination of such limitations a requestor may ask for, are ''tailored'' to the specific request. In this condition, ''tailored to the specific request'' means the practice is no broader than necessary to do, and in fact does, what the requestor asked for in writing. The § 171.304(b) *implementation* condition would also require (see subparagraph (2)) that the request be implemented in a consistent and non-discriminatory manner. This requirement parallels similar requirements in existing exceptions, such as the Preventing Harm Exception (§ 171.201(f)(1)(iii)), Privacy Exception (§ 171.202(b)(1), (c)(3) and (3)), and the Security Exception (§ 171.203(c)). For purposes of § 171.304, discriminatory implementation practices would include, for example, the actor moving more slowly to modify or remove tailoring restrictions (see proposed condition (d)) from access, exchange, or use of EHI based on whether the requestor is a business competitor of the actor or if the requestor's access, exchange, or use of EHI is likely to facilitate competition with the actor. As innovation in biomedical informatics

[253] Although we are proposing revision to § 171.202(e) in this rule (*see* section IV.B.1.c of this preamble), we do not propose any change to the documentation requirement of the § 171.202(e) sub-exception. (The § 171.202(e) documentation requirement was discussed in the ONC Cures Act Final Rule; *see* 85 FR 25642 at 25858.)

and health IT advances, we anticipate that the EHI a requestor needs or wants to inform decisions related to seeking or accepting healthcare, or for public health activities or providing or paying for healthcare may change. Therefore, a requestor's preferences for restrictions on the amount of EHI or the conditions or timing of EHI availability to the requestor (or any combination of these) may well change over time. The requirement that the actor's practice be consistent and non-discriminatory is intended, for example, to ensure the exception will not apply to practices that are implemented in a manner that disadvantages competitors, potential competitors, or persons whose access, exchange, or use of EHI may facilitate competition with the actor in comparison to persons who are affiliates or whose access, exchange, or use of EHI would not be expected to facilitate competition with the actor.

The *transparency* condition (§ 171.304(c)) is intended to mitigate a risk of a specific unintended consequence of creating an exception that explicitly applies to an actor's choosing to agree to a requestor's ask that EHI availability to the requestor be tailored to the requestor's preferences. For example, to the surprise of the requestor, the tailoring of EHI ended up being more or less restrictive than what the requestor thought they agreed to. The risk of surprise to the requestor may arise either when a requestor first asks for tailoring or when an actor may no longer be able to maintain certain tailoring that they have previously agreed to implement in response to a requestor's ask. To mitigate the risk of surprise to a requestor, it is important for a requestor who has asked for tailoring to be informed of what the actor can and will do, or cannot or will not continue to do. To meet the *transparency* condition (§ 171.304(c)), an actor would be required to provide, in plain language, whether verbally or in writing, at least the explanation and notification described in the proposed § 171.304(c)(1) and (2) and to document in writing any explanation or notice that is not made in writing.

Meeting the *transparency* condition (§ 171.304(c)) would not require a contract or other formal agreement between actors and requestors. We also are not suggesting that we believe an actor's agreement to tailor when, how much, or under what conditions EHI becomes available to any given requestor should be treated as establishing a contract or binding agreement.

To meet the requirement in subparagraph (1) of § 171.304(c), an actor would be required to explain to the requestor what they can and will do to tailor EHI availability to the requestor. Meeting subparagraph (2) of § 171.304(c) would require an actor who experiences a change in operational status or technical capabilities affecting the actor's ability to maintain tailoring to make ''reasonable efforts'' to promptly notify each requestor for whom the actor had implemented affected tailoring. We have used the ''reasonable efforts'' standard in the existing *precondition not satisfied* sub-exception of the Privacy Exception (see § 171.202(b)(2)(i)). As we stated in the ONC Cures Act Final Rule preamble discussion of the finalized § 171.202(b), a ''reasonable efforts'' standard aligns with the case-by-case approach that is captured in the statutory information blocking provision (see 85 FR 25852). Similar to the ''reasonable efforts'' standard in § 171.202(b)(2)(i), the ''reasonable efforts'' standard in the proposed § 171.304(c)(2) would be met if the actor used reasonable efforts within its control to promptly provide the requestor with notice of the change in the actor's ability or willingness to continue applying the tailoring of EHI availability to the requestor that the requestor had requested, and the actor had implemented or agreed to implement. (We refer those who would like to read more about the ''reasonable efforts'' standard in context of the existing § 171.202(b)(2)(i) to the preamble discussion of the finalized § 171.202(b)(2)(i) at 85 FR 25852).

''Plain language'' is the standard proposed in § 171.304(c) for required explanations and notices rather than ''plain writing'' because we intend for the § 171.304(c) *transparency* condition as a whole to accommodate various methods of communication that are efficient and effective for both the actor who wants to satisfy the exception and the requestor who asks for tailoring. However, regardless of whether the actor and requestor communicate verbally or in writing, plain language would use terminology familiar to the requestor and make it easy for the requestor to understand what tailoring of their EHI access, exchange, or use the requestor can expect to be implemented or to have changed.[254]

To meet the *transparency* condition, subparagraph (c)(3) specifies that the actor must contemporaneously document in writing any required explanation or notice that is not provided to the requestor in writing. This requirement, like the use of ''plain language'' rather than ''plain writing'' as a standard for the explanations and notices, leaves flexibility for actors to communicate with requestors in writing, verbally, or in other ways that are efficient and effective for both the actor and requestor or otherwise mutually agreeable to them. Contemporaneous written documentation of explanations and notices not provided (initially made or later confirmed) to the requestor in writing would enable the actor to demonstrate what explanation or notice they provided and when. Contemporaneous written records of notices made or attempted would also be relevant, where notice fails to reach the requestor or the requestor does not recall details of the notice, to the actor's demonstration of the efforts the actor made to provide notice consistent with § 171.304(c)(2).

The *reduction or removal* condition (§ 171.304(d)) recognizes that a requestor's tailoring preferences may change over time and requires that an actor's tailoring practice accommodate such changes in requestor preferences. For the actor's practices restricting a requestor's access, exchange, or use of EHI based on the requestor's request to remain covered by this proposed exception when the requestor asks for reduction or removal of restrictions, the *reduction or removal* condition (§ 171.304(d)) would require the actor to act promptly as feasible on that request.

We do not propose to set a specific timeframe within which an actor would need to act on requests to reduce or remove restrictions upon receipt of any such request from the requestor. Rather, to satisfy the *reduction or removal* condition, the actor would need to act as promptly as feasible upon receiving such a request. Basing this requirement on what is feasible for the actor allows for consideration of the specific facts and circumstances under which the actor received the request. We believe this is preferable to setting a single fixed timeframe due to the considerable variation in actors' technical capabilities and operational circumstances at any given point in time. However, we recognize that actors and individuals may find some value in consistent maximum timeframe expectations for acting on a requestor's ask for removal or reduction of previously requested restrictions on their access, exchange, or use of EHI in individual access scenarios. (By ''individual access scenarios,'' we mean here those where the requestor is either: (a) the individual

[254] If an actor and a particular requestor do not both have at least limited working proficiency in any one language, the actor may need to employ a translator (whether human or an appropriate software application) to achieve communication with the requestor.

who is the subject of the EHI in question; or (b) their legal representative, including, but not limited to, personal representatives treated as the individual consistent with 45 CFR 164.502(g)). Therefore, we are considering specifying in § 171.304(d) that the maximum time any actor would have to reduce or remove the tailoring in any individual access scenario would be the time within which a HIPAA covered entity must provide an individual (as defined in 45 CFR 160.103) or their personal representative (see 45 CFR 164.524(g)) access to PHI in the designated record set under 45 CFR 164.524. Under this alternative proposal, the ''as promptly as feasible'' standard would apply to all other requestor scenarios without a specified maximum limit on the time an actor could take; but meeting the proposed § 171.304(d) *reduction or removal* condition in individual access scenarios would require the actor to reduce or remove restrictions in response to the requestor's request as promptly as feasible but in no case later than the maximum time permitted to fulfill individual access requests under 45 CFR 164.524. (This is an alternative proposal that is not reflected in the draft of § 171.304 in the ''Regulatory Text'' section of this proposed rule.) This alternative proposal for § 171.304(d) requirements would apply to individual access scenarios regardless of whether 45 CFR 164.524 would, in any given scenario, be implicated (*e.g.,* even if the actor were not a HIPAA covered entity or business associate).

This alternative proposed timeliness requirement for the § 171.304(d) *reduction or removal* condition specific to individual access scenarios would establish, by cross-reference to 45 CFR 164.524, that the maximum time the actor would have for acting on a request to reduce or remove restrictions would be the same timeframe within which a HIPAA covered entity must fulfill individual access under 45 CFR 164.524. For purposes of the § 171.304 exception under this alternative proposal, the time for responding to a request for reduction or removal of EHI access, exchange, or use tailoring in individual access scenarios would start on the date on which the actor receives the individual's (or their legal representative's) request for reduction or removal of tailoring. We would craft this additional requirement in this manner specifically so that, in the event the 45 CFR 164.524 timeliness standard were to change in the future (*see,* for example, the proposal to modify that standard at 86 FR 6459 and 6535), the § 171.304(d) condition would apply the same timeframe in effect for 45 CFR 164.524 at the point in time when an individual who is the subject of the EHI (or their legal representative) requested removal or reduction of restrictions on the individual's (or the legal representative's) EHI access. Such requests are, effectively, the requestor requesting their EHI be made available more promptly or completely than they had previously requested it be available to them. For clarity, once the reduction or removal of tailoring is complete for purposes of this proposed exception, all future requests for access, exchange, or use of EHI previously affected by the reduced or removed tailoring could implicate the interference and information blocking definition particularly §§ 171.103 and 171.104 (new proposed section).

If we finalize the proposed § 171.304 exception, with or without any explicit cross-reference to 45 CFR 164.524, this exception would operate as do all other 45 CFR part 171 exceptions: independently from the HIPAA Privacy Rule. We reiterate that an actor who is also a HIPAA covered entity or business associate *must* comply with the HIPAA Privacy Rule's requirements implicated in any circumstances or scenario, including without limitation the individual right of access (45 CFR 164.524(a)(1)), regardless of whether any given practice in any given scenario might not be considered ''information blocking'' on the basis of having satisfied any 45 CFR part 171 exception(s) to the definition codified in § 171.103.

We welcome comment on this proposed new exception.

5. Exceptions That Involve Practices Related to Actors' Participation in The Trusted Exchange Framework and Common Agreement™ (TEFCA™)

In the HTI–1 Proposed Rule (88 FR 23872), we proposed to add a *TEFCA*™ *manner* condition to the proposed revised and renamed Manner Exception. We stated that this approach ''aligns with the Cures Act's goals for interoperability and the establishment of TEFCA by acknowledging the value of TEFCA in promoting access, exchange, and use of EHI in a secure and interoperable way'' (88 FR 23872). In the HTI–1 Final Rule (89 FR 1437), in Part 171, we finalized a new subpart D ''Exceptions That Involve Practices Related to Actors' Participation in The Trusted Exchange Framework and Common Agreement (TEFCA).'' We noted that the new subpart consists of three sections, § 171.400 ''availability and effect of exceptions,'' which mirrors §§ 171.200 and 171.300, stating that a practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision as set forth in subpart D by meeting all applicable requirements and conditions of the exception at all relevant times (89 FR 1388). We reserved § 171.401 for definitions in a future rulemaking, and also reserved § 171.402 for future use. In § 171.403 we finalized a new TEFCA Manner Exception based on the *TEFCA manner* condition we proposed in HTI–1 Proposed Rule.

a. Definitions

We stated that while we reserved § 171.401 for possible future use as a ''definitions'' section, we declined to finalize any definitions in the HTI–1 Final Rule and instead referred readers to the definitions in the most recent version of the Common Agreement (88 FR 76773) for the terms relevant to the new exception (89 FR 1388). For example, when we refer to Framework Agreement(s), we mean any one or combination of the Common Agreement, a Participant-QHIN Agreement, a Participant-Subparticipant Agreement, or a Downstream Subparticipant Agreement, as applicable (86 FR 76778). We noted that this approach would allow us to maintain consistency and harmony between the Common Agreement and the new subpart D regulatory text.

We now propose to include definitions in § 171.401 by cross-referencing the TEFCA definitions included in the proposed new 45 CFR part 172, ''Trusted Exchange Framework and Common Agreement'' (see section IV.B.5.a of this proposed rule). We specifically propose to adopt in § 171.401 the definitions from § 172.102 for the following terms: Common Agreement, Framework Agreement, Participant, QHIN™, and Subparticipant. The definitions would apply to all of Subpart D. We welcome comment on this approach.

b. TEFCA™ Manner Exception

As briefly discussed above, we finalized a new TEFCA Manner Exception in the HTI–1 Final Rule. We stated that the new TEFCA Manner Exception (§ 171.403) provides that an actor's practice of limiting the manner in which it fulfills a request to access, exchange, or use EHI to be providing such access, exchange, or use to only via TEFCA will not be considered information blocking when it follows certain conditions (89 FR 1388). Those conditions require that (1) the actor and requestor both be part of TEFCA; (2) that

the requestor is capable of such access, exchange, or use of the requested EHI from the actor via TEFCA; and (3) any fees charged by the actor and the terms for any license of interoperability elements granted by the actor in relation to fulfilling the request are required to satisfy, respectively, the Fees Exception (§ 171.302) and the Licensing Exception (§ 171.303). In addition to these three requirements, we also included a limitation in § 171.403(c), stating that the exception is available only if the request is not made via the standards adopted in 45 CFR 170.215, which include the FHIR API standards.

Our finalized TEFCA Manner Exception differed from the proposed *TEFCA manner* condition in two ways. First, when we proposed the *TEFCA manner* condition, we stated that the Fees Exception and the Licensing Exceptions would not apply, because ''we mistakenly assumed that all actors participating in TEFCA would have *already* reached overarching agreements on fees and licensing such that there would be no need for application of the Fees and Licensing Exceptions (See 88 FR 23872)'' (89 FR 1389). We believe that by soliciting comments specifically on this point we provided notice to parties that we either would or would not apply the Fees and Licensing Exceptions. In response to our proposal, some commenters expressed concern that because the Common Agreement prohibits fees between QHINs™ but is otherwise silent on fees between Participants and Subparticipants, the proposal could allow actors to charge fees to access, exchange, or use EHI that did not comply with the Fees or Licensing Exceptions. Some commenters also expressed that this could have the effect of disincentivizing participation in TEFCA, and could cause actors to use other options of electronic exchange outside of TEFCA, where the actors believed the Fees and Licensing Exceptions would apply. As such, in the HTI–1 Final Rule, we finalized the TEFCA Manner Exception to include that any fees charged by the actor, and any licensing of interoperability elements, must satisfy the Fees Exception (§ 171.302) and the Licensing Exception (§ 171.303) (89 FR 1389). While we continue to believe that it was clear that the alternative would be *to* apply the exceptions, we are requesting comment now on whether there are drawbacks to applying the Fees and Licensing Exceptions, and if we should continue to apply them to the TEFCA Manner Exception as currently required in § 171.403(d).

The other change made to the proposed *TEFCA manner* condition was the limitation that carves out requests made for access, exchange, or use of EHI via FHIR API standards (89 FR 1389). We finalized this limitation in response to comments noting that a request could be made for access, exchange, or use via FHIR-based API and an actor could respond in a different manner and satisfy the exception (89 FR 1390 through 91). Commenters further noted that this potential outcome could undermine our stated purpose in incentivizing TEFCA participation with the new exception (See 89 FR 1390). We now solicit comment on this limitation within the TEFCA Manner Exception for requests via FHIR API standards. For example, should the limitation be expanded to include exchange based on versions of the FHIR standards that are more advanced than those adopted in 45 CFR 170.215 or approved through the 45 CFR 170.405(b)(8) ''Standards Version Advancement Process—voluntary updates of certified health IT to newer versions of standards and implementation specifications''? Currently, the limitation would only cover requests made via FHIR API standards codified in § 170.215, including standards that may be updated from time to time through § 170.405(b)(8), which may involve a delay before the version is formally approved under Standards Version Advancement Process (SVAP).

We also seek comment on a different approach. Eventually all TEFCA QHINs will be required to support exchange via FHIR API standards. A Participant or Subparticipant who makes a request for access, exchange, or use of EHI via FHIR API will at first make such a request through a QHIN, but in time, a Participant or Subparticipant could directly request access, exchange, or use of EHI via FHIR API standards from another Participant or Subparticipant in a different QHIN. One option would be to sunset the limitation in § 171.403(c) once all QHINs can support brokered FHIR. Another option would be to sunset the limitation in § 171.403(c) if all QHINs, Participants and Subparticipants support facilitated FHIR exchange. As an alternative to these options, we could maintain the exception as is, regardless of FHIR API adoption among TEFCA entities. We request comment on all of the options, including whether or not the limitation should remain as it is currently.

V. Trusted Exchange Framework and Common Agreement™

Section 3001(c)(9)(B)(i) of the PHSA provides the National Coordinator with the authority to ''develop or support a trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information networks.'' The components of this Trusted Exchange Framework and Common Agreement™ (TEFCA™) include the Trusted Exchange Framework (a common set of principles designed to facilitate trust between HINs) and the Common Agreement (the agreement Qualified Health Information Networks™ (QHINs™) sign), which includes, among other provisions, privacy, compliance, and security requirements). The Common Agreement also references the QHIN Technical Framework (QTF) (which describes technical requirements for exchange among QHINs) as well as, where necessary, standard operating procedures (SOPs). These documents further the statute's overall goal of ensuring full network-to-network exchange of health information by establishing a governance, policy, and technical floor for nationwide interoperability and securely facilitating the exchange of information across different networks nationwide.

By providing a common and consistent approach for the exchange of health information across many different networks, TEFCA simplifies and significantly reduces the number of separate networks of which individuals, health care providers, and other interested parties need to be a part of in order to access the health information they seek. TEFCA establishes a method for authenticating trusted health information network participants, potentially lowering the cost and expanding the nationwide availability of secure health information exchange capabilities. The establishment of technical services for health information networks that voluntarily join TEFCA creates interoperability at scale nationwide. These technical services, such as an electronic address directory and security services, will be critical to scale network exchange. In addition, the organizational and operational policies established through TEFCA enable the exchange of health information among health information networks and include minimum conditions required for such exchange to occur. Health information networks that voluntarily join TEFCA will facilitate exchange in a secure and interoperable manner. Updates in Common Agreement Version 2.0 reflect the latest technical specifications, among other changes, including updates to network-based exchange using FHIR® APIs, which are a cornerstone of the interoperability initiatives of not only ONC but also of other Federal agencies such as CMS, the

CDC, HRSA, and the U.S. Department of Veterans Affairs Veterans Affairs.

Under TEFCA, QHINs play an important role in advancing secure, standardized health information exchange. QHINs have significant organizational and technical capabilities, facilitate exchange at the highest level of the TEFCA infrastructure, and are the entities with which Participants (and their Subparticipants) interact in order to engage in TEFCA Exchange. ''TEFCA Exchange,'' which we propose to define in § 172.102, means the transaction of electronic protected health information (ePHI) between Nodes [255] using a TEFCA-specific purpose of use code, meaning a code that identifies the Exchange Purpose for which exchange is occurring. QHINs voluntarily agree to follow certain organizational and operational policies that allow Participants (entities who have entered into an agreement with the QHIN that includes the Participant/Subparticipant Terms of Participation) and Subparticipants (entities that have entered into an agreement with a Participant or other Subparticipant that includes the Participant/Subparticipant Terms of Participation) to simplify their operations and promote efficiency of scale.

QHINs must meet policy and technical requirements under the Common Agreement. The QTF and SOPs provide additional information on how QHINs meet those requirements. If finalized, QHINs will have to comply with the provisions proposed in this proposed rule. QHINs also perform a vital role by ensuring that Participants and Subparticipants meet the requirements of TEFCA.

We propose to establish rules in 45 CFR part 172 to implement our obligations under section 3001(c)(9)(D) of the PHSA to publish a directory of health information networks that ''have adopted the common agreement and are capable of trusted exchange pursuant to the common agreement'' and to establish a process through notice-and-comment rulemaking for health information networks to attest to adopting the Trusted Exchange Framework and Common Agreement. These regulations would further our obligations to ''support'' TEFCA under sections 3001(c)(9)(A) and (B) of the PHSA. The provisions included in this proposed rule would establish the qualifications for health information networks to receive and maintain Designation as a QHIN capable of trusted exchange pursuant to TEFCA, as well as establish procedures governing QHIN Onboarding and Designation, suspension, termination, and administrative appeals to ONC as described in the sections below. We believe establishing these provisions in regulation would strengthen the trust of interested parties in TEFCA and support its success at scale.

A. Subpart A—General Provisions

For the purposes of subpart A, we propose in § 172.100 the basis, purpose, and scope for the proposed TEFCA provisions in part 172 of Title 45 of the Code of Federal Regulations. We propose in § 172.100(a) that the basis for these provisions would be to implement section 3001(c)(9) of the PHSA (42 U.S.C 300jj–11(c)(9)). We propose in § 172.100(b) the dual purposes of proposed part 172: (1) to ensure full network-to-network exchange of health information; and (2) to establish a voluntary process for QHINs to attest to adoption of the Trusted Exchange Framework and Common Agreement. Section 172.100(b)(1) supports the statutory basis because the organizational and operational policies covered by part 172 would enable the exchange of health information among health information networks using the common set of rules found in these regulations. Section 172.100(b)(2) supports the statutory basis because it implements PHSA § 3001(c)(9)(D). We propose in § 172.100(c) the scope for part 172, which would include: (1) minimum qualifications needed to be Designated as a QHIN capable of trusted exchange under TEFCA; (2) procedures governing QHIN Onboarding and Designation, suspension, termination, and further administrative review; (3) attestation submission requirements for a QHIN to attest to its adoption of TEFCA; and (4) ONC attestation acceptance and removal processes for publication of the list of attesting QHINs in the QHIN Directory. In proposed § 172.101, we specify the applicability of part 172 by proposing that part 172 would apply only to Applicant QHINs, QHINs, and terminated QHINs. We note that our proposed QHIN definition in § 172.102 captures suspended QHINs (since a suspended QHIN is still a QHIN) and so we do not address them separately in proposed § 172.101. In § 172.102, we propose definitions for certain terms in part 172. We intend for the definitions provided in the Common Agreement to be consistent with these proposed definitions. Differences in phrasing would generally be attributable to differences in context, though in the case of any true conflict, we would intend for the regulatory definitions to control.

Additionally, ONC has hired a contractor to help administer and implement TEFCA Exchange. This contractor, chosen through a competitive solicitation, is known as the Recognized Coordinating Entity® (RCE™). While the RCE is currently one entity, in the future, ONC may choose to assign some or all of its responsibilities to a different entity or multiple entities. Assigning to a different or multiple entities in the future could, for example, allow for more efficient use of resources or best leverage expertise. In § 172.103, ''Responsibilities ONC may delegate to the RCE,'' we propose that ONC may assign certain responsibilities to such an entity or entities for these purposes. Specifically, we propose in § 172.103(a)(1)–(4) that ONC may assign any of its responsibilities in Subpart C—QHIN Onboarding and Designation Process; Subpart D—Suspension, § 172.501 QHIN self-termination, and § 172.503 Termination by mutual agreement. In § 172.103(b), we propose that any authority exercised by the RCE under this section is subject to review by ONC under Subpart F (''Review of RCE Decisions''). For further discussion of the current RCE and the authority it exercises on behalf of ONC, please see the discussion in ''*C. Subpart C—QHIN Onboarding and Designation Processes*'' below.

B. Subpart B—Qualifications for Designation

In subpart B, we propose qualifications for Designation. In § 172.200, we propose to tie QHIN status to meeting the requirements specified in § 172.201. We propose that an Applicant QHIN (as we propose to define it in § 172.102) would need to meet all requirements in § 172.201 to be *Designated,* and a QHIN would need to continue to meet all requirements in § 172.201 to *maintain its Designation.* That means that the requirements we propose in § 172.201 would be ongoing; a QHIN that does not meet those requirements at all times would be subject to suspension or termination, consistent with the regulations we propose in subparts D and E of part 172. Among other benefits, the continuing obligation to meet the requirements in § 172.201 would help to ensure the reliability of TEFCA Exchange and to ensure QHINs could not maintain their status based on technology and standards that have become obsolete. Because the obligations would be

[255] Node: a technical system that is controlled directly or indirectly by a QHIN, Participant, or Subparticipant and that is listed in the RCE Directory Service.

ongoing, throughout this section we refer to Applicant QHINs as well as Designated QHINs as ''QHINs'' unless there is a need to differentiate.

As we explain below, the Designation qualifications proposed in § 172.201 would describe certain requirements for Designation. For an entity to become a QHIN, that entity must sign the Common Agreement, thus memorializing its agreement to the comprehensive Designation requirements—as well as other requirements—for trusted exchange under TEFCA. The comprehensive Designation requirements in the Common Agreement correspond to the proposed requirements included in this subpart.

In § 172.201, we propose Designation requirements in three categories: (a) ownership; (b) exchange requirements; and (c) Designated Network Services.

In § 172.201(a), we propose the ownership requirements. In § 172.201(a)(1), we propose that a QHIN must be a U.S. Entity, as we propose to define *U.S. Entity/Entities* in § 172.102. Under that proposed definition, a U.S. Entity must be a corporation, limited liability company, partnership, or other legal entity organized under the laws of a State or commonwealth of the United States or the Federal law of the United States, be subject to the jurisdiction of the United States and the State or commonwealth under which it was formed, and have its principal place of business be in the United States under Federal law. Additionally, we propose that none of the entity's directors, officers, or executives, and none of the owners with a five percent (5%) or greater interest in the entity, may be listed on the *Specially Designated Nationals and Blocked Persons List* published by the United States Department of the Treasury's Office of Foreign Asset Control or on the Department of Health and Human Services, Office of Inspector General's List of Excluded Individuals/Entities. This requirement would help to promote organizational and operational policies that enable the exchange of health information among networks by ensuring that those who actually control the health information exchanged under these provisions are subject to U.S. laws, and it would help to avoid giving access to that information to actors whom the government has previously identified as national security or fraud risks.

We request comment on whether the above approach, including the specific five percent (5%) threshold, will effectively limit access of bad actors trying to join TEFCA as a QHIN, or whether commenters believe the threshold should be a different percentage.

In § 172.201(a)(2), we propose that an Applicant QHIN must not be under Foreign Control, which is a term we propose to define in § 172.102. If, in the course of reviewing a QHIN application, ONC believes or has reason to believe the Applicant QHIN may be under Foreign Control, ONC will refer the case to the HHS Office of National Security (ONS) for review. If information available to ONS supports a determination of Foreign Control, ONS will notify ONC. An application will be denied if ONS notifies ONC that the Applicant is under Foreign Control. Given the scale of the responsibilities that a Designated QHIN would have with respect to supporting health information exchange and the importance that healthcare data has to the critical infrastructure of our nation's health care system, we believe that a QHIN should not be under Foreign Control. We believe the requirements proposed in § 172.201(a)(1) and (a)(2), in conjunction with the proposed definitions that those provisions reference, are necessary to ensure that all QHINs are subject to United States law and that compliance by QHINs is enforceable under United States law. Further, these proposals are designed to strengthen the security of the network. We believe that the above proposals promote organizational and operational policies that enable the exchange of health information among networks by minimizing the risk to TEFCA that may be posed by foreign state actors who wish to harm the United States, lessening the risks of subjecting QHINs to potentially conflicting foreign laws, and encouraging trust in the security of exchange under the system.

We note that within the proposed definition of *U.S. Entity/Entities* in § 172.102, we propose that for an entity seeking to become a QHIN to meet the definition, none of the entity's directors, officers, or executives, and none of the owners with a five percent (5%) or greater interest in the entity, can be listed on the *Specially Designated Nationals and Blocked Persons List* published by the United States Department of the Treasury's Office of Foreign Asset Control or on the Department of Health and Human Services, Office of Inspector General's List of Excluded Individuals/Entities. We believe the five percent (5%) threshold strikes the right balance between protecting the security of the network from high-risk or known bad actors and achieving practical administrability of TEFCA. Individuals with less than five percent (5%) ownership in an entity would likely have limited means of influencing the actions of an entity connected to TEFCA. We believe that entities—particularly those with a large number of shareholders—would face undue hardship without this sort of exception for small shareholders. That said, this regulation only would provide the standard that ONC will apply when evaluating QHINs; it would not supersede any stricter requirements imposed by other applicable laws, including, for example national security laws. It remains the responsibility of QHINs (and any other entity) to comply with all applicable laws.

In § 172.201(b), we propose exchange requirements for QHINs. We believe these exchange requirements are necessary to build a data sharing infrastructure that is private and secure and that meets all the requirements of PHSA section 3001(c)(9). We believe each of the exchange requirements below is important to the implementation and operationalization of TEFCA Exchange, as described in § 172.201, at scale. We propose that an entity seeking to become a QHIN must, beginning at the time of application, either directly or through the experience of its parent entity, meet certain exchange requirements, including: (1) be capable of exchanging information among more than two unaffiliated organizations; (2) be capable of exchanging all Required Information (as that term is defined in § 172.102); (3) be exchanging information for at least one of the Exchange Purposes (as that term is defined in § 172.102) authorized, in the Common Agreement or an SOP(s) n; (4) be capable of receiving and responding to transactions from other QHINs for all Exchange Purposes; and (5) be capable of initiating transactions for the Exchange Purposes that such entity will permit its Participants and Subparticipants to use through TEFCA Exchange. Collectively, we believe these requirements are tailored to help ensure that a QHIN is capable of TEFCA Exchange, supports a trusted exchange framework, and maintains consistent practices of exchanging information at scale to support nationwide interoperability.

The first requirement, proposed in § 172.201(b)(1), that the entity seeking to become a QHIN be capable of exchanging information among more than two unaffiliated organizations, is a requirement that would ensure a minimum technical ability exists and that exchange would be enabled beyond just the QHIN itself.

The second requirement, proposed in § 172.201(b)(2), is also a minimum condition, except it is directed at the minimum quantity of *data* a QHIN must be capable of exchanging. This proposed requirement would ensure that every QHIN can exchange Required Information (as that term is defined in § 171.102), and provides certainty to Participants and Subparticipants who seek to join a QHIN that there is a minimum scope of data that they can reliably expect to be able to exchange via TEFCA Exchange Purposes.

The proposed requirements in § 172.201(b)(3) through (5) are intended to establish basic parameters and expectations for QHINs in order to qualify for Designation. We propose, in § 172.201(b)(3), that a QHIN or Applicant QHIN must be exchanging information for at least one Exchange Purpose.

If a QHIN is not exchanging information for at least one of the Exchange Purposes authorized under TEFCA (for examples, see the ''Exchange Purpose'' definition in § 172.102) at the time of application, it is not meeting a minimum condition necessary for such exchange to occur and cannot be Designated. While exchange for an Exchange Purpose under TEFCA requires an Exchange Purpose Code, Applicant QHINs can demonstrate that they are meeting the requirement to exchange information for at least one of the Exchange Purposes by conducting exchange for an Exchange Purpose without use of an Exchange Purpose Code.

We propose in § 172.201(b)(4) to require a QHIN to be capable of receiving and responding to transactions from other QHINs for all Exchange Purposes, to ensure that health information can be exchanged among health information networks under TEFCA. For this same reason, we propose in § 172.201(b)(5) to require a QHIN to be capable of initiating transactions for the Exchange Purposes that such entity will permit its Participants and Subparticipants to use through TEFCA Exchange. Ensuring that QHINs will respond to Participant or Subparticipant requests for information, and that the Participants or Subparticipants are able to receive the information from QHINs, enables health information exchange among the QHINs, Participants and Subparticipants.

A QHIN's ability to transact for all Exchange Purposes is a threshold requirement for an entity that seeks Designation and is essential for ensuring that the TEFCA framework facilitates exchange for each Exchange Purpose authorized in the Common Agreement or an SOP(s) for implementation. Without this requirement, there would be no certainty that the TEFCA framework would advance exchange beyond the Treatment Exchange Purpose, which is the most prevalent purpose for health information exchange today and the purpose of use that most health care entities seeking Designation would be most familiar with. TEFCA's network connectivity, including this requirement that QHINs have the ability to exchange for all Exchange Purposes, and scale would help, for example, health care providers gain access to more comprehensive and complete information about their patients, which can support improved care, better outcomes, decreased provider burden, and reduced costs.

Entities performing TEFCA Exchange as described in § 172.201 will have the option to request information for all Exchange Purposes. At the time of publication of this Proposed Rule, TEFCA supports exchange for the following Exchange Purposes: treatment; payment; health care operations; public health; Individual Access Services (IAS), and government benefits determination. Over time, additional Exchange Purposes may be added. Information regarding whether responses are required for a given Exchange Purpose will be included in a TEFCA standard operating procedure.

In § 172.201(c), we propose that an Applicant QHIN must meet certain Designated Network Services requirements. Based on our experience in the health IT ecosystem, we believe adequate network performance is important for the success of TEFCA, as those participating in TEFCA Exchange would be most likely to trust the TEFCA infrastructure if it is performing at a high level. Unreliable network performance would dilute confidence in the network and discourage participation.

In § 172.201(c)(1), we propose that a QHIN must maintain the organizational infrastructure and legal authority to operate and govern its Designated Network. For instance, under this proposal, QHINs would be required to have a representative and participatory group or groups that approve the processes for fulfilling the TEFCA governance functions and that participate in governance for the Designated Network. In § 172.201(c)(2), we propose that a QHIN must maintain adequate written policies and procedures to support meaningful TEFCA Exchange as described in § 172.201 and fulfill all responsibilities of a QHIN in this part (which an entity agrees to by signing the Common Agreement). For instance, under this proposal, QHINs would be required to have a detailed written policy that describes the oversight and control of the technical framework that enables TEFCA Exchange.

In § 172.201(c)(3), we propose that a QHIN must maintain a Designated Network (as proposed to be defined in § 172.102) that can support a transaction volume that keeps pace with the demands of network users. Since TEFCA is a nationwide network and will be used daily to support various health data needs to inform care delivery, quality assessments, public health, and health care operations, QHINs must be capable of transacting high volumes of data reliably and at scale. In § 172.201(c)(4), we propose that a QHIN must maintain the capacity to support secure technical connectivity and data exchange with other QHINs. One of the most fundamental aspects of interoperable network exchange is technical connectivity, which makes network-to-network exchange possible and, therefore, is important to include in this regulation.

In §§ 172.201(c)(5)–(7), we propose certain requirements related to governance for TEFCA to ensure all QHINs are aligned and able to manage risk effectively. In § 172.201(c)(5), we propose that a QHIN must maintain an enforceable dispute resolution policy governing Participants in the Designated Network that permits Participants to reasonably, timely, and fairly adjudicate disputes that arise between each other, the QHIN, or other QHINs. This proposed requirement would afford flexibility to QHINs to establish their own dispute resolution process while ensuring the process is timely and fair. Disputes may arise for a variety of reasons, so the QHIN, as the entity overseeing its Participants, is best placed to handle such disputes in a way that minimizes disruptions for the rest of the network. Ensuring that a QHIN has such a dispute resolution policy would, therefore, likely minimize such disruptions. Similarly, in § 172.201(c)(6), we propose that a QHIN maintain an enforceable change management policy consistent with its responsibilities as a QHIN. A change management policy establishes the standard procedures to approve different types of changes to TEFCA documents (*e.g.,* standard operating procedures) and policies and will help to avoid changes that are disruptive or in conflict across entities. In § 172.201(c)(7), we propose that a QHIN must maintain a representative and participatory group or groups with the

authority to approve processes for governing the Designated Network. The participatory network governance built into the TEFCA infrastructure is important to ensure that the requisite engagement exists between QHINs, Participants, and Subparticipants participating in TEFCA Exchange. We believe the above requirements are fundamental aspects of a network-of-networks focused on participatory governance and the ability to adapt to an ever-changing health information exchange landscape.

Regarding the proposed requirement in § 172.201(c)(7) specifically, we emphasize that TEFCA uses a representative and participatory governance structure. Representative and participatory governance gives those participating in the network a role in informing the policies and decisions that ultimately would affect them. Such a governance structure helps to motivate health care entities and their networks to voluntarily join TEFCA. We believe that requiring a QHIN to have a representative and participatory group or groups that has the ability to review and provide input on the governance requirements of the QHIN's Designated Network is an optimal approach for this requirement.

In § 172.201(c)(8), we propose that an entity seeking to become a QHIN must maintain privacy and security policies that permit the QHIN to support TEFCA Exchange. These policies currently include, but are not limited to, the following:

- Maintaining certification under a nationally recognized security framework by a qualified, independent third party that ensures its assessments are consistent with the NIST Cybersecurity Framework (CSF) (using both NIST 800–171 (Rev. 2) and NIST 800–53 (Rev. 5) as a reference), that reviews the QHIN's HIPAA Security Rule risk analysis (consistent with § 164.308(a)(1)(ii)(A)), and verifies all requirements for technical audits and assessments are met.
- Having a qualified, independent third party complete an annual security assessment consistent with the NIST Cybersecurity Framework (CSF) (using both NIST 800–171 (Rev. 2) and NIST 800–53 (Rev. 5) as a reference). The third party would review the QHIN for compliance with HIPAA Security Rule risk analysis requirements consistent with § 164.308(a)(1)(ii)(A). Additionally, the annual security assessment must include comprehensive internet-facing penetration testing, must include an internal network vulnerability assessment, and must use methodologies and security controls consistent with Recognized Security Practices, as defined by Public Law No: 116–321 (42 U.S.C. 17931 and 300jj–52).
- Employing a Chief Information Security Officer with executive-level responsibility.
- Disclosing any breaches of electronic protected health information (including disclosure of any such breaches within the three (3) years preceding applying to become a QHIN) to the RCE and to all QHINs that are likely impacted;
- Complying with 45 CFR part 164, subparts A, C, and E, as applicable, as if the QHIN were a covered entity as described in that regulation; and
- Maintaining and complying with a written privacy policy.

These policies and requirements will provide privacy and security protections for the health information that will be exchanged through TEFCA. All entities that elect to participate in TEFCA, including entities not regulated under HIPAA, will be expected to meet a high bar for privacy and security given the nature of the data being exchanged. Further, the policies would advance TEFCA exchange by making it clear to those interested in participating that privacy and security measures are in place. It is unlikely that an entity would wish to participate in a network without privacy and security standards, thereby inhibiting TEFCA exchange.

To further support the security of TEFCA, we propose in § 172.201(c)(9), that a QHIN must maintain data breach response and management policies that support secure TEFCA Exchange. For instance, given the number of electronic connections TEFCA will support, a data breach response and management policy would support a transparent process and timely awareness of a data breach or other security events (*e.g.,* ransomware attacks) which could enable the QHIN to manage secure connectivity services without disrupting patient care. These proposed policies and requirements reflect the available privacy and security standards.

In § 172.201(c)(10), we propose that a QHIN must maintain adequate financial and personnel resources to support all its responsibilities as a QHIN, including, at a minimum, sufficient financial reserves or insurance-based cybersecurity coverage, or a combination of both. This requirement will help to provide stability to TEFCA in the event of unexpected financial or economic occurrences—whether system-wide or specific to individual QHINs.

For instance, this requirement could be met if the QHIN has available a minimum amount of cash, cash equivalents, borrowing arrangements (*e.g.,* a line of credit) or a mix of the three that is equal to six (6) calendar months of operating reserves. Regarding insurance requirements, a QHIN's general liability coverage and the cyber risk/technology coverage should each have limits of at least $2,000,000 per incident and $5,000,000 in the aggregate, which limits can be met through primary coverage, excess coverage, available internal funds, or a combination thereof. We note that the requirements proposed here may be insufficient for larger QHINs, and recognize that certain QHINs will meet and exceed these minimums.

QHINs will be the central connection points for TEFCA Exchange, responsible for routing queries, responses, and messages among many participating entities and individuals. We propose, in § 172.201(c)(10), that QHINs must have sufficient financial resources and personnel capacity to perform such functions successfully. We also believe that QHINs must be prepared to address incidents should they arise and must have the ability to fulfill potential liability obligations, either through insurance, sufficient financial reserves, or some combination of the two.

One goal of TEFCA is to support patients gathering their healthcare information. In § 172.202, ''QHINS that offer individual access services,'' we propose Individual Access Services (IAS) requirements for a QHIN to obtain and maintain Designation under TEFCA if that QHIN voluntarily offers IAS. In § 172.202(a), we propose that a QHIN would be required to obtain express consent from any individual before providing IAS, as defined in § 172.102. We believe this is an important requirement so that individuals who use IAS that a QHIN offers are informed of the privacy and security practices that are being employed to protect their data. In § 172.202(b), we propose that a QHIN would be required to make publicly available a privacy and security notice that meets minimum TEFCA privacy and security standards to support transparent exchange practices. We believe this requirement would provide transparency to all individuals who are considering using IAS regarding how their data is protected and secured by a QHIN providing IAS.

In § 172.202(c), we propose a QHIN that is the IAS provider for an individual, would be required to delete the individual's Individually Identifiable Information (as defined in § 172.102) maintained by the QHIN upon request by the individual except as prohibited by Applicable Law or where such information is contained in

audit logs. We believe this requirement would provide individuals with reassurance that they control access to their data. We believe the carve out for audit logs is appropriate because audit logs are generally used to provide chronological records of system activities and should not be deleted. In § 172.202(d), we propose that a QHIN would be required to permit any individual to export in a computable format all of the individual's Individually Identifiable Information maintained by the QHIN as an IAS provider. We believe this requirement would ensure that individuals may access, control, and use their own data held by an IAS provider.

In § 172.202(e), we propose that all Individually Identifiable Information the QHIN maintains must satisfy certain criteria, including: (1) all Individually Identifiable Information must be encrypted; (2) without unreasonable delay and in no case later than sixty (60) calendar days following discovery of the unauthorized acquisition, access, Disclosure, or Use of Individually Identifiable Information, the QHIN must notify, in plain language, each individual whose Individually Identifiable Information has been or is reasonably believed to have been affected by unauthorized acquisition, access, Disclosure, or Use involving the QHIN; and (3) a QHIN must have an agreement with a qualified, independent third-party credential service provider and must verify, through the credential service provider, the identities of individuals seeking IAS prior to the individuals' first use of such services and upon expiration of their credentials. We note that to the extent the QHIN is already required by Applicable Law to notify an individual as described in proposed § 172.202(e)(2), we are not proposing that it be required to duplicate such a notification. Lastly, the proposed requirement in § 172.202(e)(3) would set a baseline for proving the identity of IAS users that are requesting data via TEFCA Exchange.

In some ways, IAS providers—should we finalize these proposals in § 172.202—would meet requirements above and beyond what the HIPAA Rules require of covered entities or business associates, including providing individuals with the right to delete their data and a requirement to encrypt all Individually Identifiable Information, as we propose in § 172.202(c) and § 172.202(e)(1). Encryption is an industry standard practice to protect data, and we believe the requirement we propose in § 172.202(e)(1) would create strong security of data while not creating undue burden to implement. We believe these proposed requirements are important because IAS providers will not always be HIPAA covered entities or business associates. Establishing these IAS requirements would ensure that QHINs that are IAS providers will meet certain minimum privacy and security requirements to protect patient data while also advancing the goal of improving patients' ability to access their data.

We welcome comments on the proposed qualifications and requirements in this subpart.

C. Subpart C—QHIN™ Onboarding and Designation Processes

TEFCA establishes a universal floor for interoperability across the country through a network of networks. In 2019, ONC issued a Notice of Funding Opportunity and subsequently awarded a cooperative agreement to The Sequoia Project to serve as the RCE to support the implementation of TEFCA. In August 2023, ONC awarded The Sequoia Project a five-year contract to continue serving as the RCE.

To establish nationwide health information exchange, TEFCA calls for the Designation of QHINs—HINs that agree to the common policy, functional, and technical requirements for TEFCA Exchange. The QHIN Designation Requirements as described in § 172.201 define the baseline legal and technical requirements for secure information sharing on a nationwide scale—all under commonly agreed-to rules. Exchange through TEFCA simplifies connectivity and creates efficiency by establishing a standardized approach to exchange policies and technical frameworks.

Under the 2019 to 2023 cooperative agreement [256] and the current RCE contract,[257] the RCE's role has been to support the implementation of TEFCA, including the solicitation and review of applications from HINs seeking QHIN status and administration of the Designation and monitoring processes. For entities seeking Designation, the application provides the RCE with the information needed to determine a prospective QHIN's ability to meet its obligations and responsibilities for TEFCA Exchange. All work or activities conducted by the Sequoia Project in their capacity as the RCE under the RCE contract, including work or activities related to Designation, is conducted on behalf of ONC.

In subpart C of part 172, we describe the proposed QHIN Onboarding and Designation processes. *Onboarding,* as we propose to define it in § 172.102, is the process a prospective QHIN must undergo to become a QHIN and become operational in the production environment.[258] *Designation,* on the other hand, we propose to define in § 172.102, as the written determination that an Applicant QHIN has satisfied all regulatory requirements and is now a QHIN.[259]

In § 172.300, we explain that subpart C of part 172 would establish, for QHINs, the application, review, Onboarding, withdrawal, and redetermination processes that ONC will follow for Designation. Establishing these processes will ensure that ONC (or an RCE) takes a consistent approach to QHIN Onboarding and Designation.

The first step in becoming a QHIN under TEFCA is submission of an application. In § 172.301, we propose to establish the information Applicant QHINs must submit in order to be Designated as a QHIN. We propose that an Applicant QHIN must submit: (1) a completed QHIN application; and (2) a signed copy of the Common Agreement. Regarding the first proposed requirement, in § 172.301(a), the application may be updated over time and the most recent version will be available on ONC's and the RCE's website. The application will specify what supporting documentation an Applicant QHIN must submit. We propose the second requirement in § 172.301(b) because the Applicant QHIN would sign the Common Agreement upon application, but the RCE would only countersign and create a binding agreement with the Applicant QHIN once the Applicant QHIN completes Onboarding and is Designated.

The next step to becoming a QHIN is application review. In § 172.302, we propose a process, with required timelines and allowable extensions, for ONC (or an RCE) to review applications. We propose in § 172.302(a) that, on receipt of an application, ONC (or an RCE) will review the application to determine if the Applicant QHIN has completed all parts of the application and provided the necessary supporting documentation. Further, we propose that, if the QHIN Application is not complete, ONC (or an RCE) will notify the applicant in writing of the missing

[256] Notice of Funding Opportunity (NOFO)—Trusted Exchange Framework and Common Agreement—Recognized Coordination Entity (RCE) Cooperative Agreement, *https://www.healthit.gov/sites/default/files/facas/TEFCA%20NOFO_FINAL_508.pdf.*

[257] *See USASPENDING.gov, https://www.usaspending.gov/award/CONT_AWD_75P00123C00019_7570_-NONE-_-NONE-.*

[258] 87 FR 2822.

[259] 87 FR 2818.

information within thirty (30) calendar days of receipt of the application. Last, we propose that ONC (or an RCE) may extend this period by providing written notice to the Applicant QHIN. We note that ''written notice'' throughout part 172 would include notice provided by email to the points of contact the Applicant QHIN listed in their application.

We believe the above timeframe and allowable extensions would allow ONC (or an RCE) enough time to perform a thorough review of each application and ensure that ONC (or an RCE) is provided with the responses and supporting documentation needed to assess the merits of an application. We believe the 30-day review timeframe—along with the ability of ONC (or an RCE) to extend this period by providing written notice to the Applicant QHIN—strikes the right balance between moving an application forward as quickly as possible while still providing ONC (or an RCE) with enough time to conduct a review of the application to ensure it is complete and contains all the required material.

We propose in § 172.302(b) that once the QHIN application is complete, ONC (or an RCE) will review the application to determine whether the Applicant QHIN satisfies the requirements for Designation set forth in § 172.201, and, if the Applicant QHIN proposes to provide IAS, the requirements set forth in § 172.202. We propose this step to make clear that ONC (or an RCE) will review an application not only for completeness but also to determine if the qualifications are met. We also propose ONC (or an RCE) would complete its review within sixty (60) calendar days of providing the Applicant QHIN with written notice that its application is complete. We further propose that ONC (or an RCE) may extend this period by providing written notice to the Applicant QHIN. We believe that sixty (60) calendar days will *generally* be an adequate amount of time to conduct a thorough, comprehensive review of the substance of the application. However, we are cognizant that there may be complex applications that require additional time for review and have, therefore, proposed that ONC (or an RCE) may extend this period by providing written notice to the Applicant QHIN.

We propose in § 172.302(c) that ONC (or an RCE) may contact the Applicant while the application is being reviewed to request additional information. ONC (or an RCE) will provide the timeframe for responding to its request and the manner to submit additional information, which may be extended on written notice to the Applicant QHIN. We believe this provision would be beneficial because the Applicant QHIN will need to provide detailed responses that may be complex and will vary among Applicant QHINs. We anticipate there will often need to be a discussion between ONC (or an RCE) and the Applicant QHIN to reach a resolution and shared understanding. This provision would provide for this vital communication between ONC (or an RCE) and the Applicant QHINs. We propose that an Applicant QHIN must respond to ONC (or an RCE) within the timeframe ONC (or an RCE) identifies because ONC (or an RCE) will be in the best position to understand the complexity of the question and estimate a reasonable amount of time for the Applicant QHIN to respond. That said, we understand that each application, as well as the questions associated with each application, will vary significantly on a case-by-case basis and, therefore, are proposing that ONC (or an RCE) may extend the timeframe by providing written notice to the Applicant QHIN. We believe this approach creates appropriate flexibility regarding timing of Applicant QHIN responses, while still leaving the discretion to decide the need for and length of such extensions.

We propose in § 172.302(d) that failure to respond to a request within the proposed timeframe, or in the manner specified, is a basis for a QHIN Application to be deemed withdrawn, as set forth in § 172.305(c)). In such situations, we propose that ONC (or an RCE) would provide the Applicant QHIN with written notice that application has been deemed withdrawn. We believe this requirement is important to support an efficient application process and to ensure that Applicant QHINs respond to requests in a timely manner. We reiterate that under proposed § 172.302(c), as discussed above, the ONC (or an RCE) can extend the timeframe for responding to a request for information. An Applicant QHIN should request an extension if it does not believe it can meet the proposed response timeframe.

We propose in § 172.302(e) that if, following submission of the application, any information submitted by the Applicant QHIN becomes untrue or materially changes, the Applicant QHIN must notify ONC (or an RCE), in the manner specified by ONC (or an RCE), of such changes in writing within five (5) business days of the submitted material becoming untrue or materially changing. This proposed requirement takes into consideration the possibility that, over the course of ONC's (or an RCE's) review of an application, an Applicant QHIN's circumstances or information provided with the Applicant QHIN's application may change. This provision would ensure that if such changes occur, the Applicant QHIN would promptly notify ONC (or an RCE) of such changes. We believe, based on ONC's experience with health IT implementation and coordination efforts, that five (5) business days is enough time for the Applicant QHIN to notify ONC (or an RCE) of the change(s).

In § 172.303, we propose requirements related to QHIN approval and Onboarding. We propose in § 172.303(a) that an Applicant QHIN would have the burden of demonstrating its compliance with all qualifications for Designation in § 172.201, and, if the Applicant QHIN proposes to provide IAS, the qualifications in § 172.202. We propose in § 172.303(b) that if ONC (or an RCE) determines an Applicant QHIN meets the requirements for Designation set forth in § 172.201, and, if the Applicant QHIN proposes to provide IAS, the qualifications set forth in § 172.202, then ONC (or an RCE) will notify the Applicant QHIN in writing that it has approved its application, and the Applicant QHIN can proceed with Onboarding. These proposed requirements are important for ensuring that the Applicant QHIN is notified of its status and support the transparency and efficiency of the Onboarding process.

We propose in § 172.303(c) that an approved Applicant QHIN would be required to submit a signed version of the Common Agreement within a timeframe set by ONC (or an RCE). This proposed provision is important in addition to § 172.301(b) (which would require an Applicant QHIN to submit a signed version of the Common Agreement when applying) to ensure that, if the Common Agreement changes between the time the QHIN applies and when it is approved, the QHIN will have signed the most recent version. We did not propose a specific timeframe for submission, and instead propose to allow ONC (or an RCE) to set the timeframe for each Applicant QHIN, since we believe each timeframe should be tailored to the needs of the Applicant QHIN and the complexity of each application.

We propose in § 172.303(d) that an approved Applicant QHIN must complete the Onboarding process set forth by ONC (or an RCE), including any tests required by ONC (or an RCE) to ensure the Applicant QHIN's network can connect to those of other QHINs, within twelve (12) months of approval of the QHIN application, unless that

time is extended in ONC's (or an RCE's) sole discretion by up to twelve (12) months. Based on ONC's experience with health IT implementation and discussions with the current RCE, we believe the proposed twelve (12) month timeframe is sufficient time for approved Applicant QHINs to complete the Onboarding process including any tests with QHINs and other Applicant QHINs. We believe that timeframe strikes an appropriate balance between the need to onboard QHINs promptly and the need to ensure that all QHINs can connect immediately and seamlessly once Designated. We note that during the Onboarding process, the Applicant QHIN would have regular check-ins with ONC (or an RCE) to monitor the progress on any outstanding requirements, to coordinate technical testing, and to address any issues that could put the Applicant QHIN in jeopardy of failing to meet the proposed Onboarding timeframe detailed above.

In § 172.304, we propose the specific procedural requirements for the Designation of QHINs. In § 172.304(a), we propose the process that would follow an Applicant QHIN's satisfaction of the Onboarding process requirements. We propose that once the Onboarding process requirements are satisfied, the Common Agreement would be countersigned and the Applicant QHIN would receive a written determination indicating that it had been provisionally Designated as a QHIN, along with a copy of the countersigned Common Agreement.

In § 172.304(b), we propose that within thirty (30) calendar days of receiving its written determination of provisional Designation, each QHIN would be required to demonstrate in a manner specified by ONC (or an RCE) that it has completed a successful transaction with all other in-production QHINs according to standards and procedures for TEFCA Exchange. This proposed provision is important because it would ensure that a Designated QHIN is able to exchange information with other QHINs, which is a core function of QHINs. We believe that the thirty (30)-day timeframe will afford a Designated QHIN ample time to move from testing to production. We also believe that the standards and procedures for such exchanges should remain flexible such that ONC (or an RCE) may update the requirements from time to time as appropriate.

We propose in § 172.304(c) that if a QHIN is unable to complete the requirement in § 172.304(b), described above, within the thirty (30)-day period provided, the QHIN would be required to provide to ONC (or an RCE) with a written explanation as to why the QHIN is unable to complete the requirement within the allotted time and include a detailed plan and timeline for completion of the requirement. We propose that ONC (or an RCE) will then review and approve or reject the QHIN's plan, basing its decision on the reasonableness of the explanation based on the specific facts and circumstances, within five (5) business days of receipt. We propose that if the QHIN fails to provide ONC (or an RCE) its plan or ONC (or an RCE) rejects the QHIN's plan, ONC (or an RCE) will rescind its approval of the application, rescind the provisional QHIN Designation, and deny the application. We believe these proposals would provide QHINs with the appropriate flexibility to request an extension if the circumstances do not allow the QHIN to meet the timeline. We believe the proposed five (5)-business day timeframe would provide ONC (or an RCE) with enough time to review the request and reach a decision regarding the request based on the information provided. We propose that within thirty (30) calendar days of the end of the term of the plan, each QHIN must demonstrate in a manner specified by ONC (or an RCE) that it has completed a successful transaction with all other in-production QHINs according to standards and procedures for TEFCA Exchange. We believe that the thirty (30)-day timeframe will afford a Designated QHIN ample time to move from testing to production.

In § 172.304(d), we propose that a QHIN Designation will become final sixty (60) days after a Designated QHIN has submitted its documentation, in a manner specified by ONC (or an RCE), that it has completed a successful transaction with all other in-production QHINs. This proposal will allow ONC (or an RCE) to exercise its ability to review a Designation.

In § 172.305, we propose requirements related to withdrawal of an application. In § 172.305(a), we propose that an Applicant QHIN may withdraw its application by providing ONC (or an RCE) with written notice in a manner specified by ONC (or an RCE). In § 172.305(b), we propose that an Applicant QHIN may withdraw its application at any point prior to Designation. In § 172.305(c), we propose that on written notice to the Applicant QHIN, an application may be deemed as withdrawn as a result of the Applicant QHIN's failure to respond to requests for information from ONC (or an RCE). We believe the approach in proposed § 172.305 would create an efficient process for ONC (or an RCE) to deem applications withdrawn if an Applicant QHIN fails to respond to requests for information, and also supports a flexible process by allowing an Applicant QHIN, for whatever reason, to decide to withdraw its application without penalty. Given the requirements placed on Applicant QHINs seeking to be Designated, we think it is reasonable to believe that some Applicant QHINs will need to withdraw their applications to address any number of issues that could arise during the application process.

In § 172.306, we propose that if an Applicant QHIN's application is denied, the Applicant QHIN will be provided with written notice that includes the basis for the denial. We do not propose a specific template that would be used to explain the basis of a denial, as such explanation would likely vary based on the specific facts and circumstances.

In § 172.307, we propose requirements for re-application. In § 172.307(a), we propose that Applicant QHINs may resubmit their applications by complying with the provisions of § 172.301 in the event that an application was denied or withdrawn. We note that re-application pursuant to § 172.307(a) would also be conditioned on meeting the requirements of proposed paragraphs (b)–(d) of § 172.307, as applicable. We propose in § 172.307(b) that an Applicant QHIN may reapply at any time after it has voluntarily withdrawn its application as specified in § 172.305(a). We want to create flexibility for Applicant QHINs to reassess their applications and, if desired, resubmit the application. We also believe that providing an Applicant QHIN that withdraws its application with discretion to choose when to re-apply would result in better applications and create administrative efficiency. This is because Applicant QHINs would be motivated to self-identify issues and correct them in a subsequent application. Also, Applicant QHINs that withdraw applications early would allow ONC (or an RCE) to avoid expending resources to review and identify such issues.

In § 172.307(c), we propose that if ONC (or an RCE) deems an application to be withdrawn as a result of the Applicant QHIN's failure to respond to requests for information from ONC (or an RCE), then the Applicant QHIN may reapply by submitting a new application no sooner than six (6) months after the date on which its previous application was submitted. We propose that the Applicant QHIN must respond to the prior request for information and must include an explanation as to why no response was previously provided within the required timeframe. We propose in § 172.307(d) that if ONC (or

an RCE) denies an application, the Applicant QHIN may reapply by submitting a new application consistent with the requirements in § 172.301, no sooner than six (6) months after the date shown on the written notice of denial. The application must specifically address the deficiencies that constituted the basis for denying the Applicant QHIN's previous application. We believe that six (6) months is an appropriate minimum time period for re-application because we would expect the Applicant QHIN to take such time to reconsider and address the deficiencies in its application. Our goal with such proposed requirements is that the Applicant QHIN will be thoughtful about its new application and will work to address the problems with its initial application.

We believe the proposed six (6)-month minimum time period before re-application, in § 172.307(c) and (d), would support efficiency in the review process, as ONC (or an RCE) could shift its attention to other Applicant QHINs or issues while the Applicant QHIN whose application was withdrawn as a result of the Applicant QHIN's failure to respond to requests for information or denied reconsiders its application and addresses the previously identified deficiency or deficiencies. These requirements would also support efficiency in the application process, as ONC (or an RCE) should only allocate resources to review a re-application if the Applicant QHIN has clearly addressed outstanding questions and previously identified deficiencies. On the other hand, we believe that if an Applicant QHIN withdraws its application, then the Applicant QHIN is best positioned to determine when it is ready to re-apply. Because the Applicant QHIN that withdraws its application has not had its application denied or deemed withdrawn for failure to respond to ONC (or an RCE) requests for information, the Applicant QHIN may be prepared to reapply much sooner than is the case for Applicant QHINs that have had their application denied or deemed withdrawn. We welcome comments on the proposed processes and requirements in this subpart. Specifically, we request comment on whether the six-month timeframe for re-application after an application has been deemed to be withdrawn as a result of the Applicant QHIN's failure to respond to requests for information or has been denied is appropriate, as well as other timeframes we propose.

D. Subpart D—Suspension

Within this subpart, we propose provisions associated with suspension, notice requirements for suspension, and the effect of suspension. In § 172.401, we propose provisions related to ONC (or the RCE) suspension of a QHIN or directed suspension of a Participant or Subparticipant. In § 172.401(a), we propose that ONC (or an RCE) may suspend a QHIN's authority to engage in TEFCA Exchange if the ONC (or an RCE) determines that a QHIN is responsible for a Threat Condition. Within the TEFCA infrastructure, QHINs are expected to meet a high bar for security, including, but not limited to, third-party certification to industry-recognized cybersecurity standards; compliance with the HIPAA Security Rule or the standards required by the HIPAA Security Rule; annual security assessments; designation of a Chief Information Security Officer; and having cyber risk coverage.

This proposed provision would support the overall security of TEFCA and align with the security requirements for QHINs by enabling ONC (or an RCE) to suspend a QHIN's authority to engage in TEFCA Exchange if the QHIN is responsible for a Threat Condition. According to the definition proposed in § 172.102, a Threat Condition may occur in three circumstances: (i) a breach of a material provision of a Framework Agreement that has not been cured within fifteen (15) calendar days of receiving notice of the material breach (or such other period of time to which contracting parties have agreed), which notice shall include such specific information about the breach that is available at the time of the notice; or (ii) a TEFCA Security Incident, as that term is defined in § 172.102; or (iii) an event that ONC (or an RCE), a QHIN, its Participant, or their Subparticipant has reason to believe will disrupt normal TEFCA Exchange, either due to actual compromise of, or the need to mitigate demonstrated vulnerabilities in, systems or data of the QHIN, Participant, or Subparticipant, as applicable; or through replication in the systems, networks, applications, or data of another QHIN, Participant, or Subparticipant; or (iv) any event that could pose a risk to the interests of national security as directed by an agency of the United States government. We propose this policy because we believe that in each of these situations, in order to protect the security of TEFCA Exchange, ONC (or an RCE) must be able to take immediate action to suspend a QHIN's authority to engage in TEFCA exchange and limit the potential effects of the Threat Condition.

In § 172.401(b), we propose if ONC (or an RCE) determines that one of a QHIN's Participants or Subparticipants has done something or failed to do something that results in a Threat Condition, ONC (or an RCE) may direct the QHIN to suspend that Participant's or Subparticipant's authority to engage in TEFCA Exchange. This provision proposes to extend the ONC (or an RCE's) authority to suspend a QHIN's authority to engage in TEFCA Exchange to also include the authority to order a QHIN to suspend a Participant's or Subparticipant's authority to engage in TEFCA Exchange. We believe this provision would help protect the security of TEFCA Exchange because any Threat Condition—whether due to the action or inaction by a QHIN, Participant, or Subparticipant—could jeopardize the security of TEFCA and must be addressed once identified. We believe that in order to protect the security of TEFCA Exchange, ONC (or an RCE) must be able to take immediate action to order a QHIN to suspend a Participant's or Subparticipant's authority to engage in TEFCA Exchange and limit the potential effects of a Threat Condition resulting from something a Participant or Subparticipant has done or failed to do.

In § 172.401(c), we propose that ONC (or an RCE) will make a reasonable effort to notify a QHIN in writing, in advance, of ONC's (or an RCE's) intent to suspend the QHIN or to direct the QHIN to suspend one of the QHIN's Participants or Subparticipants, and give the QHIN an opportunity to respond. Such notice would identify the Threat Condition giving rise to such suspension. We acknowledge that a suspension would significantly disrupt the activities of a QHIN, Participant, or Subparticipant and therefore § 172.401(c) proposes to require ONC (or an RCE) to make a reasonable effort to notify affected parties in advance of the ONC's (or an RCE's) intent to suspend. We propose to only require ONC (or an RCE) to make a reasonable effort to notify the entity because the circumstances surrounding a Threat Condition may limit ONC's (or an RCE's) ability to provide advance written notice to the QHIN or the QHIN's Participants or Subparticipants, despite ONC's (or an RCE's) best efforts. In § 172.401(d), we propose ONC (or an RCE) shall lift a suspension once the Threat Condition is resolved. We believe that it would no longer be necessary to continue a suspension once a Threat Condition is resolved.

We believe the provisions outlined in § 172.401 would help maintain the integrity of TEFCA and offer a transparent approach to suspension that would communicate the reason for suspension, require timely notification of suspension, and afford QHINs an opportunity to resolve the issue(s), including in concert with their Participants or Subparticipants, that led to the suspension and resume TEFCA Exchange.

In § 172.402, we propose provisions related to selective suspension of TEFCA Exchange between QHINs. In § 172.402(a), we propose that a QHIN may, in good faith and to the extent permitted by Applicable Law, suspend TEFCA Exchange with another QHIN because of reasonable concerns related to the privacy and security of information that is exchanged. In § 172.402(b), we propose that if a QHIN decides to suspend TEFCA exchange with another QHIN, it is required to promptly notify, in writing, ONC (or an RCE) and the QHIN with which it is suspending exchange of its determination and the reason(s) for making the decision.

These proposed provisions are intended to further strengthen the privacy and security protections within TEFCA by extending suspension rights to QHINs to suspend exchange with another QHIN due to reasonable concerns related to the privacy and security of information that is exchanged. We emphasize that we are proposing that the concerns must be ''reasonable'' *and* must be related to the ''privacy and security of information that is exchanged'' in order to ensure that suspension of TEFCA Exchange between QHINs is not based on other factors, such as competitive advantage. We solicit comments on examples of reasonable concerns related to the privacy and security of information that is exchanged. These proposed requirements would support trust between QHINs, which is a foundational element of TEFCA and would help TEFCA establish a universal floor for interoperability across the country. We believe prompt notification of the selective suspension to ONC (or an RCE) and the suspended QHIN would enable all parties involved to be aware of the situation in a timely fashion and take action to maintain the privacy and security of TEFCA Exchange activities.

In § 172.402(c), we propose that if a QHIN suspends TEFCA Exchange with another QHIN under § 172.402(a), it must, within thirty (30) calendar days, initiate the TEFCA dispute resolution process in order to resolve the issues that led to the decision to suspend, or the QHIN may end its suspension and resume TEFCA Exchange with the other QHIN within thirty (30) calendar days of suspending TEFCA Exchange with the QHIN. We propose this provision to provide the parties with an opportunity to resolve concerns related to privacy and security and potentially continue exchange once the issues have been resolved. We believe the thirty (30)-day timeframe would provide sufficient time to resolve issues that led to the suspension, end the suspension, and resume TEFCA Exchange activities in a timely manner. Ultimately, TEFCA will be most impactful and successful if QHINs trust each other and are able to confidently exchange information with each other, so it is in the best interests of the QHINs involved, as well as TEFCA overall, to address and resolve a selective suspension quickly, and by the least disruptive means possible.

In § 172.402(d), we propose that, provided that a QHIN suspends TEFCA exchange with another QHIN in accordance with other provisions in § 172.402 and in accordance with Applicable Law, such selective suspension would not be deemed a violation of the Common Agreement. This provision would promote the integrity of TEFCA by ensuring that a QHIN with reasonable and legitimate concerns related to the privacy and security of information that is exchanged would not be deterred from suspending exchange activities with another QHIN for fear of being in violation of the Common Agreement.

We welcome comments on the proposed processes and requirements in this subpart.

E. Subpart E—Termination

In this subpart, we propose provisions related to a QHIN's right to terminate its own Designation, ONC's (or an RCE's) obligation to terminate a QHIN's Designation and related notice requirements, and requirements related to the effect of termination. In § 172.501, we propose that a QHIN may terminate its own QHIN Designation at any time without cause by providing ninety (90) calendar days prior written notice. This provision supports the voluntary nature of TEFCA by allowing a QHIN that, for whatever reason, no longer wants to serve as a QHIN, to terminate its own QHIN Designation with ninety (90) business days prior written notice. We believe a QHIN should be able to terminate its Designation, regardless of the circumstances or reason and that ninety (90) business days would provide enough time for ONC, the RCE and the departing QHIN to analyze and address the impacts of the QHIN's departure.

In § 172.502, we propose that a QHIN's Designation will be terminated with immediate effect by ONC (or an RCE) giving written notice of termination to the QHIN if the QHIN: (a) fails to comply with any regulations of this part and fails to remedy such material breach within thirty (30) calendar days after receiving written notice of such failure; provided, however, that if a QHIN is diligently working to remedy its breach at the end of this thirty (30) day period, then ONC (or an RCE) must provide the QHIN with up to another thirty (30) calendar days to remedy its material breach; or (b) a QHIN breaches a material provision of the Common Agreement where such breach is not capable of remedy. We request comments on examples of material provisions of the Common Agreement where a breach is not capable of remedy.

We believe these proposals would promote transparency in TEFCA and strengthen the underlying trust among and between entities connected to TEFCA. These termination provisions would enable ONC (or an RCE) to take swift action to remove a non-complaint QHIN and ensure that entities that fail to meet their obligations as QHINs (by failing to comply with the regulations of this Part or by breaching a material provision of the Common Agreement) are no longer able to act as QHINs under the TEFCA framework. Without the ability for ONC (or an RCE) to terminate non-compliant QHINs, this trust—which is foundational to TEFCA and necessary for the ultimate success of TEFCA—could quickly erode and undermine TEFCA's progress.

In § 172.503, we propose that QHINs and ONC (or an RCE) would be able to terminate the QHIN's Designation at any time and for any reason by mutual, written agreement. Allowing two parties to terminate an agreement by mutual, written agreement ensures that two parties are not forced to follow an agreement that neither wants to follow. ONC believes it is reasonable and efficient to allow termination at any time where both ONC (or an RCE) and the QHIN are satisfied that a QHIN's termination is in the best interest of all.

We welcome comments on the proposed processes and requirements in this subpart.

F. Subpart F—Review of RCE® or ONC Decisions

ONC oversees the RCE's work and has the right to review the RCE's conduct and its execution of nondiscrimination and conflict of interest policies that demonstrate the RCE's commitment to treating QHINs in a transparent, fair,

and nondiscriminatory way.[260] This subpart proposes to establish processes for review of RCE or ONC actions, including QHIN appeal rights and the process for filing an appeal. These appeal rights would ensure that a QHIN or Applicant QHIN that disagrees with certain RCE or ONC decisions will have recourse to appeal those decisions. Our proposed § 172.600 reflects this overall scope as an applicability section for this subpart.

In § 172.601, we propose provisions to establish ONC's authority to review RCE determinations, policies, and actions, as well as procedures for exercising such review. We propose in § 172.601(a) that ONC may, in its sole discretion, review all or any part of any RCE determination, policy, or action. In § 172.601(b) we propose ONC may, in its sole discretion and on notice to affected QHINs or Applicant QHINs, stay any RCE determination, policy, or other action. In § 172.601(c), we propose ONC may, in its sole discretion and on written notice, request that a QHIN, Applicant QHIN, or the RCE provide ONC additional information regarding any RCE determination, policy, or other action. In § 172.601(d), we propose that on completion of its review, ONC may affirm, modify, or reverse the RCE determination, policy, or other action under review. Additionally, we propose to provide notice to affected QHINs or Applicant QHINs that includes the basis for ONC's decision. In § 172.601(e), we propose ONC will provide written notice under this section to affected QHINs or Applicant QHINs in the same manner as the original RCE determination, policy, or other action under review. We believe these proposals provide transparency into the level of oversight ONC has in reviewing RCE determinations, policies, or actions and firmly establish ONC's authority to affirm, modify, or reverse such determinations, policies, and actions. We believe these provisions are important to assure QHINs and Applicant QHINs that we have the ability to effectively exercise oversight of the RCE, as well as provide all parties with an interest in the administration of TEFCA with confidence that we can and will take necessary action to ensure that QHINs and Applicant QHINs comply with the regulations we propose in part 172.

In § 172.602, we propose to establish bases for Applicant QHINs and QHINs to appeal decisions to ONC. We propose that an Applicant QHIN or QHIN may appeal certain decisions to ONC or a hearing officer, as appropriate. In § 172.602(a)(1), we propose that an Applicant QHIN would be able to appeal the denial of its application. In § 172.602(a)(2), we propose that a QHIN would be able to appeal a decision to (1) suspend a QHIN or instruct a QHIN to suspend its Participant or Subparticipant; or (2) terminate a QHIN's Common Agreement. We request comment on the proposed bases for appeal.

In § 172.603, we propose the method and timing for filing an appeal. In § 172.603(a), we propose that to initiate an appeal, an authorized representative of the Applicant QHIN or QHIN must submit electronically, in writing to ONC, a notice of appeal that includes the date of the notice of appeal, the date of the decision being appealed, the Applicant QHIN or QHIN who is appealing, and the decision being appealed within fifteen (15) calendar days of the Applicant QHIN's or QHIN's receipt of the notice of (1) denial of an application, (2) suspension or instruction to suspend its Participant or Subparticipant, or (3) termination. With regard to an appeal of a termination, the fifteen (15) calendar day timeframe may be extended by ONC up to another fifteen (15) calendar days if the QHIN has been granted an extension for completing its remedy under § 172.502(a). The notice of appeal would serve to notify ONC that the Applicant QHIN or QHIN is planning to file an appeal and would require inclusion of only the minimum amount of information necessary to provide such notice (*i.e.,* the date of the notice of appeal, the date of the decision being appealed, the Applicant QHIN or QHIN who is appealing, and what is being appealed). As such, we believe fifteen (15) business days would be an adequate amount time for deciding whether to initiate an appeal and submitting such information.

In § 172.603(b), we propose that an authorized representative of an Applicant QHIN or QHIN must submit electronically, to ONC, within thirty (30) calendar days of filing the intent to appeal: (1) A statement of the basis for appeal, including a description of the facts supporting the appeal with citations to documentation submitted by the QHIN or Applicant QHIN; and (2) Any documentation the QHIN would like considered during the appeal.

We expect that it would take an Applicant QHIN or QHIN some time to collect all of the relevant information and documentation to support its appeal, and accordingly have proposed a timeframe for requesting an appeal of thirty (30) calendar days from the filing of the intent to appeal with ONC. We welcome comments on whether this timeframe, as well as the timeframe for submitting an intent to appeal, are adequate and appropriate.

In § 172.603(c), we propose that an Applicant QHIN or QHIN filing the appeal may not submit on appeal any evidence it did not submit prior to the appeal, except by permission of the hearing officer. We believe this provision balances a QHIN or Applicant QHIN's right to introduce evidence with the need for orderly proceedings. We are aware that under our proposed regulations, QHINs facing suspension or termination do not have an express right to introduce evidence. We solicit comments on whether and when a QHIN facing suspension or termination should have a right to introduce that evidence—for example as part of demonstrating that a material breach has been remedied or is capable of remedy under § 172.502, at the hearing officer stage, or some combination of the two based on circumstances of the suspension or termination.

In § 172.604, we propose that an appeal would not stay a suspension or termination, unless otherwise ordered by ONC or the hearing officer assigned under § 172.605(b). This means that in the event of an appeal of a suspension or termination, the appeal would not stop the suspension or termination from being effective. We believe this proposed approach is important because a QHIN would only be suspended or terminated for infractions that could, for example, jeopardize the privacy and security of TEFCA Exchange.

Before a QHIN is terminated under § 172.502(a), the QHIN would have already been given an opportunity to remedy the breach unless the breach is not capable of remedy. The move by ONC or and RCE to terminate a QHIN would mean either the QHIN tried and failed to remedy the issue, or a remedy is not possible. In either case, we believe it would be appropriate not to stay the termination. In the case of a suspension, the QHIN would have been found to be responsible for a Threat Condition, and we believe the risk to the privacy and security of the TEFCA ecosystem would far outweigh any perceived benefit of staying the suspension.

In § 172.605, we propose provisions related to the assignment of a hearing officer. In § 172.605(a), we propose that, in the event of an appeal, the National Coordinator may exercise authority under § 172.601 to review the RCE determination being appealed. We

[260] *See* Common Agreement Section 3.1, *https://www.federalregister.gov/documents/2024/05/01/2024-09476/notice-of-publication-of-common-agreement-for-nationwide-health-information-interoperability-common.*

further propose an appealing QHIN or Applicant QHIN that is not satisfied with ONC's subsequent determination may appeal that determination to a hearing officer by filing a new notice of appeal and other appeal documents that comply with § 172.603. In § 172.605(b), we propose if ONC declines review under subsection (a), or if ONC made the determination under review, ONC would arrange for assignment of the case to a hearing officer to adjudicate the appeal.

We specify in proposed § 172.605(c) that the hearing officer must be an officer appointed by the Secretary of Health and Human Services (for more information about officers and appointments, see section III.D.5.c, above). In § 172.605(d), we propose, the hearing officer may not be responsible to, or subject to the supervision or direction of, personnel engaged in the performance of investigative or prosecutorial functions for ONC, nor may any officer, employee, or agent of ONC engaged in investigative or prosecutorial functions in connection with any adjudication, in that adjudication or one that is factually related, participate or advise in the decision of the hearing officer, except as a counsel to ONC or as a witness.

In § 172.606, we propose requirements related to adjudication. In § 172.606(a), we propose that the hearing officer would decide issues of law and fact *de novo* and would apply a preponderance of the evidence standard when deciding appeals. *De novo* review means that the hearing officer would decide the issue on appeal without deference to a previous decision (*i.e.,* ONC's or the RCE's decision to (1) deny an application, (2) suspend a QHIN or to instruct a QHIN to suspend its Participant or Subparticipant, or (3) terminate a QHIN's Common Agreement). We believe *de novo* review is appropriate for appeals by Applicant QHINs or QHINs because ONC ultimately has responsibility for TEFCA operations and implementation, even though the RCE is a contractor acting on ONC's behalf. Given the gravity and potentially significant implications (financial, effect on existing contracts, etc.) of a denied application, suspension, or termination, we believe the hearing officer assigned by the National Coordinator should make an independent decision, taking all of the facts and evidence the parties present into consideration.

The ''preponderance of the evidence'' standard means the burden of proof is met when the party with the burden (the appealing Applicant QHIN or QHIN) convinces the fact finder (hearing officer) that there is a greater than 50% chance that the claim is true. This standard is used in most civil cases and would only require the appealing party to show that a particular fact or event was more likely than not to have occurred. We believe this threshold creates the right balance for requiring an appealing Applicant QHIN or QHIN to make a strong case to succeed on appeal, while not imposing a standard that would be extremely difficult for the appeal Applicant QHIN or QHIN to meet. We request comment on whether the ''preponderance of the evidence'' is the appropriate standard, or if another standard (*e.g.,* clear and convincing evidence, beyond a reasonable doubt, etc.) would be more suitable.

In § 172.606(b), we propose that a hearing officer would make a determination based on the written record or any information from a hearing conducted in-person, via telephone, or otherwise (for example, via video teleconference). We propose that the written record would include ONC's or the RCE's determination and supporting information, as well as all appeal materials submitted by the Applicant QHIN or QHIN pursuant to § 172.603. We propose these requirements for the written record because it is important that the written record reflect both the position of ONC or the RCE and the Applicant QHIN or QHIN. We propose that the hearing officer would have sole discretion to conduct a hearing in certain situations. We propose that the hearing officer could conduct a hearing to require either party to clarify the written record under paragraph (b)(1) of this section. Last, we propose that the hearing officer could conduct a hearing if they otherwise determine a hearing is necessary. We believe the last provision is necessary because it gives the hearing officer discretion to conduct a hearing based on the specific circumstances surrounding the appeal, even if the need for the hearing does not fit under the first or second criteria detailed above.

In § 172.606(c), we propose that a hearing officer would neither receive witness testimony nor accept any new information beyond what was provided in accordance with paragraph (b) of this section, except for good cause shown by the party seeking to submit new information. We believe this provision will help ensure that the appeals process is consistent and fair for all involved.

In § 172.607, we propose requirements related to a decision by the hearing officer. In § 172.607(a), we propose that the hearing officer would issue a written determination. We request comment on whether we should include a specific timeframe for issuing the written determination, or whether abstaining from including a specific timeframe is a better approach given the varying complexity and circumstances of each appeal.

To ensure accountability, and to ensure that the hearing officer's decisions would be subject to the discretionary review of a principal officer of the United States, we propose in § 172.607(b) that a hearing officer's decision on an appeal is the final decision of HHS unless within 10 business days, the Secretary, at the Secretary's sole discretion, chooses to review the determination. We also propose that ONC would notify the appealing party if the Secretary chooses to review the determination and once the Secretary makes his or her determination. This provision would also align § 172.607 procedures with the ONC Health IT Certification Program appeals procedures in § 170.580(g) as we propose to revise them in this Proposed Rule (see Section III.D.2.b of this preamble). We have not proposed a specific timeframe for the Secretary to complete their review (if the Secretary chooses to review) because we believe that if the Secretary makes the decision to review a hearing officer's determination, the Secretary would be informed enough on the issues of the case to determine an appropriate review timeframe.

We welcome comments on the proposed appeal processes outlined in this subpart.

G. Subpart G—QHIN™ Attestation for the Adoption of the Trusted Exchange Framework and Common Agreement™

Section 4003(b) of the Cures Act added section 3001(c)(9), ''Support for Interoperable Networks Exchange,'' to the PHSA. Section 3001(c)(9)(D)(ii) requires HHS to establish, through notice and comment rulemaking, a process for HINs that voluntarily elect to adopt TEFCA to attest to such adoption of the framework and agreement. Section 3001(c)(9)(D)(i) also requires the National Coordinator to publish on ONC's website a list of the HINs that have adopted the Common Agreement and are capable of trusted exchange pursuant to the Common Agreement.

QHINs are the only entities permitted to ''adopt'' the Common Agreement, which is accomplished by becoming a signatory to the Common Agreement. As such, we propose that only QHINs would be able to attest to the adoption of the Common Agreement and the Trusted Exchange Framework. While the Trusted Exchange Framework was

foundational for creating the provisions of the Common Agreement, it is, as noted above, a separate set of principles. Therefore, we propose that for purposes of attesting to the adoption of the Trusted Exchange Framework, QHINs would be required to expressly attest to their agreement and adherence to the Trusted Exchange Framework.[261]

Once attestation is complete and deemed valid, QHINs would be publicly listed on ONC's website. This regulatory provision would implement the HIN attestation provision from the Cures Act and would provide benefits to the public, Federal partners, and interested parties. For example, a Federal website listing of attesting QHINs would make it easy for the public to identify whether an entity is or is not a QHIN and provide a resource for Federal partners to help determine whether participants in some of their programs also belong to a network that is recognized as a QHIN. Section 3001(c)(9)(E) provides the option for Federal agencies to require, under certain circumstances, adoption of TEFCA for health information exchange networks that they contract with or enter into agreements with.

To implement sections 3001(c)(9)(D)(i) and (ii) of the PHSA, we propose to establish subpart G in part 172 titled, ''QHIN Attestation for the Adoption of the Trusted Exchange Framework and Common Agreement.''

We propose in § 172.700 that subpart G would establish the attestation submission requirements applicable to QHINs. In § 172.701, we propose attestation submission requirements for QHINs and review and acceptance processes that ONC will follow for TEFCA attestations. In § 172.701(b), we propose that in order to be listed in the QHIN Directory described in proposed § 172.702, a QHIN would be required to submit to ONC an attestation affirming agreement with and adherence to the Trusted Exchange Framework and its adoption of the Common Agreement. We further propose in § 172.701(b) that a QHIN would be required to submit to ONC identifying information consisting of its name, address, city, State, zip code, and a hyperlink to its website. We also propose that the QHIN would be required to submit to ONC identifying information about its authorized representative including the representative's name, title, phone number, and email address. We propose that a QHIN would also be required to provide documentation confirming its Designation as a QHIN. We also propose that a QHIN would be required to provide ONC with written notice of any changes to its identifying information provided in accordance with § 172.701 within 30 calendar days of the change(s) to its identifying information. We believe the above provisions provide clear instructions for submitting a QHIN attestation that will support a consistent and transparent QHIN attestation process and provides ONC with the information needed to identify the entity and contact the authorized representative.

We propose in § 172.701(c) that a QHIN must electronically submit its attestation and documentation specified in § 172.701(b) either via an email address identified by ONC or via a submission on the ONC website, if available. We propose in § 172.701(d) that once a QHIN has submitted its attestation and documentation, ONC would either accept or reject the submission within 30 calendar days. We propose that ONC would accept the submission if it determines that the QHIN has satisfied the requirements of §§ 172.701(b) and (c). In such instances, we propose that ONC would provide written notice to the applicable QHIN's authorized representative that the submission has been accepted. In § 172.701(d), we also propose that ONC would reject a submission if it determines that the requirements of § 172.701(b), § 172.701(c), or both, have not been satisfied. In such instances, we propose that ONC would provide written notice to the QHIN's authorized representative of the determination along with the basis for the determination. We propose that an ONC determination would be a final agency action and not subject to administrative review, except the Secretary may choose to review the determination as provided in § 172.607(b). However, we propose that a QHIN may, at any time, resubmit an attestation and documentation in accordance with §§ 172.701(b) and (c). We believe these submission procedures will support a consistent and transparent QHIN attestation process. We welcome comments on these procedures.

In § 172.702, we propose the requirements for a QHIN directory. We propose in § 172.702(a) that this subpart would establish processes for publishing a directory of QHINs on the ONC website. We propose in § 172.702(b)(1) that, within fifteen (15) calendar days of notifying a QHIN that its submission has been accepted, ONC would publish, at a minimum, the QHIN's name in the QHIN directory.

We propose § 172.702(b)(2) to identify within the QHIN directory those QHINs that have been suspended under the Common Agreement. A QHIN directory that includes QHINs that have adopted the Common Agreement and are capable of TEFCA Exchange and those QHINs suspended under the Common Agreement offers a transparent list of QHINs participating in TEFCA. As noted above, the QHIN directory may serve as a useful tool for the public, Federal partners, and other interested parties seeking information about QHINs. Therefore, we welcome comments regarding the information we propose to include in the QHIN directory.

We propose in § 172.702(c) to establish requirements for removal of a QHIN from the QHIN directory. We propose in § 172.702(c)(1) that ONC will remove a QHIN that is no longer eligible for QHIN status from the QHIN directory. We propose that a QHIN whose Common Agreement has been terminated would no longer be considered a QHIN and so would be removed from the QHIN directory. The removal of a QHIN whose Common Agreement has been terminated from the QHIN Directory would be a ministerial action by ONC.

We propose in § 172.702(c)(2) that upon termination of a QHIN's Common Agreement, ONC (or an RCE) will send a written statement of intent to remove the QHIN from the QHIN Directory to the authorized representative of the QHIN. Under § 172.702(c)(3), we propose that the written statement would include, as appropriate, (i) the name of the terminated QHIN and the name and contact information of the authorized representative of the QHIN; (ii) a short statement setting forth findings of fact with respect to any violation of the Common Agreement or other basis for the QHIN's termination; (iii) other materials as the RCE may deem relevant. In § 172.702(d), we propose that a QHIN that is removed from the QHIN Directory would remain removed until a new attestation is accepted by ONC in accordance with the processes specified in subpart G of this part. In § 172.702(e), we propose that an ONC determination under § 172.702 is final agency action and not subject to further administrative review, except the Secretary may choose to review the determination as provided in § 172.607(b). We believe this proposal is appropriate because a QHIN would have had ample opportunity to appeal its termination under the provisions proposed in Subpart F of this Proposed Rule.

[261] The Trusted Exchange Framework (TEF): Principles for Trusted Exchange (January 2022), *https://www.healthit.gov/sites/default/files/page/2022-01/Trusted_Exchange_Framework_0122.pdf.*

We seek comments on alternative ways to structure the requirements to remove a QHIN from the QHIN directory.

VI. Incorporation by Reference

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(a)). Specifically, § 51.5(a) requires agencies to discuss, in the preamble of a proposed rule, the ways that the materials it proposes to incorporate by reference are reasonably available to interested parties or how it worked to make those materials reasonably available to interested parties; and summarize, in the preamble of the proposed rule, the material it proposes to 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 most of these instances, access to the standard or implementation specification can be gained through no-cost (monetary) participation, subscription, or membership with the applicable standards developing organization (SDO) or custodial organization. Alternatively, 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 III.A.1 of this preamble, we have followed the NTTAA and OMB Circular A–119 in proposing standards and implementation specifications for adoption, including describing any exceptions in the proposed 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 propose to adopt, and subsequently adopt and incorporate by reference in the **Federal Register**, available to interested parties. As described above, this includes making the standards and implementation specifications available through no-cost memberships and no-cost subscriptions.

As required by § 51.5(a), we provide summaries of the standards we propose to adopt and subsequently incorporate by reference in the Code of Federal Regulations. We also provide relevant information about these standards and implementation specifications throughout the preamble.

We have organized the following standards and implementation specifications that we propose to adopt through this rulemaking according to the sections of the Code of Federal Regulations (CFR) in which they would be codified and cross-referenced for associated certification criteria and requirements that we propose to adopt. We note, in certain instances, that we request comment in this proposed rule on multiple standards or implementation specifications that we are considering for adoption *and incorporation by reference* for particular use cases. We include all of these standards and implementation specifications in this section of the preamble.

Content Exchange Standards and Implementation Specifications for Exchanging Electronic Health Information—45 CFR 170.205

- HL7 CDA R2 IG: Consolidated CDA (C–CDA) Templates for Clinical Notes, Edition 3—US Realm (C–CDA Edition 3), May 18, 2024

URL: https://hl7.org/cda/us/ccda/.

This is a direct access link.

Summary: C–CDA 3.0 merges the C–CDA R2.1 and the C–CDA Companion Guides, adds C–CDA enhancement requests, and incorporates new design and guidance for USCDI V4. Annual updates will occur to provide design for USCDI releases and to address comments or requests from the US Realm C–CDA community.

- HL7 Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1—US Realm Standard for Trial Use, July 2019

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=503.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: The scope of this document is to provide guidelines for transmitting HL7 v.2.5.1-compliant messages that also conform with specific profiles that facilitate communications from emergency departments, urgent care centers, and ambulatory care and inpatient settings to the PHAs that conduct syndromic surveillance. The intent of this guide is to facilitate data exchange between different systems for syndromic surveillance purposes.

- HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 2018 Update

URL: https://www.cdc.gov/vaccines/programs/iis/technical-guidance/hl7.html.

This is a direct access link.

Summary: This document combines the original HL7 2.5.1 Release 1.5 Implementation Guide and Release 1.5 Addendum, as well as additional guidance published by AIRA. The purpose of this document is to provide a single document containing essential HL7 information, so that implementers and developers have a convenient single set of information to work from. Further, the new Appendix C provides references to additional guidance documents published by AIRAafter the release of the addendum.

- HL7 Version 2.5.1 Implementation Guide: Laboratory Orders (LOI) from EHR, Release 1, STU Release 4—US Realm, December 3, 2013

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=152.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: This implementation guide focuses on key points of broad interoperability, including use of strong identifiers for key information objects and use of vocabulary standards. This version supports additional data elements needed for newborn dried bloodspot screening (NDBS), Public Health reporting (PH) including pandemic response requirements, the

ability to request withholding results reporting to patients/caregivers until the provider had the opportunity to share those results, and references to preliminary guidance to include SOGI/Gender Harmony data.

• HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface (LRI), Release 1 STU Release 4—US Realm (Public Health Profile), July 16, 2012

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=279.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: This guide provides guidance on how to communicate laboratory results in general from a (reference) Laboratory's LIS to a system interested in lab results, *e.g.,* EHR, Public Health, or other Laboratory. It covers general lab results, as well as specifications focused on micro-biology, newborn dried bloodspot screening, and clinical genomics. The guide includes particular guidance that can be pre-adopted to support pandemic response reporting to public health and references preliminary guidance to include SOGI/Gender Harmony data.

• HL7 FHIR Central Cancer Registry Reporting Content IG, 1.0.0—STU 1, December 21, 2023

URL: https://build.fhir.org/ig/HL7/fhir-central-cancer-registry-reporting-ig/index.html.

This is a direct access link.

Summary: This standard facilitates automated, standardized exchange of cancer surveillance data from ambulatory healthcare provider EHR systems to central cancer registries. The goal of this IG is to leverage existing technology frameworks and standards (*e.g.,* minimal Common Oncology Data Elements (mCODE)), facilitate automated electronic collection and exchange, reduce reporting burden on data providers, augment secure transfers, and enhance data completeness, timeliness, and accuracy of cancer surveillance data using modern IT standards.

• HL7 FHIR Cancer Pathology Data Sharing, 1.0.0—STU1, August 18, 2023

URL: https://build.fhir.org/ig/HL7/cancer-reporting/.

This is a direct access link.

Summary: The Cancer Pathology Data Sharing implementation guide (IG) reporting process documents best practices for transmitting pathology data as FHIR resource bundles and distributing them to the Central Cancer Registry (CCR) via two pathways: (1) Laboratory Information Systems (LIS) to CCR via an EHR intermediary; and (2) LIS to CCR directly. This publication promotes structured data collection and exchange of cancer pathology data, provides the data model, defined data items and their corresponding code and value sets. This guide specifies the collection and exchange of data specific to a cancer pathology synoptic report for public health reporting. This guide contains a library of FHIR profiles to create a cancer pathology message bundle and is compliant with FHIR Release 4.

• HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release 3—US Realm, December 2, 2020

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=426.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: The implementation guide supports electronic submission of HAI data to the National Healthcare Safety Network (NHSN). The implementation guide enables more than 3000 hospitals in 22 States to meet requirements that Healthcare Associated Infection data be submitted through the NHSN to CDC and revises existing reports and adds new ones to collect data that is relevant to CDC's mandate.

• HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1—US Realm, January 6, 2022

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=385.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: This standard is an HL7 Clinical Document Architecture (CDA) Implementation Guide for representing data extracted from provider systems as required by the Centers for Disease Control and Prevention's National Center for Health Statistics (CDC/NCHS) for the National Ambulatory Medical Care Survey (NAMCS) and the National Hospital Care Survey (NHCS). The implementation guide creates a standardized format to represent ambulatory, inpatient, and outpatient healthcare data; enables automation of the survey data collection process by using CDA to streamline the collection of data and increase the sample pool by allowing all providers who participate in the surveys to do so electronically; the IG also supports physician offices'/hospitals' ability to participate in the NCHS surveys by providing electronic files from their EHRs.

• HL7 FHIR Vital Records Birth and Fetal Death Reporting 1.1.0—STU 1.1, October 10, 2023

URL: https://hl7.org/fhir/us/bfdr/.

This is a direct access link.

Summary: This implementation guide (IG) defines a series of Health Level Seven (HL7®) Fast Healthcare Interoperability Resources (FHIR®) profiles on the Composition resource to represent electronic birth and fetal death reporting (BFDR). It includes the content of medical/health information on live births and fetal deaths for select State and Federal birth and fetal death reporting, as indicated in the 2003 Revision of the U.S. Standard Certificate of Live Birth and the 2003 Revision of the U.S. Standard Report of Fetal Death Additionally, it includes the content that is exchanged between EHR systems, jurisdictions, and the Centers for Disease Control and Prevention/National Center for Health Statistics (CDC/NCHS).

• CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting, Implementation Guide for 2024, Version 1.1, August 31, 2023

URL: https://ecqi.healthit.gov/sites/default/files/QRDA-HQR-2024-CMS-IG-v1.1-508.pdf.

This is a direct access link.

Summary: This quality reporting document architecture (QRDA) guide contains CMS implementation guide to the HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture Category I, Release 1, Standard for Trial Use (STU) Release 5.3, US Realm, and any subsequent errata update, for the 2024 reporting period.

• HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I)—US Realm, STU 5.3 with errata, December 2022

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=35.

This is a direct access link.

Summary: A QRDA Category I report is an individual-patient-level quality report. Each report contains quality data for one patient for one or more quality measures, where the data elements in the report are defined by the particular measure(s) being reported on. A QRDA

Category I report contains raw applicable patient data. When pooled and analyzed, each report contributes the quality data necessary to calculate population measure metrics. This two-volume implementation guide (IG) describes constraints on the Clinical Document Architecture Release 2 (CDA R2) header and body elements for Quality Reporting Document Architecture (QRDA) documents.

• CMS Implementation Guide for Quality Reporting Document Architecture Category III, Eligible Clinicians Programs, Implementation Guide for 2024, Version 1.1, November 22, 2023

URL: https://ecqi.healthit.gov/sites/default/files/2024-CMS-QRDA-III-EC-IG-v1.1-508.pdf.

This is a direct access link.

Summary: This QRDA guide contains CMS supplemental implementation guide to the HL7 CDA R2 Implementation Guide: Quality Reporting Document Architecture (QRDA III), Release 1—US Realm (September 2021) for the 2024 performance period. This is a normative release approved by American National Standards Institute (ANSI) and HL7. This HL7 base standard is referred to as the HL7 QRDA III R1.

• HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture (QRDA III), Release 1—US Realm (ANSI/HL7 Normative Release 1), September 2021

URL: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=286.

This is a direct access link.

Summary: A QRDA Category III report is an aggregate quality report. Each report contains calculated summary data for one or more measures for a specified population of patients within a particular health system over a specific period of time. Data needed to generate QRDA Category III reports must be included in the collected QRDA Category I reports, as the processing entity will not have access to additional data sources. The QRDA Category III Implementation Guide directs implementers on how to construct QRDA Category III instances to report aggregated results for electronic clinical quality measures (eCQMs).

Vocabulary Standards for Representing Electronic Health Information—45 CFR 170.207

• Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), U.S. Edition, September 2023 Release

URL: https://www.nlm.nih.gov/healthit/snomedct/us_edition.html.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: This release contains 163 new active concepts specific to the US Extension. The September 2023 US Edition of SNOMED CT is based on the content published in the June 2023 SNOMED CT International Edition and includes any SNOMED CT COVID–19 Related Content published in the June 2023 SNOMED CT International Edition. This latest version of the US Edition also includes the SNOMED CT to ICD–10–CM reference set, with over 126,000 SNOMED CT source concepts mapped to ICD–10–CM targets.

• Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.76, a Universal Code System for Identifying Laboratory and Clinical Observations Produced by the Regenstrief Institute, Inc., September 18, 2023

URL: https://loinc.org/downloads/.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: LOINC version 2.76 is a Hotfix release only. No new concepts have been added.

This Hotfix addresses issues discovered after the release of version 2.75 in August 2023. Version 2.76 includes updates to 196 concepts.

• RxNorm, a Standardized Nomenclature for Clinical Drugs Produced by the United States National Library of Medicine, December 4, 2023, Full Monthly Release

URL: https://www.nlm.nih.gov/research/umls/rxnorm/docs/rxnormfiles.html.

Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: RxNorm, a standardized nomenclature for clinical drugs, is produced by the National Library of Medicine. RxNorm's standard identifiers and names for clinical drugs are connected to the varying names of drugs present in many different controlled vocabularies within the Unified Medical Language System (UMLS) Metathesaurus, including those in commercially available drug information sources. These connections are intended to facilitate interoperability among the computerized systems that record or process data dealing with clinical drugs.

• CDC National Center of Immunization and Respiratory Diseases (NCIRD) Code Set (CVX)—Vaccines Administered, Updates Through September 29, 2023

URL: https://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx.

This is a direct access link.

Summary: The CDC's National Center of Immunization and Respiratory Diseases (NCIRD) developed and maintains the CVX (vaccine administered) code set. It includes both active and inactive vaccines available in the US. CVX codes for inactive vaccines allow transmission of historical immunization records. When a MVX (manufacturer) code is paired with a CVX (vaccine administered) code, the specific trade named vaccine may be indicated. These codes should be used for immunization messages using either HL7 Version 2.3.1 or HL7 Version 2.5.1.

• National Drug Code Directory (NDC)—Vaccine NDC Linker, Updates Through November 6, 2023

URL: https://www2.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.

This is a direct access link.

Summary: The Drug Listing Act of 1972 requires registered drug establishments to provide the FDA with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution. Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which serves as the universal product identifier for drugs. This standard is limited to the NDC vaccine codes identified by the CDC.

Standards for Health Information Technology To Protect Electronic Health Information Created, Maintained, and Exchanged—45 CFR 170.210

• Annex A: Federal Information Processing Standards (FIPS) Publication 140–2, Security Requirements for Cryptographic Modules, October 8, 2014

URL: https://web.archive.org/web/20150218170400/http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.

This is a direct access link.

Summary: Federal Information Processing Standards Publication (FIPS

PUB) 140–2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module.

• Annex A: Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, October 12, 2021

URL: https://csrc.nist.gov/files/pubs/fips/140-2/upd2/final/docs/fips1402annexa.pdf.

This is a direct access link.

Summary: Federal Information Processing Standards Publication (FIPS) 140–2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

United States Core Data for Interoperability—45 CFR 170.213

• United States Core Data for Interoperability (USCDI), Version 4 (v4), October 2023 Errata

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 to set a foundation for broader sharing of electronic health information. ONC has established a predictable, transparent, and collaborative expansion process for USCDI based on public evaluation of previous versions and submissions by the health IT community and the public, including input from a Federal advisory committee.

Application Programming Interface Standards—45 CFR 170.215

• HL7 FHIR® US Core Implementation Guide, Version 7.0.0—STU7, May 8, 2024

URL: https://hl7.org/fhir/us/core/.

This is a direct access link.

Summary: The US Core Implementation Guide is based on FHIR Version R4. It defines the minimum constraints on the FHIR resources to create the US Core Profiles. The elements, extensions, vocabularies, and value sets that SHALL be present are identified, and how they are used is defined. It also documents the minimum FHIR RESTful interactions for each US Core Profiles to access patient data. Establishing the ''floor'' of standards to promote interoperability and adoption through common implementation allows for further standards development evolution for specific use cases.

• United States Public Health Profiles Library Implementation Guide. US Public Health Profiles Library 1.0.0—STU1, October 4, 2023

URL: https://build.fhir.org/ig/HL7/fhir-us-ph-common-library-ig/.

This is a direct access link.

Summary: The US Public Health Profiles Library (USPHPL) is a collection of reusable architecture and content profiles representing common public health concepts and patterns. It is intended as a complement to the US Core Implementation Guide (US Core) to ease implementation burden of healthcare organizations, electronic health record companies, public health agencies, and others involved in the US public health endeavor.

• HL7® SMART App Launch Implementation Guide Release 2.2.0—STU 2.2, April 30, 2024

URL: https://hl7.org/fhir/smart-app-launch/.

This is a direct access link.

Summary: This implementation guide describes a set of foundational patterns based on Auth 2.0 for client applications to authorize, authenticate, and integrate with FHIR-based data systems.

• HL7 FHIR Bulk Data Access IG, 2.0.0—STU 2 Ballot, November 26, 2021

URL: https://build.fhir.org/ig/HL7/bulk-data/.

This is a direct access link.

Summary: This implementation guide defines a standardized, FHIR based approach for exporting bulk data from a FHIR server to a pre-authorized client. This implementation guide is designed to support sharing any data that can be represented in FHIR. This means that the IG should be useful for such diverse systems as, ''native'' FHIR servers that store FHIR resources directly, EHR systems and population health tools implementing FHIR as an interoperability layer, and financial systems implementing FHIR as an interoperability layer.

• HL7 CDS Hooks Release 2.0, August 23, 2022

URL: https://cds-hooks.hl7.org/.

This is a direct access link.

Summary: The CDS Hooks specification describes the RESTful APIs and interactions using JSON over HTTPS to integrate Clinical Decision Support (CDS) between CDS Clients (typically EHR Systems or other health information systems) and CDS Services.

• SMART Health Cards Framework Version 1.4.0, June 15, 2023

URL: https://spec.smarthealth.cards/.

This is a direct access link.

Summary: This implementation guide provides a framework for ''Health Cards''. The framework supports documentation of any health-related details that can be modeled with HL7 FHIR. This enables a consumer to receive COVID–19 Vaccination or Laboratory results and present these results to another party in a verifiable manner. Key use cases included conveying point-in-time infection status for return-to-workplace and travel.

• HL7 FHIR SMART Health Cards: Vaccination and Testing Implementation Guide Version 1.0.0—STU 1, December 27, 2023

URL: https://build.fhir.org/ig/HL7/fhir-shc-vaccination-ig/.

This is a direct access link.

Summary: This FHIR Implementation Guide describes the FHIR contents of a SMART Health Card (SHC) for infectious disease vaccination records and laboratory testing status. This includes a minimal set of patient information (name and contact information) that are needed for this use case.

• HL7 FHIR Subscriptions R5 Backport Implementation Guide Version 1.1.0—Standard for Trial Use, January 11, 2022

URL: https://hl7.org/fhir/uv/subscriptions-backport/STU1.1/.

This is a direct access link.

Summary: The Subscription R5 Backport Implementation Guide enables

servers running versions of FHIR earlier than R5 to implement a subset of R5 Subscriptions in a standardized way. During the development of FHIR R5, the Subscriptions Framework has gone through a significant redesign. Many implementers have expressed a need for functionality from the FHIR R5 version of Subscriptions to be made available in FHIR R4. The goal of publishing this guide is to define a standard method of back-porting the R5 Subscriptions Framework for greater compatibility and adoption.

• HL7 FHIR® Unified Data Access Profiles (UDAP™) Security for Scalable Registration, Authentication, and Authorization Implementation Guide Release 1.0.0—STU 1 U.S., September 27, 2022

URL: https://hl7.org/fhir/us/udap-security/.

This is a direct access link.

Summary: This implementation guide describes how to extend oAuth 2.0 using UDAP workflows for both consumer-facing apps that implement the authorization code flow, and business-to-business (B2B) apps that implement the client credentials flow or authorization code flow. This guide covers automating the client application registration process and increasing security using asymmetric cryptographic keys bound to digital certificates to authenticate ecosystem participants. This guide also provides a grammar for communicating metadata critical to healthcare information exchange.

• HL7 FHIR® Da Vinci—Payer Data Exchange (PDex) Implementation Guide: Version 2.0.0—STU2, January 6, 2024

URL: https://hl7.org/fhir/us/davinci-pdex/STU2/.

This is a direct access link.

Summary: The Payer Data Exchange (PDex) Implementation Guide is provided for payers/health plans to enable them to create a Member's Health History using clinical resources (based on U.S. Core Profiles established from FHIR R4) which can be understood by providers and, if they choose to, committed to their Electronic Medical Records (EMR) System.

• HL7 FHIR Da Vinci—Coverage Requirements Discovery (CRD) Implementation Guide, Version 2.0.1—STU 2, January 8, 2024

URL: https://hl7.org/fhir/us/davinci-crd/STU2/.

This is a direct access link.

Summary: The Da Vinci Coverage Requirements Discovery (CRD) Implementation Guide defines a workflow to allow payers to provide information about coverage requirements to healthcare providers through their provider systems at the time treatment decisions are being made. This will ensure that clinicians and administrative staff have the capability to make informed decisions and meet the requirements of the patient's insurance coverage.

• HL7 FHIR Da Vinci—Documentation Templates and Rules (DTR) Implementation Guide, Version 2.0.1—STU 2, January 11, 2024

URL: https://hl7.org/fhir/us/davinci-dtr/STU2/.

This is a direct access link.

Summary: The Da Vinci Documentation Templates and Rules (DTR) Implementation Guide provides a mechanism for payers to express their documentation requirements computably in a way that allows clinicians and other EHR users to navigate and quickly specify the needed information in a context-specific way. The guide allows rules to be written in a way that supports automatically extracting existing EHR information for review/confirmation and adjusting the information prompted for based on what data is already known or entered, minimizing impact on provider time, while expediting subsequent payer interactions.

• HL7 FHIR Da Vinci—Prior Authorization Support (PAS) FHIR IG, Version 2.0.1—STU 2, December 1, 2023

URL: https://hl7.org/fhir/us/davinci-pas/STU2/.

This is a direct access link.

Summary: The Da Vinci Prior Authorization Support (PAS) Implementation Guide enables direct submission of prior authorization requests from EHR systems using FHIR. The implementation guide also defines capabilities around the management of prior authorization requests, including checking the status of a previously submitted request, updating a previously submitted request, and canceling a request. Direct submission of prior authorization requests from the EHR can result in faster prior authorization decisions, reducing costs for both providers and payers and improving patient experience.

• HL7 FHIR® Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) Implementation Guide, Version 2.0.0—STU 2, November 28, 2022

URL: https://hl7.org/fhir/us/carin-bb/.

This is a direct access link.

Summary: This implementation guide describes the CARIN for Blue Button® Framework and Common Payer Consumer Data Set (CPCDS), providing a set of resources that payers can display to consumers via a FHIR API. The CARIN for Blue Button IG was defined by the CARIN Alliance to meet the requirements in the CMS Interoperability and Patient Access final rule for impacted payers to make available claims and encounter data via a Patient Access API. This IG is primarily used to exchange financial (claims and encounter) data, with some limited associated clinical data.

• *HL7 FHIR Da Vinci—Payer Data Exchange (PDex) U.S. Drug Formulary Implementation Guide, Version 2.0.1—STU 2, December 1, 2023*

URL: https://hl7.org/fhir/us/davinci-drug-formulary/STU2.0.1/.

This is a direct access link.

Summary: This implementation guide defines a FHIR interface to a health insurer's drug formulary information for patients/consumers. The primary use cases for this FHIR interface enable consumers/members/patients to understand the costs and alternatives for drugs that have been prescribed, and to compare their drug costs across different insurance plans.

• HL7 FHIR Da Vinci Payer Data Exchange (PDex) Plan Net Implementation Guide, Version 1.1.0—STU1.1 US, April 4, 2022

URL: https://hl7.org/fhir/us/davinci-pdex-plan-net/STU1.1/.

This is a direct access link.

Summary: This implementation guide defines a FHIR interface to access information about a health insurer's insurance plans, their associated networks, and the organizations and providers that participate in these networks. Publication of this data through a standard FHIR-based API will enable third parties to develop applications through which consumers and providers can query the participants in a payer's network that may provide services that address their healthcare needs.

VII. Response to Comments

Because of the large number of public comments normally received in response to **Federal Register** documents, we are not able to acknowledge or respond to them individually. We will consider all comments we receive by the date and time specified in the **DATES** section of this preamble, and when we proceed with a subsequent document, we will

respond to the comments in the preamble of that document.

VIII. 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, section 3506(c)(2)(A) of 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 explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section. To comment on the collection of information or to obtain copies of the supporting statements and any related forms for the proposed paperwork collections referenced in this section, email your comment or request, including your address and phone number to *sherrette.funn@hhs.gov,* or call the Reports Clearance Office at (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above email address within 60 days.

A. Qualified Health Information Networks™

We propose in § 172.301 to establish the information Applicant QHINs must submit in order to be Designated as a QHIN. We propose that an Applicant QHIN must submit: (1) a completed QHIN application; and (2) a signed copy of the Common Agreement. We note that the application may be updated over time and the most recent version will be available on ONC's and the RCE's website.

In § 172.701, we propose attestation submission requirements for QHINs and review and acceptance processes that ONC would follow for TEFCA attestations. In § 172.701(b), we propose that in order to be listed in the QHIN Directory described in proposed § 172.702, a QHIN would be required to submit to ONC an attestation affirming agreement with and adherence to the Trusted Exchange Framework and its adoption of the Common Agreement. We further propose in § 172.701(b) that a QHIN would be required to submit to ONC identifying information consisting of its name, address, city, State, zip code, and a hyperlink to its website. We also propose that the QHIN would be required to submit to ONC identifying information about its authorized representative including the representative's name, title, phone number, and email address.

We propose that a QHIN would also be required to provide documentation confirming its Designation as a QHIN. We also propose that a QHIN would be required to provide ONC with written notice of any changes to its identifying information provided in accordance with § 172.701 within 30 calendar days of the change(s) to its identifying information.

We believe QHINs will face minimal burden in complying with the proposed application, attestation, and supporting documentation requirements. For the purposes of estimating the potential burden, at this time, we are estimating that 15 Applicant QHINs would apply and subsequently submit an attestation to ONC. We believe it will take approximately one hour on average for an applicant QHIN to submit a completed QHIN application. We believe it will also take approximately one hour on average for a QHIN to complete and submit to ONC their attestation and required documentation. We expect a general office clerk could complete these required responsibilities.[262] We welcome comments if interested parties believe more or fewer QHINs should be included in our estimate. We also welcome comments if interested parties believe more or less time should be included in our estimate.

Table 2. Estimated Annualized Total Burden Hours for QHINs to Comply with Application and Attestation Requirements

Code of Federal Regulations Section	Number of Applicant QHIN or QHINs	Average Burden Hours	Total
45 CFR 172.301	15	1	15
45 CFR 172.701	15	1	15
Total Burden Hours			30

[262] According to the May 2022 BLS occupational employment statistics, the mean hourly wage for Office Clerks, General (43–9061) is $19.78.

B. ONC–ACBs

We propose in § 170.556(d)(7), new requirements for an ONC–ACB to report specific information to ONC when a developer fails to timely complete an approved corrective action plan (CAP). This proposal would apply to an identified non-conformity with respect to any Program requirement codified in subpart D for which an ONC–ACB has responsibilities under § 170.523. Under this proposal in § 170.556(d)(7), an ONC–ACB would be required to notify the National Coordinator when an ONC–ACB's requirement to initiate suspension procedures is triggered by the developer's failure to engage (successfully or failure to engage at all, as applicable) with the CAP process for a non-conformity to a Maintenance of Certification requirement.

We propose in § 170.556(d)(7)(ii) that an ONC–ACB must report certain information to ONC when a developer fails to submit an approved CAP or to complete an approved CAP with respect to any Program requirement codified in subpart D for which an ONC–ACB has responsibilities under § 170.523. We propose the ONC–ACBs would report the information specified in § 170.523(x) to the National Coordinator pursuant to the requirements in § 170.556(d)(7)(i) and must notify the developer immediately when an ONC–ACB begins the notification procedures in paragraph § 170.556(d)(7)(i).

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). We continue to estimate fewer than 10 ONC–ACB respondents for all of the regulatory ''collection of information'' requirements under part 170 of Title 45. We welcome comments on this conclusion and our supporting rationale for this conclusion.

IX. Regulatory Impact Analysis

A. Statement of Need

This proposed rule is necessary to meet our statutory responsibilities under the Cures Act and to advance HHS policy goals to promote interoperability and mitigate burden for health IT developers and users. Policies that could result in monetary costs for health IT developers and users include: (1) updates to ONC Certification Criteria for Health IT; and (2) developing the Patient, Provider, and Payer APIs.

While much of this proposed rule's costs will fall on health IT developers who seek to certify health IT under the Program, we believe the implementation and use of ONC Certification Criteria for health IT, Dynamic Client Registration Protocol and the provisions related to information blocking will 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 proposed rule will remove barriers to interoperability and EHI exchange, which will greatly benefit health care providers and patients.

We note in this RIA that there were instances in which we had difficulty quantifying certain benefits due to a lack of applicable studies, data, or both. However, in such instances, we highlight the significant non-quantified benefits of our policies to advance an interoperable health system that empowers individuals to use their EHI to the fullest extent and enables health care providers and communities to deliver smarter, safer, and more efficient care.

B. Alternatives Considered

If there are alternatives to our policies, we have described them within each of the sections within this RIA. In some cases, we have been unable to identify alternatives that would appropriately implement our responsibilities under the Cures Act and support interoperability consistent with our policy goals. We believe our policies take the necessary steps to fulfill the mandates specified in the PHSA, as amended by the HITECH Act and the Cures Act, in the least burdensome way. We welcome comments on our assessment and any alternatives we should consider.

C. Overall Impact

1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis

We have examined the impacts of this 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 14094 entitled ''Modernizing Regulatory Review'' (April 6, 2023), the Regulatory Flexibility Act (RFA) (September 19, 1980, Pub. L. 96354), section 1102(b) of the Social Security Act, section 202 of the Unfunded Mandates reform Act of 1995 (March 22, 1995; Pub. L. 104–4), and the Executive Order 13132 on Federalism (August 4, 1999).

Executive Orders 12866 and 13563 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). The Executive Order 14094 entitled ''Modernizing Regulatory Review'' (hereinafter, the Modernizing E.O.) amends section 3(f)(1) of Executive Order 12866 (Regulatory Planning and Review). The amended section 3(f) of Executive Order 12866 defines a ''significant regulatory action'' as an action that is likely to result in a rule: (1) having an annual effect on the economy of $200 million or more in any 1 year (adjusted every 3 years by the Administrator of OIRA for changes in gross domestic product), or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, territorial, or Tribal governments or communities; (2) creating a serious inconsistency or otherwise interfering with an action taken or planned by another agency; (3) materially altering the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise legal or policy issues for which centralized review would meaningfully further the President's priorities or the principles set forth in this Executive Order, as specifically authorized in a timely manner by the Administrator of OIRA in each case.

A regulatory impact analysis (RIA) must be prepared for major rules with significant regulatory action(s) and/or with significant effects as per section 3(f)(1) ($200 million or more in any 1 year). Based on our estimates, this rulemaking is significant per section 3(f)(1) as measured by the $200 million or more in any 1-year threshold.

a. Costs and Benefits

We have estimated the potential monetary costs and benefits of this proposed rule for health IT developers, health care providers, patients, and the Federal Government (*i.e.,* ONC), and have broken those costs and benefits out by section. In accordance with Executive Order 12866, we have included the RIA summary table as Table 80. The impact analysis primarily assesses the costs and benefits of proposed changes to the Program. The Program, as described elsewhere in this

rule, is voluntary. Developers who present their technology for certification do so for varied reasons, including so their users can meet Federal requirements and to demonstrate conformance with federally adopted standards. However, we recognize there are real costs associated with any changes to certified health IT and requirements for developers of certified health IT to maintain certification. We estimate these costs to the best of our ability, examining the development tasks and burden associated with each proposal. We also estimate and articulate the expected benefits of these proposals. Whereas we estimate the costs associated with development tasks for developers of certified health IT, benefits can be more far reaching—affecting developers directly through standards harmonization and clear processes for technology development as well as health care providers, patients, and payers who are end-users of the technology and whose use derives direct benefit through improvements to electronic health information exchange, access to electronic health information, and automation of clinical and administrative processes. Although participation in the Program is voluntary, we believe that requirements to use certified health IT by Federal programs, to adopt health IT standards, and exchange and make data available to health care providers, patients, and payers provide levers to technology developers to present their IT for certification. Program requirements are meant to harmonize health IT development and promote interoperability through common health IT standards and rules of information exchange and access. The benefits described more thoroughly, below, such as those for interoperability, as we have described in prior rulemaking, such as the ONC Cures Final Rule (85 FR 25642), are derived from more universal adoption of these standards and rules that enable data to be electronically recorded, stored, exchanged, and accessed more harmoniously. These actions may remove artificial barriers to information exchange and access that often result in the duplication of diagnostic and laboratory testing, fragmented care, missing medical record information, and less consumer choice in the healthcare market.[263] [264]

Our cost calculations quantify health IT developers' time and effort to implement these policies through new development and administrative activities. Our cost estimates use publicly available data and information, if available, to estimate time and effort. We also, where applicable, carry forward cost estimates from prior rulemakings to be consistent in time and effort estimates. Novel cost estimates also use a mix of subject matter expertise and appropriate proxies to quantify costs. We note these methods and sources in the tables. We recognize that the costs developers incur as a result of these policies may be passed on to certified health IT end-users. These end-users include, but are not limited to, the nearly 5,000 non-Federal hospitals that provide acute, inpatient care and over 1 million clinicians who provide outpatient care to all Americans. Official statistics show that nearly all U.S. non-Federal acute care hospitals and the vast majority of outpatient physicians use certified health IT.[265] [266] These policies affect the technology that all these health care providers use.

However, we are clear in our analysis and estimates of costs, below, that we do not assess the costs on health care providers to use this technology. This may include changes to how the provider electronically documents information in the medical record, changes to workflow, or how technology is implemented by a provider and at a particular health care delivery site. The costs estimate the expected burden on health IT developers to develop and provide the revised technology to their users, not the expected burden on users to use the revised technology, which is considered out of scope for this rulemaking, as we do not require the use of the technology, just the development of the technology. Other Federal agencies do require, as of their official rulemaking and policymaking, the use of certified health IT to participate in programs or receive payment for treating a patient. The costs and benefits of these requirements on health care providers to adopt and use certified health IT are estimated and explained in those rules' regulatory impact analysis. For example, the CMS Interoperability and Prior Authorization final rule (89 FR 8758) describes how the implementation of electronic, standards-based prior authorization and other information exchange integrated into the EHR can reduce burden on patients, providers, and payers resulting in an estimated $15 billion of savings over ten years. The proposals described below will help establish and build these standards and other technology into certified health IT for use by health care providers and others to achieve these estimated savings.

The benefits, both quantifiable and not quantifiable, articulated in this impact analysis have the potential to remove barriers to interoperability and EHI exchange for all these health care providers. Though these policies first require effort by developers of certified health IT to reflect them in their software, they must then be implemented by end-users to achieve the stated benefits—to improve healthcare delivery and the overall efficacy of the technology to document, transmit, and integrate EHI across multiple data systems.

To this end, we acknowledge that these estimated costs may not be borne solely by the developers of certified health IT and could be passed on to end-users through health IT developers' licensing, maintenance, and other operating fees and costs. We assume health IT developers may pass on up to the estimated costs of these policies, but not amounts above those estimated totals. We request comment on the increase in software licensing costs and other fees resulting from these proposals and if ongoing licensing costs and fees already consider the costs of meeting new regulations and certification requirements (*i.e.,* some or none of the estimated costs of this proposed rulemaking would be passed on to technology end-users.)

However, we have limited data on the fees and costs charged by health IT developers and how those fees and costs are distributed across various customer organizations. Given the ongoing nature of updates made by ONC to the Program, EHR developers may have already built in the costs associated with making these updates in their existing contracts. To the extent the costs associated with the updates have not been taken into account, these costs may be passed on to end-users in different ways by developers of certified health IT and across different health care provider organization types. Large integrated healthcare systems may face different fees and other pricing than different sized or structured health care provider organizations. The incredible

[263] Jones SS, Rudin RS, Perry T, Shekelle PG. Health information technology: an updated systematic review with a focus on meaningful use. Ann Intern Med. 2014 Jan 7;160(1):48–54. doi: 10.7326/M13–1531. PMID: 24573664.*https://pubmed.ncbi.nlm.nih.gov/24573664/.*

[264] Everson J, Adler-Milstein J. Sharing information electronically with other hospitals is associated with increased sharing of patients. Health Serv Res. 2020 Feb;55(1):128–135. doi: 10.1111/1475–6773.13240. Epub 2019 Nov 12. PMID: 31721183; PMCID: PMC6980958.*https://pubmed.ncbi.nlm.nih.gov/31721183/.*

[265] *https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records.*

[266] *https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption.*

diversity of the healthcare system also limits our ability to accurately model how these costs could be passed on, even if there were data available to estimate how these policies might alter the pricing models and fee rates of the health IT developers we estimate will be impacted.

What we can say with more certainty is the overall impact of these policies on the healthcare system as a whole. These policies affect the certified technology used by the providers who give care to a vast majority of Americans. Nearly all emergency room visits, hospital stays, and regular check-ups are documented and managed using certified health IT. These policies affect the interoperability of EHI for these care events and patients' electronic access to their health information. Certified health IT is now a nearly ubiquitous part of U.S. healthcare, and the costs and benefits estimated here encompass the widespread use of these technologies and their impact on all facets of care.

Overall, it is highly speculative to quantify benefits associated with the new technical requirements and standards for certification criteria we have proposed in this proposed rule. Emerging technologies may be used in ways not originally predicted. For example, ONC helped support the development of SMART on FHIR®, which defines a process for an application to securely request access to data, and then receive and use that data. ONC could not have predicted the scale this technical approach has already achieved. Not only is it used to support major EHR products, but is also leveraged, for example, by numerous digital health and technology companies to connect and integrate with EHRs to provide healthcare and other services to app and digital services users.[267] It is also speculative to quantify benefits for specific stakeholders because benefits associated with many of ONC's policies, which advance interoperability, do not necessarily accrue to stakeholders making the investments in developing and implementing the technologies. Benefits related to interoperability are spread across the healthcare ecosystem and can be considered a societal benefit. We have sought to describe benefits for each of the specific policies, and we welcome comments on how to quantify these benefits across a variety of stakeholders.

We note that we have rounded all estimates to the nearest dollar and that all estimates are expressed in 2022 dollars as it is the most recent data available to address all cost and benefit estimates consistently. The wages used to derive the cost estimates are from the May 2022 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics.[268] We also 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 Proposed Regulations'' sections are used throughout this RIA.

For policies where research supported direct estimates of impact, we estimated the benefits. For policies where no such research was identified to be available, we developed estimates based on a reasonable proxy.

We note that interoperability can positively impact patient safety, efficacy, care coordination, and improve healthcare processes and other health-related outcomes.[269] However, achieving interoperability is a function of several factors including the capability of the technology used by health care providers. Therefore, to assess the benefits of our policies, we must first consider how to assess their respective effects on interoperability holding other factors constant.

Employee Assumptions and Hourly Wage

We have made employee assumptions about the level of expertise needed to complete the requirements in this section. Unless indicated otherwise, 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 2022.[270] We have assumed that other indirect costs (including benefits) are equal to 100% of pre-tax wages. Therefore, we have doubled the employee's hourly wage to account for other indirect costs. We have concluded that a 100% expenditure on benefits and overhead is an appropriate estimate based on research conducted by HHS.[271]

Unless otherwise noted, we have consistently used the May 2022 National Occupational Employment and Wage Estimates reported by the U.S. Bureau of Labor Statistics (BLS) to calculate private sector employee wage estimates (*e.g.,* health IT developers, health care providers, HINs, attorneys, etc.), as we believe BLS provides the most accurate and comprehensive wage data for private sector positions.[272] These wage estimates are a national average and we do not consider regional wage variation in our estimates. We also do not consider possible variation in the average wages for software developers in health care IT positions versus IT positions, more generally, which the BLS wage estimate is based upon. Just as with the General Schedule Federal Salary Classification calculations, we have assumed that other indirect costs (including benefits) are equal to 100% of pre-tax wages. We welcome comments on our methodology for estimating labor costs, including the effects of any regional or IT sector wage variation on our estimates.

Quantifying the Estimated Number of Health IT Developers and Products

In this section, we describe the methodology used to assess the potential impact of new certification requirements on the availability of certified products in the health IT market. This analysis is based on the number of health IT developers that certified Health IT Modules for the 2015 Edition and 2015 Edition Cures Update and the estimated number of developers that will participate in the future and the number of products these developers will certify.

We recognize that certification is ongoing for new requirements finalized

[267] Wesley Barker, Natalya Maisel, Catherine E Strawley, Grace K Israelit, Julia Adler-Milstein, Benjamin Rosner, A national survey of digital health company experiences with electronic health record application programming interfaces, Journal of the American Medical Informatics Association, Volume 31, Issue 4, April 2024, Pages 866–874, *https://doi.org/10.1093/jamia/ocae006.*

[268] May 2022 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. *https://www.bls.gov/oes/current/oes_nat.htm.*

[269] Nir Menachemi, Saurabh Rahurkar, Christopher A Harle, Joshua R Vest, The benefits of health information exchange: an updated systematic review, Journal of the American Medical Informatics Association, Volume 25, Issue 9, September 2018, Pages 1259–1265, *https://doi.org/10.1093/jamia/ocy035.*

[270] Office of Personnel and Management. 2022 General Schedule (GS) Locality Pay Tables *https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2022/general-schedule/.*

[271] *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/reports/guidelines-regulatory-impact-analysis.*

[272] May 2022 National Occupational Employment and Wage Estimates, United States. U.S. Bureau of Labor Statistics. *https://www.bls.gov/oes/current/oes_nat.htm.*

in ONC's HTI–1 Final Rule and ONC Cures Act Final Rule and the number of health IT developers certifying products to these requirements is subject to change. The figures for 2015 Edition in Table 3A reflect certifications through 2022 for products certified to 2015 Edition and 2015 Edition Cures Update requirements. Counts, therefore, do not account for all certificates as of the publication of this proposed rulemaking.

These estimates are based on observed and expected conformance to the Program requirements, market consolidation, industry trends and business decisions by participating developers, and other voluntary and involuntary withdrawals from the Program. We understand that there are possible effects from regulation on market competition. Regulatory changes can lead to withdrawal from the Program. Participation in the Program is voluntary and participants face a mix of incentives to test and certify their products. Some health IT developers participate to ensure their users, who must meet Federal requirements or receive incentives to adopt and use certified health IT, have certified technology that meets the most current requirements. Some others, like new entrants, certify to demonstrate conformance and adoption of specific standards and functionalities, despite not having a large user base. Over time, as the table, below, shows, the overall number of developers and certified products have gone down. This is due to both market dynamics (*e.g.,* developers stop production or close due to competition) and regulatory changes (*e.g.,* standards and functional requirements are too costly to adopt.) Market dynamics are expected as users select specific technology and some companies close due to lack of business. Some attrition may be due to the high ceiling to meet certain requirements, but our data show that few participants with a certain number of customer/technology users leave the program due to regulatory changes alone. Developers with low market share or no known users may leave the Program despite remaining in operation. We know of no known instance where a developer voluntarily left the program due to regulatory changes, leaving many technology users without certified health IT.

The number of participants and range of products in the Program remain diverse, providing choice to customers and ensuring competition in the market for certified health IT. Notably, changes to the program over time, like the focus on certifying ''health IT modules'' versus ''EHRs'' has created flexibility for new entrants to participate in the program and introduced more choice to technology users who may shop for a wider array of certified products. In Table 3A below, we quantify the number of participating developers and certified products for the 2011 Edition, 2014 Edition, and 2015 Edition. We found that the number of health IT developers certifying products between the 2011 Edition and 2014 Edition decreased by 22.1% and the number of certified products available decreased by 23.2%. Furthermore, we found that between the 2014 Edition and 2015 Edition the number of participating developers and certified products decreased by 38.3% and 33.9%, respectively.

Table 3A. Number of Developers and Products for the 2011 Edition, 2014 Edition, and 2015 Edition

	2011 Edition	2014 Edition	Change (%)	2015 Edition	Change (%)
Participating Health IT Developers	1,017	792	-22.1	510	-35.6
Certified Products Available	1,408	1,081	-23.2	758	-29.9

Note: Counts for 2015 Edition reflect all certificates through 2022. These counts include certificates that are active and withdrawn.

These figures give us insight into how participation in the Program and certification for individual certification editions has changed over time—the effect of both market and regulatory forces. Given historical trends and the asymmetric costs faced by developers of certified health IT with large and small client bases, we must consider the effect of certification requirements going into effect and adopted in this rulemaking on future participation in the Program to make our best estimates of the cost and benefits of this rulemaking.

As shown in Table 3B, through 2022, 510 health IT developers certified 758 products since the start of 2015 Edition certification. As of the end of 2022, 435 health IT developers certified 590 products with active certificates for the 2015 Edition or 2015 Edition Cures Update. This is a 15% decrease in the number of health IT developers and a 22% decrease in 2015 Edition certified products, overall. As of the end of 2021, 414 health IT developers certified 569 products with active certificates for the 2015 Edition or 2015 Edition Cures Update. Compared to the end of 2022, this represents a 1-year 5% increase in the number of developers of certified health IT and 4% increase in number of certified products from the end of 2021.

Table 3B. Number of Developers and Products for the 2015 Edition and 2015 Cures Update

	2015 Edition Overall[1]	2015 Edition, a/o 2021[2]	Change (%)	2015 Edition, a/o 2022[2]	1-year change (%)	Overall change (%)
Participating Health IT Developers	510	414	-18.8	435	5.1	-14.7
Certified Products Available	758	569	-24.9	590	3.7	-22.2

Note: (1) Counts for 2015 Edition/2015 Cures Update reflect all certificates through 2022. These counts include certificates that are active and withdrawn. (2) Counts, as of 2021 and 2022, include active certificates only.

However, we expect, as we modeled in the HTI–1 Final Rule,[273] that new requirements finalized by that rulemaking may lead to some exits from the Program. We assume this modeled attrition estimated for the HTI–1 Final Rule will affect the estimated number of developers of certified health IT and number of certified products that will be required to meet requirements proposed in this rulemaking. For the HTI–1 Final Rule, we estimated an 11% decrease in the number of health IT developers and a 12% decrease in the number of certified products.[274] As shown in Table 4, we use this expected attrition to estimate the numbers of developers and products that would be required to meet the proposed requirements, consistent with what we forecasted for the HTI–1 Final Rule. We do not estimate additional attrition resulting from this rule, but rather carry forward the estimated number of developers and products we expect will participate in the Program at the time when these proposed policies are required to be met. We estimate that 387 developers of certified health IT and 521 certified products will be impacted by this rulemaking. These estimates will be used throughout this RIA to model estimated costs and benefits. We request comment on the quantification of attrition from the Program that may result from these proposed policies.

Table 4. Estimated Number of Developers and Products

Scenario	Estimated number of health IT developers	Estimated number of products
All Products – End of 2022	435	590
All Products – Modeled Attrition	387 (-11%)	521 (-12%)

Note: End of 2022 counts reflect active products only.

Number of End Users That Might Be Impacted by ONC's Proposed Regulations

For the purpose of this analysis, the population of end users impacted are the number of health care providers that possess certified health IT. Due to data limitations, our analysis is based on the number of hospitals and clinicians who participate in Medicare and who may be required to use certified health IT to participate in various CMS programs, inclusive of those providers who received incentive payments to adopt certified health IT as part of the Medicare EHR Incentive Program (now known as the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category under MIPS).

One limitation of this approach is that we are unable to account for the impact of our provisions on users of certified health IT that were ineligible or did not participate in the CMS EHR Incentive Programs or current Medicare programs (*e.g.,* the Medicare Promoting Interoperability Program). For example, in 2017, 78% of home health agencies and 66% of skilled nursing facilities reported adopting an EHR.[275] 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, these Medicare program participants represent an adequate sample on which to base our estimates. An analysis of the CMS Provider of Services file for Hospitals and CMS National Downloadable File of Doctors and Clinicians provides a current accounting of Medicare-participating hospitals and practice locations. [276] [277] In total, we estimated about 4,800 non-Federal acute care hospitals from the Provider of Services file and 1.25 million clinicians (including doctors and advanced nurse practitioners) across over 350,000 practice locations. If we assume that 96% of these hospitals and 80% of these practice locations use certified health IT, as survey data estimate, approximately 4,600 hospitals and 283,000 practice locations may face some passed-on costs from these requirements.[278] [279]

[273] *https://www.federalregister.gov/d/2023-28857/p-2446.*

[274] *https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and. See* Regulatory Impact Analysis.

[275] *https://www.healthit.gov/data/data-briefs/electronic-health-record-adoption-and-interoperability-among-us-skilled-nursing.*

[276] *https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-hospital-non-hospital-facilities.*

[277] *https://data.cms.gov/provider-data/dataset/mj5m-pzi6.*

[278] *https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records.*

[279] *https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption.*

We understand there will likely not be a proportional impact of these costs across all health care providers. We can assume a hospital will face different costs than a physician practice, and no two hospitals will face the same costs, as those costs may vary based upon various characteristics, including but not limited to: staff size, patient volume, and ownership. The same is true for individual clinical practices, for which costs may vary across the same characteristics as hospitals. However, given our limited data, our approach to model pass-through costs onto health care providers assumes that hospitals face the same average costs and that they face a higher average cost per site than an individual clinical practice. Furthermore, we assume that clinical practices face the same average costs and lower average costs per site than the average hospital.

Based upon our prior modeling work for the ONC Cures Act Final Rule in 85 FR 25642, we assume that one-third of estimated costs will be passed on to hospitals and the remaining amount on to clinician practices.[280] This estimate is based off an analysis of the proportion of Medicare EHR Incentive Program dollars that went to eligible hospitals versus eligible professionals.[281] We found that one-third of those program dollars were paid to hospitals, representing the disproportionate cost of health IT investments by a single hospital versus a single clinician. Table 5 shows an assumed distribution of the costs across technology users. The cost to any one hospital or practice is small compared to the cost as a whole. The average hospital user of certified health IT could be expected to face up to $69,203 on average additional costs associated with implementing technology that adopt these policies. The average clinician practice site could be expected to face up to $2,250 on average additional costs associated with implementing technology that adopt these policies. These are considered pass-through costs incurred by the health IT developer to adopt these policies and not additional costs exogenous to health IT developer efforts to adopt and engineer these policies into their certified health IT. To the extent that the increase in prices is large, the pass-through of costs onto consumers might decrease the quantity of care demanded. Given the below estimates for per provider costs, which could subsequently be defrayed across patients within the system, ONC does not believe this additional market distortion is likely to produce a substantial impact on the expected costs of the rule.

Table 5. Estimated Pass-through Costs per Health Care Provider

Health Care Provider	Est. Count	Est. $ Per Provider	Total $ Cost
Hospitals	4,600	$69,203	$318m
Clinical Practices	283,000	$2,250	$637m
All	287,600	$3,321	$955m

These costs are not expected to be borne at once. Requirements from this proposed rulemaking may be implemented over several years, so in some cases an individual hospital or clinician's share of pass-through costs from their health IT developer may be distributed over one or more years. One issue to reiterate is that some of these costs may have already been incorporated within existing contracts and thus it is possible that the actual additional costs experienced by hospitals and clinicians may be lower than what is estimated. We do not have insights into proprietary contracts between EHR developers and their clients, and thus cannot speculate the extent to which the estimated additional costs will be passed on to their clients.

It's unknown if the estimated benefits will have the same distribution. A single clinician may not benefit the same as a single hospital, nor will one hospital benefit the same as another. However, given the same constraints to model costs across different provider types, we choose to assume a similar distribution for benefits as we propose for costs.

1. The United States Core Data for Interoperability Standard (USCDI) v4

The USCDI standard in § 170.213 is a baseline set of data that can be commonly exchanged across care settings for a wide range of uses. Certain certification criteria in § 170.315 currently require the use of the USCDI standard in § 170.213. We propose to update the USCDI standard in § 170.213 by adding USCDI v4. We propose to add USCDI v4 in § 170.213(c) and incorporate it by reference in § 170.299. We propose that as of January 1, 2028, any Health IT Modules seeking certification to certification criteria referencing § 170.213 would need to be capable of exchanging the data elements that the USCDI v4 comprises.

Additionally, we propose that for purposes of the Program, the adoption of USCDI v3 expires on January 1, 2028. We propose that, for a health IT module certified to a criterion in § 170.315 that references a version of the USCDI standard adopted in § 170.213 that is expired, a health IT developer must update the module to a version of the standard that is not expired and provide the updated version to their customers according to the expiration date or dates defined for that standard in order to maintain certification of that Health IT Module as described in § 170.315. The following certification criteria currently reference the USCDI standard via cross-reference to § 170.213:

- ''Care coordination—Transitions of care—Create'' (§ 170.315(b)(1)(iii)(A)(*1*) and (*2*));
- ''Care coordination—Clinical information reconciliation and incorporation—Reconciliation'' (§ 170.315(b)(2)(iii)(D)(*1*)–(*3*));
- ''Decision support interventions—Decision support configuration'' (§ 170.315(b)(11)(ii) (A) and (B), and (iv)(A)(*5*)–(*13*));
- ''Patient engagement—View, download, and transmit to 3rd party—View'' (§ 170.315(e)(1)(i)(A)(*1*) and (*2*), and (iii));
- ''Transmission to public health agencies—electronic case reporting'' (§ 170.315(f)(5)(i)(C)(2)(i))—Referenced until December 31, 2025;
- ''Design and performance—Consolidated CDA creation performance'' (§ 170.315(g)(6)(i)(A) and (B));

[280] *https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification.*

[281] *https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs.*

- ''Design and performance—Application access—all data request—Functional requirements'' (§ 170.315(g)(9)(i)(A)(*1*) and (2)); and
- ''Design and performance—Standardized API for patient and population services—Data response'' (§ 170.315(g)(10)(i)(A) and (B)).

If we finalize our proposal, all the above criteria, except for ''Transmission to public health agencies—electronic case reporting'', whose reference expires December 31, 2025, would refer to USCDI v4.

Costs

The USCDI v4 adds one new data class and 20 new data elements that were not in USCDI v3. This will require updates to the Consolidated Clinical Document Architecture (C–CDA) standard, the FHIR US Core Implementation Guide, and updates to the certification criteria listed above. We have estimated the proposed cost to health IT developers to add support for the additional data classes and data elements in USCDI v4 in C–CDA, and to make the necessary updates to the affected certification criteria. Both the lower and upper bound estimates in Table 6 assume 50% less effort to update technology to include new data elements introduced in USCDI version 4 compared to USCDI version 3. For the HTI–1 Final Rule (89 FR 1214), we estimated that up to 3,600 hours and as few as 1,800 hours would be needed to update technology from version 1 to version 3. These estimates are detailed in Tables 6 and 7 below and are based on the following assumptions:

1. Health IT developers will experience the assumed average costs of labor and data model use. Table 6 shows the estimated labor costs per product for a health IT developer to develop support for the additional data elements and data classes in USCDI v4 for each 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, on average, the costs noted in Table 7.

2. We estimate that 339 products certified by 263 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this proposal. However, not all these developers and products certify to USCDI applicable certification criteria and need to meet the USCDI update requirements. As of the end of 2022, 68% of developers and 65% of products certified to one of the certification criteria that cross-reference the USCDI standard in § 170.213, listed above. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the USCDI updates. In Table 7, we also applied separate modifiers for individual certification criteria, calculated from an analysis of certificates through 2022. This allows us to more accurately assess USCDI update costs for individual certification criteria.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. As noted previously, we have assumed that other indirect costs (including benefits) are equal to 100 percent of pre-tax wages, so the hourly wage including other indirect costs is $127.82.

BILLING CODE 4150–45–P

Table 6. Costs to Health IT Developers to Develop Support for the Additional USCDI Data Elements in C-CDA Standard and Affected Certification Criteria

Tasks	Details	Lower Bound Hours	Upper Bound Hours	Remarks
Update C-CDA creation	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	900	1,800	(1) Lower bound assumes USCDIv4 data elements have started to be incorporated in the certified product through the ONC Standards Version Advancement Process (SVAP). (2) Upper bound assumes certified product conforms only to USCDIv3 and needs to be updated to fully conform with USCDIv4.
§ 170.315(b)(1)(iii)(A)(*1*) and (*2*) Care coordination – Transitions of Care - Create	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	
§ 170.315(b)(2)(iii)(D)(*1*) through (*3*) Care coordination - Clinical information reconciliation and incorporation - Reconciliation	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	
§ 170.315(b)(11)(ii)(A) and (B), and (iv)(A)(*5*)-(*13*)) Decision support interventions – Decision support configuration	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	

§ 170.315(e)(1)(i)(A)(*1*) and (*2*), and (iii) Patient engagement - View, download, and transmit to 3rd party - View	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	
§ 170.315(g)(6)(i)(A) and (B) Design and performance - Consolidated CDA creation performance	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	
§ 170.315(g)(9)(i)(A)(*1*) and (*2*) Design and performance - Application access – all data request – Functional requirements	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	
§ 170.315(g)(10)(i)(A) and (B) Design and performance - Standardized API for patient and population services – Data response	New development to support USCDI v4 updates and changes to data classes and constituent data elements for C-CDA Edition 3	100	300	

Table 7. Total Cost to Develop Support for the Additional USCDI Data Elements in C-CDA Standard and Affected Certification Criteria [2022 dollars]

Tasks	Estimated number of products	Estimated Cost	
		Lower Bound	Upper Bound
Update C-CDA creation	333	$38,307,654	$76,615,308
Updates to § 170.315(b)(1)	276	$3,527,832	$10,583,496
Updates to § 170.315(b)(2)	250	$3,195,500	$9,586,500
Updates to § 170.315(b)(11)	297	$3,796,254	$11,388,762
Updates to § 170.315(e)(1)	240	$3,067,680	$9,203,040
Updates to § 170.315(g)(6)	333	$4,256,406	$12,769,218
Updates to § 170.315(g)(9)	261	$3,336,102	$10,008,306
Updates to § 170.15(g)(10)	224	$2,863,168	$8,589,504
Total Cost	333	$62,350,596	$148,744,134

Notes: The number of estimated products that certify applicable certification criteria vary. We estimated separate modifiers for each certification criterion to estimate the number of products impacted by the USCDI updates. Estimates reflect the percent of all products that certify a criterion through 2022. Modifiers: (b)(1): 53%; (b)(2): 48%; (b)(11): 57%; (e)(1): 46%; (g)(6): 64%; (g)(9): 50%; (g)(10): 43%. This estimate is subject to change.

BILLING CODE 4150–45–C

The cost to a health IT developer to develop support for the additional USCDI data classes and elements vary by the number of applicable certification criteria certified for a Health IT Module. On average, the cost to update C–CDA creation to support the additional USCDI data elements range from $115,038 to $230,076 per product. The cost to make updates to individual certification criteria to support the new data classes and elements range from $12,782 to $38,346 per product. Therefore, assuming 333 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers would, on average, range from $62 million to $149 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.

Benefits

We believe this proposal would benefit health care providers, patients, and the health IT industry as a whole. The USCDI comprises a core set of structured and unstructured data needed to support patient care and facilitate patient access using health IT; establishes a consistent baseline of harmonized data elements that can be broadly reused across use cases, including those outside of patient care and patient access; and will expand over time via a predictable, transparent, and collaborative process, weighing both anticipated benefits and industry-wide impacts. The additional data elements in USCDI v4 expand the baseline set of data available for health information exchange and thus provide more comprehensive health data for both providers and patients.[282] We expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality healthcare provided. In addition, we believe the increased availability of the additional data elements in USCDI v4 as interoperable structured data will facilitate improvements in the efficiency, accuracy, and timeliness of public health reporting, quality measurement, health care operations, and clinical research. However, we are not aware of an approach for quantifying these benefits and welcome comments on potential approaches to quantifying these benefits.

[282] *https://www.healthit.gov/sites/default/files/page/2023-07/Standards_Bulletin_2023-2.pdf.*

2. SMART App Launch 2.2

We propose to adopt SMART App Launch version 2.2. SMART App Launch version 2.0 is the most recently adopted version for use in the ONC certification program in the HTI–1 Final Rule (89 FR 1291 through 1296). Version 2.2 adds important new enhancements and features that improve upon version 2.0. However, we do not believe the adoption of the new enhancements will require additional burden beyond current program requirements to implement. We believe the effort to update health IT modules to the standard version will be *de minimis.* We request public comment on the effort needed to update to the new standard version.

3. User-Access Brands and Endpoints

In the ONC HTI–1 Final Rule, we finalized requirements in § 170.404(b)(2) that for all Health IT Modules certified to § 170.315(g)(10, Certified API Developers must publish certain service base URLs and related organization details in a standardized FHIR format (89 FR 1285 through 1290). Currently, user-access brands (Brands) is a sub-specification in the HL7 FHIR SMART Application Launch Framework Implementation Guide Release 2.2.0 (SMART v2.2 Guide). Brands provides guidelines for API providers to publish ''Brands'' associated with their FHIR endpoints that apps can collect and present to users. Each Brand can include information like organization name, location, identifier, patient portal details, FHIR API Endpoint, and more. These Brands are assembled in FHIR ''Bundle'' format, and these Bundles can made available in two ways: by FHIR servers including a link in their ''.well-known/smart-configuration'' metadata file, or through vendor-consolidated Brand Bundles that are openly published. The specification is very similar to the service base URLs requirement finalized in the HTI–1 Final Rule, and we believe the effort to adopt Brands will be de minimis. Our proposal to adopt Brands, in section III.B.3, will align with industry practice and standards, ensuring the service base URL requirements remain in line with best development practice. We request public comment on the additional effort beyond current requirements needed to adopt PAB.

4. Standards for Encryption and Decryption of Electronic Health Information

We propose to adopt the October 12, 2021, version of Annex A of the FIPS Publication 140–2 in § 170.210(a)(3).

Adopting the October 12, 2021, version of Annex A of the FIPS Publication 140–2 in § 170.210(a)(3) would implicate three certification criteria that reference standards in § 170.210(a):

- § 170.315(d)(7) End-user device encryption, which we propose to rename ''Health IT encryption'';
- § 170.315(d)(9) Trusted connection; and
- § 170.315(d)(12) Encrypt authentication credentials, which we propose to rename ''Protect stored authentication credentials''.

Since the finalization of the 2015 Edition Final Rule that adopted the October 8, 2014 version of Annex A of FIPS 140–2 in § 170.210(a)(2), encryption techniques and security best practices have continued to advance. The National Institute of Standards and Technology (NIST) has published several updated versions of Annex A of the FIPS Publication 140–2.[283] FIPS 140–2 specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments.[284] Adopting the, October 12, 2021, version of Annex A of the FIPS Publication 140–2 in § 170.210(a)(3) will help ensure patients' data are protected and cybersecurity risks are mitigated.[285]

Costs

This proposal updates the standard referenced by § 170.315(d)(7), (d)(9), and (d)(12) to include an updated set of encryption algorithms identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2, Security Requirements for Cryptographic Modules, October 8, 2014. The proposed change updates the standards referenced and does not change the functional requirements to test and certify the aforementioned certification criteria. We estimate effort to be de minimis for certified health IT developers, since the proposal does not functionally change how developers must meet the certification criteria's requirements.

[283] *See* pages 4–6 of the October 12, 2021 version of Annex A for a revision history of the standard. Available at: *https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.*

[284] *https://csrc.nist.gov/pubs/fips/140-2/upd2/final.*

[285] *https://davidhoglund.typepad.com/files/white-paper---fips-in-medical-environments-0919.pdf.*

5. Minimum Standards for Code Sets Updates

We established a policy in the 2015 Edition Final Rule for minimum standards code sets that update frequently (80 FR 62612). As we stated in the HTI–1 Final Rule, when determining whether to propose newer versions of minimum standards code sets, we consider the impact on interoperability and whether a newer version would require substantive effort for developers of certified health IT to implement (89 FR 1224). If adopted, newer versions of minimum standards code sets would serve as the baseline for certification and developers of certified health IT would be able to use newer versions of these adopted standards on a voluntary basis. While minimum standard code sets update frequently, perhaps several times in a single year, these updates are confined to concepts within the code system, not substantive changes to the standards themselves. We do not assess the burden to voluntarily adopt the updated code sets.

6. New Imaging Requirements for Health IT Modules

We propose to revise the certification criteria found at ''transitions of care'' in § 170.315(b)(1); ''application access—all data request'' in § 170.315(g)(9); and ''standardized API for patient and population services'' in § 170.315(g)(10) to include certification requirements to support capturing and documenting hyperlinks to diagnostic imaging. We also propose to revise the certification criterion ''view, download, and transmit to 3rd party'' in § 170.315(e)(1) to add functional support for (a) viewing and direct download of diagnostic and lower quality images and (b) inclusion of a hyperlink to those diagnostic images in either a downloaded or transmitted Continuity of Care Document (CCD). The view and download functionalities must be accessible to the patient through the same internet-based technology as the other functionalities of § 170.315(e)(1).

We are not, however, proposing a specific standard associated with the support of this functionality, and we note that this requirement can be met with a context-sensitive link to an external application which provides access to images and their associated narrative. A Health IT Module certified to these certification criteria is not required to support a specific standard. We believe that this proposal will promote more consistent access to images for providers.

Costs

The proposed revisions to §§ 170.315(b)(1), 170.315(g)(9), 170.315(g)(10), and 170.315(e)(1) require modifications to the currently adopted certification criteria to support capturing and documenting hyperlinks to diagnostic imaging and view and download of the diagnostic images by patients. These tasks have their own levels of effort, and their estimates are detailed in Tables 8 and 9 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 8 shows the estimated labor costs per product to modify § 170.315(b)(1), § 170.315(g)(9), § 170.315(g)(10), and § 170.315(e)(1). 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 9.

2. We estimate that 330 products certified by 256 developers will be affected by our proposal. These estimates are a subset of the total estimated number of health IT developers and certified products we estimated above.

The estimate of 330 products certified by 256 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers certify all of these products to § 170.315(b)(1), § 170.315(g)(9), § 170.315(g)(10), and § 170.315(e)(1) certification criteria and need to meet the proposed requirements. As of the end of 2022, 60% of developers and 53% of products certified to § 170.315(b)(1); 56% of developers and 50% of products certified to § 170.315(g)(9); 47% of developers and 43% of products certified to § 170.315(g)(10); and 53% of developers and 46% of products certified to § 170.315(e)(1). We, then, calculated the percentage of developers and products that certify to any of the four certification criteria to estimate the total of products and developments impacted by this proposal overall. We applied these modifiers to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

Table 8. Estimated Labor Hours to Modify §§ 170.315(b)(1), 170.315(g)(9), 170.315(g)(10), and 170.315(e)(1)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: § 170.315(b)(1): support capturing and documenting hyperlinks to diagnostic imaging	No specific standard associated with the support of this functionality, and we note that this requirement can be met with a context-sensitive link to an external application which provides access to images and their associated narrative.	100	300	Lower bound: Assumes Health IT Modules document hyperlinks to diagnostic imaging but must map to be included in transition of care/referral summary document. Upper bound: Assumes health IT does not capture and document hyperlinks to diagnostic imaging and must build this functionality.
Task 2: § 170.315(g)(9): support capturing and documenting hyperlinks to diagnostic imaging		100	300	
Task 3: § 170.315(g)(10): support capturing and documenting hyperlinks to diagnostic imaging		100	300	
Task 4: § 170.315(e)(1): (a) viewing and direct download of diagnostic and lower quality images and (b) inclusion of a hyperlink to those diagnostic images in either a downloaded or transmitted Continuity of Care Document (CCD)		250	500	Lower bound: Assumes Health IT Modules document hyperlinks to diagnostic imaging but must enable patient access to hyperlinks through access portal. Upper bound: Assumes health IT does not capture and document hyperlinks to diagnostic imaging and must build this functionality.

Table 9. Total Cost to Modify §§ 170.315(b)(1), 170.315(g)(9), 170.315(g)(10), and 170.315(e)(1) [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (276 products)	$3,527,832	$10,583,496
Task 2 (261 products)	$3,336,102	$10,008,306
Task 3 (224 products)	$2,863,168	$8,589,504
Task 4 (240 products)	$7,669,200	$15,338,400
Total (330 products and 256 developers)	$17,396,302	$44,519,706

BILLING CODE 4150–45–C

The cost to a health IT developer to modify § 170.315(b)(1), § 170.315(g)(9), § 170.315(g)(10), and § 170.315(e)(1) for their Health IT Modules would range from $52,716 to $134,908 per product, on average. Therefore, assuming 330 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, would range from $17.4 million to $44.5 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to patient access and interoperable exchange of health information to significantly benefit patients and health care providers and improve the quality of health care provided. Better capture and documentation of diagnostic imaging results within the electronic health record can promote greater access to this information at the point of care and enable improvements to interoperable exchange of these results between health care providers, which can reduce redundant testing and support diagnostics. Furthermore, making diagnostic imaging results electronically available to patients through their online medical records may further enable patient-mediated exchange with other health care providers. Patients would be able to access the imaging results online, download the images to their personal device, and securely transmit the results to their provider from their online medical record. Access and exchange of diagnostic imaging results is a known challenge, and these proposed modifications to the certification criteria are one step toward resolving barriers to exchange and access.

7. Revised Clinical Information Reconciliation and Incorporation Certification Criterion

We propose a primary proposal and an alternative proposal for revising the ''Clinical information reconciliation and incorporation'' certification criterion in § 170.315(b)(2) to expand the number and types of data elements that Health IT Modules certified to this criterion would be required to reconcile and incorporate. Our primary proposal would require Health IT Modules certified to this criterion to be capable of reconciling and incorporating all 21 data classes in USCDI Version 4 (v4), which would include expanding ''clinical information reconciliation and incorporation'' certification criterion to 18 new data classes beyond the existing three data classes presently required as part of the current certification criterion's functionality. Our alternative proposal would require Health IT Modules certified to this criterion to be capable of reconciling and incorporating six additional USCDI v4 data classes beyond the existing three data classes presently required as part of the current certification criterion's functionality. We also propose a new functional requirement that would allow end users to configure how their product handles information received from external sources.

Costs

The primary proposal would require Health IT Modules certified to this § 170.315(b)(2) to be capable of reconciling and incorporating all USCDI v4 data classes. We have estimated the proposed cost to health IT developers to reconcile and incorporate all USCDI v4 data classes. These estimates are detailed in Tables 10 to 13 below and are based on the following assumptions:

1. Health IT developers will experience the assumed average costs of labor and data model use. Tables 10 and 12 shows the estimated labor costs per product for a health IT developer to develop support for the additional data classes in USCDI v4. We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur, on average, the costs noted in Tables 11 and 13.

2. We estimate that 250 products certified by 209 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above and apply to both the primary and alternative proposal.

The estimate of 250 products certified by 209 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify to § 170.315(b)(2) certification criterion and need to meet the proposed requirements. As of the end of 2022, 54% of developers certified a product to the § 170.315(b)(2) certification criterion and 48% of all products were certified to the § 170.315(b)(2) certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

Table 10. Estimated Labor Hours to Incorporate All USCDI v4 Data Classes in § 170.315(b)(2) [2022 dollars]

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Support for additional data classes	Reconciliation and incorporation to support all USCDI v4 data classes beyond the existing three data classes	2700	8100	For the 2014 Edition EHR Certification Criteria, it was estimated that it would require 100-300 labor hours to implement two new data classes for the revised CIRI criterion. We assume a greater level of effort to reconcile and incorporate the new data classes proposed in this rulemaking, given the diversity of new data classes and level of their standardization. We estimate that 1 new data class will require 150 to 450 hours of development time.
Task 2: Automatic reconciliation and incorporation	Update technology to support automatic reconciliation and incorporation of data	1000	5000	
Task 3: Automatic incorporation rules	Provide functionality that allows users to set rules that would indicate specific data elements and/or specific data sources that can be automatically incorporated	500	2500	

Table 11. Total Cost to Incorporate All USCDI v4 Data Classes to Meet the Proposed Requirements in § 170.315(b)(2) [2022 dollars]

Activity	Estimated Number of Products	Estimated Cost	
		Lower bound	Upper bound
Task 1: Support for additional data classes	250	$86,278,500	$258,835,500
Task 2: Automatic reconciliation and incorporation	250	$31,955,000	$159,775,000
Task 3: Automatic incorporation rules	250	$15,977,500	$79,887,500
Total cost for all products (250 products)	**250**	**$134,211,000**	**$498,498,000**

Notes: We used a 48% modifier for the § 170.315(b)(2) certification criterion to estimate the number of products impacted by the Clinical Reconciliation and Incorporation updates. Estimates reflect the percent of all products that certify to the § 170.315(b)(2) certification criterion through 2022. This estimate is subject to change.

The cost to health IT developers to meet the proposed requirements in § 170.315(b)(2) would range from $536,844 to $1,993,992 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 250 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $134 million to $498 million.

Table 12. Estimated Labor Hours to Incorporate Six Additional USCDI Classes to Meet the Proposed Requirements in § 170.315(b)(2) [2022 dollars] [Alternative Proposal]

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Support for additional data classes	Reconciliation and incorporation to support 6 data classes beyond the existing three data classes	900	2700	For the 2014 Edition EHR Certification Criteria, it was estimated that it would require 100-300 labor hours to implement two new data classes for the revised CIRI criterion. We assume a greater level of effort to reconcile and incorporate the new data classes proposed in this rulemaking, given the diversity of new data classes and level of their standardization. We estimate that 1 new data class will require 150 to 450 hours of development time.
Task 2: Automatic reconciliation and incorporation	Update technology to support automatic reconciliation and incorporation of data	350	1700	
Task 3: Automatic incorporation rules	Provide functionality that allows users to set rules that would indicate specific data elements and/or specific data sources that can be automatically incorporated	170	850	

Table 13. Total Cost to Incorporate Six Additional USCDI Classes to Meet the Proposed Requirements in § 170.315(b)(2) [2022 dollars] [Alternative Proposal]

Activity	Estimated Number of Products	Estimated Cost	
		Lower bound	Upper bound
Task 1: Support for additional data classes	250	$28,759,500	$86,278,500
Task 2: Automatic reconciliation and incorporation	250	$11,184,250	$54,323,500
Task 3: Automatic incorporation rules	250	$5,432,350	$27,161,750
Total cost for all products (250 products)	**250**	**$45,376,100**	**$167,763,750**

Notes: We used a 48% modifier for the § 170.315(b)(2) certification criterion to estimate the number of products impacted by the Clinical Reconciliation and Incorporation updates. Estimates reflect the percent of all products that certify to the § 170.315 (b)(2) certification criterion through 2022. This estimate is subject to change.

Table 14. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(b)(2) [2022 dollars]

	Estimated Number of Products	Estimated Lower Bound Cost	Estimated Upper Bound Cost
Total cost for all products (250 products)	250	$45,376,100	$498,498,000

BILLING CODE 4150–45–C

The cost to health IT developers to meet the proposed alternative requirements in § 170.315(b)(2) would range from $178,948 to $664,664 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 250 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $45 million to $168 million.

Benefits

We believe this proposal would benefit health care providers, patients, and the health IT industry. Expanding our clinical information reconciliation and incorporation (certification criterion to include all USCDI data classes would expand functionality by encouraging developers to include features that would allow end users (*i.e.,* providers) to configure how their product handles information received from external sources, thus benefiting providers by reducing the burden of incorporation and reconciliation in clinical workflows, which may otherwise have occurred via manually documenting information from external source in the Health IT Module. By reducing the time clinicians spent on incorporation and reconciliation in clinical workflows, more quality time could be used on making clinical decisions.[286] Additionally, we believe that these requirements supporting automatic reconciliation would help equip providers with relevant and critical clinical information that can improve overall patient care and safety. For instance, automatic reconciliation of radiology reports and discharge summaries has demonstrated improvements in patient safety by identifying potentially undiagnosed limb abnormalities, this example is applicable to USCDI v4's data elements, including discharge summary note and diagnostic imaging report.[287] In a Hosseini, et al. study asking health care providers to reconcile healthcare information across multiple electronic documents from a health information exchange network, automatic reconciliation was more accurate and significantly reduced the reconciliation time for medications, referrals and problems (38.1%, 58.8%, and 65.1%, respectively).[288] Another Hosseini study showed automating reconciliation of Continuity of Care Documents took 3.3 minutes with high accuracy compared to manual reconciliation that required approximately 150 hours with the same data, resulting in additional staff time and cost savings.[289] [290]

These two studies offer supporting evidence on the potential benefits of our proposed updates to the certification criterion in § 170.315(b)(2) by

[286] *https://go.chilmarkresearch.com/from-connectivity-to-real-provider-usability.*

[287] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4765582/.*

[288] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6804409/pdf/ocy158.pdf.*

[289] *https://www.sciencedirect.com/science/article/pii/S1532046417301983.*

[290] *https://www.healthcareitnews.com/news/rural-hospital-improves-meds-reconciliation-ai-automation-ehr.*

expanding our existing CIRI certification requirements to additional data elements and promoting new capabilities that would benefit providers by reducing the burden of reconciliation and incorporation in clinical workflows. There are potential time and cost savings by using consolidated documents to reconcile patient information and automatic reconciliation to de-duplicate information received from external sources. Our proposal to expand CIRI certification requirements to include additional data elements and promoting new capabilities will help scale these benefits to create greater impact.

As information exchange, especially across large networks, grows, reconciling these documents—often received or pushed via automatic machine queries—can be a large burden on clinicians who must review and reconcile when new documents are received. For example, Carequality, a large national network that connects over 600,000 clinicians and 4,200 hospitals, alone claims to facilitate the exchange of 400,000,000 documents monthly.[291]

Measuring the volume of record exchange and the rate of reconciliation are important to fully quantify the impact and potential benefits of manual versus automatic reconciliation of these documents. For instance, in the Hosseini, et al. study referenced above, the authors studied the effect of manual review and reconciliation of over 500 documents and entries in three document data classes—Problems, Allergies, and Medications—and found an over 99% reduction in time spent comparing and de-duplicating the information across all documents manually versus through a software program.[292] However, how the reconciliation time savings for these data classes compare to other data classes proposed to be included in the certification criterion are unknown. In addition, the representativeness of the CCDs used in the study to all CCDs exchanged nationally is unknown. Whether the CCDs selected for the study present more or less burden to reconcile than the average document is unknown.

We seek public comments on our proposed updates to the certification criterion in § 170.315(b)(2). Specifically, we seek public comments on the (1) volume of documents received electronically from external sources where reconciliation is necessary, and automation would reduce clinician burden and (2) the similarity of reconciliation burden between the problems, allergies, and medications data classes included currently in the certification criterion and data classes proposed to be included in the certification criterion.

Although the exact benefits of these modifications are not quantifiable at this time, research has shown promising potential in cost savings, and we expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients while improving the quality of health care provided.[293] [294] Health care providers, patients, and the health IT industry will benefit from the proposed updates to the certified criterion through support of clinical information reconciliation and incorporation of an expanded list of data elements and functionalities that would increase standardization and interoperability better support of. We look forward to public comments that will inform the quantifiable benefits of this proposal.

8. Revised Electronic Prescribing Certification Criterion

We propose to update the ''electronic prescribing'' certification criterion in § 170.315(b)(3) to incorporate the NCPDP SCRIPT standard version 2023011. In addition to incorporating NCPDP SCRIPT standard version 2023011, we also propose updates to the current transactions included in § 170.315(b)(3), propose removing some transactions, and propose several new transactions considering new and updated developments in the NCPDP SCRIPT standard version 2023011 and other considerations, as well as other necessary updates to vocabulary standards and coding.

Costs

The proposed updates to the ''electronic prescribing'' certification criterion include six tasks: (1) incorporate NCPDP SCRIPT Standard Version 2023011 for all required transactions; (2) (i) require 8 Electronic Prior Authorization transactions, currently optional under the certification criterion, and (ii) adopt and require the PANotification transaction; (3) require Signatura (Sig) transaction and require that health IT developers must be able to send an unstructured Sig and a structured and codified Sig from a prescriber to a pharmacy containing a consistent expression for communication between the prescriber and the pharmacist, according to the standard; (4) adopt FDA National Drug Code (NDC) terminology for coded drugs; (5) adopt RxNorm July 5, 2022, Full Monthly Release, which updates the current reference to RxNorm, September 8, 2015; and (6) we propose in § 170.315(b)(3)(ii)(B) that a Health IT Module certified to the ''electronic prescribing'' certification criterion must enable a user to exchange race and ethnicity information for a patient when performing the following prescription-related electronic transactions: RxFill; RxChangeRequest, RxChangeResponse; CancelRx; and RxRenewalRequest, RxRenewalResponse in accordance with NCPDP SCRIPT Standard Version 2023011. These tasks have their own levels of effort, and these estimates are detailed in Tables 15 and 16 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 15 shows the estimated labor costs per product to modify the ''electronic prescribing'' certification criterion. 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 16.

2. We estimate that 208 products certified by 163 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 208 products certified by 163 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify to the ''electronic prescribing'' certification criterion and need to meet the proposed requirements. As of the end of 2022, 42% of developers and 40% of products certified to the ''electronic prescribing'' certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

[291] *https://carequality.org/.* Accessed: January 2, 2024.

[292] *https://www.sciencedirect.com/science/article/pii/S1532046417301983.*

[293] *https://academic.oup.com/jamia/article/19/3/328/2909132.*

[294] *https://www.healthcareitnews.com/news/rural-hospital-improves-meds-reconciliation-ai-automation-ehr.*

Table 15. Estimated Labor Hours to Modify § 170.315(b)(3) Electronic Prescribing Certification Criterion

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adopt NCPDP SCRIPT Standard Version 2023011 for all required transactions.[1]	Update required electronic prescribing transactions from NCPDP SCRIPT Standard Version 2017071 to NCPDP SCRIPT Standard Version 2023011.	200	600	There are no changes in these transactions between standard versions. We expect low effort to update how certified technology enable these transactions for the new standard version. For the 2014 Certification Edition, ONC finalized requirements to adopt NCPDP Script Standard Version 10.6 for NewRx (the only required transaction for the 2014 Edition criterion.) It was estimated, according to the final rule's impact analysis, that 50-150 labor hours were required to implement the change. We reduce the level of effort by half, given no changes were made to the transactions between standard versions and multiply these labor hours by the number of required transactions (8) this task applies to.

Task 2: (i) Require Electronic Prior Authorization transactions and (ii) adopt and require new PANotification transaction	Electronic Prior Authorization transactions were optional under Cures Update regulations. We propose to require them. We also propose to adopt and require transaction, PANotification.	250	3600	For the 2015 Certification Edition, new transactions were required for this criterion. It was estimated that it would require 250-400 labor hours to implement each new transaction. We take a similar approach here. Those who voluntarily adopted the transactions as part of a certified Health IT Module under prior rulemaking will face less development costs to adopt under new regulations.
Task 3: Require Signatura (Sig) transaction	Sig was an optional transaction under Cures Update regulations.	40	400	The transaction was optional in prior rulemaking. Those who voluntarily adopted the transactions as part of certified Health IT Module under prior rulemaking will face less development costs to adopt under new regulations.
Task 4: Require FDA National Drug Code (NDC) terminology for coded drugs.	NDC is required in NCPDP SCRIPT Standard Version 2023011 for coded drugs.	40	80	NDC is already widely adopted and seen as critical for coding drugs. NDC is now a required part of adopting 2023011 but high current adoption should reduce

				overall effort to implement in certified Health IT Modules.
Task 5: Update to RxNorm July 5, 2022, Full Monthly Release terminology	Aligns with current version of vocabulary standard	40	80	Vocabulary standard is likely to already be incorporated into fielded technology. Some effort expected to align with updated certification requirements.
Task 6. Support exchange of Race and Ethnicity data for four transactions	NCPDP standard supports exchange of these data as an optional feature for transactions.	40	80	Developers must map to patient's race and ethnicity data and support exchange of this data for four transactions.

Notes: ^1 New prescription (NewRx); Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse); Request and respond to cancel prescriptions (CancelRx, CancelRxResponse); Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse); Receive fill status notifications (RxFill); Relay acceptance of a transaction back to the sender (Status); Respond that there was a problem with the transaction (Error); Respond that a transaction requesting a return receipt has been received (Verify).

Table 16. Total Cost to Modify Electronic Prescribing [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (208 products)	$5,317,312	$15,951,936
Task 2 (208 products)	$6,646,640	$95,711,616
Task 3 (208 products)	$1,063,462	$10,634,624
Task 4 (208 products)	$1,063,462	$2,126,925
Task 5 (208 products)	$1,063,462	$2,126,925
Task 6 (208 products)	$1,063,462	$2,126,925
Total (208 products and 163 developers)	$16,217,802	$128,678,950

BILLING CODE 4150–45–C

The cost to a health IT developer to make the proposed modifications to the ''electronic prescribing'' certification criterion for its Health IT Module would range from $77,970 to $618,649 per product, on average. Therefore, assuming 208 products overall and a labor rate of $128 per hour, we estimate that the total cost to all health IT developers would, on average, range from $16.2 million to $128.7 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed updates to the ''electronic prescribing'' certification criterion in § 170.315(b)(3) align the certification criterion with an updated version of the NCPDP SCRIPT Standard. For *Task 1,* this alignment is in step with a reciprocal Medicare Part D requirement for Part D sponsors, prescribers, and dispensers, when electronically transmitting prescriptions and prescription-related information for covered Part D drugs for Part D eligible individuals, to use a standard in § 170.205(b), which includes the NCPDP SCRIPT standard version 2023011, for all required and optional electronic prescribing transactions. NCPDP SCRIPT standard version 2023011 includes important updates to terminology standards, transactions, and other data elements. Moreover, the adoption through rulemaking of a new NCPDP SCRIPT standard version and new proposed updates to the certification criterion for *Electronic Prescribing* align with public feedback and consensus on how to make these transactions and the ''electronic prescribing'' certification criterion more interoperable.

For *Task 2,* comments from ONC's ''Request for Information: Electronic Prior Authorization Standards, Implementation Specifications, and Certification Criteria,'' published on January 24, 2022, stated that making the Prior Authorization transactions required would help to advance interoperability and reduce administrative burden around prior authorization processes for medications. Requiring these transactions would help ensure pharmacy data systems are able to communicate similarly across all Health IT modules certified to this certification criterion and would not have to build different processes for prior authorization across different certified health IT.

For *Task 3,* communicating how a prescriber intends for a patient to take a medication is critical for safe and effective care. These instructions are essential for accurate prescription labeling, appropriate patient counseling and education from a pharmacist, and optimal medication use. The industry has been slow to adopt structured and codified Sig functionality, most frequently using the unstandardized format of unstructured free text Sigs. The wide variation in unstructured Sig limits the clarity, utility, and reusability of the data—curbing its potential impact on patient safety and clinical outcomes. Sig is also an important factor in a provider's capacity to follow the CDC Guideline for Prescribing Opioids for Chronic Pain, especially in cases where the provider lacks information about days' supply, but still seeks to calculate quality improvement opioid measures as part of a larger strategy to support careful and selective use of long-term opioid therapy in the context of managing chronic pain.[295] The Sig requirement provides greater clarity, utility, and reusability of the data, moving from an unstructured free text Sig to a structured and codified functionality.

For *Task 4,* the NDC is critical for specific product identification in research, dispensing and administrative workflows. The NDC is the key, unique, product identifier and is the standard of practice used throughout the pharmacy industry to identify the specific product. The pharmacy industry heavily relies on the NDC in all aspects of its business, including, but not limited to, drug ordering, medication dispensing, reporting, billing, rebates, adverse event reporting and patient safety. In NCPDP SCRIPT standard version 2023011, NDC is now required for coded drugs in the standard. NDC is also adopted as a medical data code set for reporting drugs and biologics on retail pharmacy claims under the HIPAA Transaction and Code Set rule.[296] Use of NDC will ensure greater interoperability with pharmacy data systems and facilitate correct identification of prescribed products.

For *Task 5,* updating Health IT Modules to the latest RxNorm standard version is very important for interoperability. Modules certified to this certification criterion, currently, align with a prior RxNorm standard version, so this new requirement transitions technology to the newest standard version, which will ensure Health IT modules certified to this certification criterion all use the same code sets and can communicate with pharmacy data systems more effectively.

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit prescribers, pharmacists, payers, and patients and improve the quality of health care provided. These proposed requirements align with a reciprocal Medicare Part D requirement in ''Medicare Program; Contract Year 2025 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicare Parts A, B, C, and D Overpayment Provisions of the Affordable Care Act and Programs of All-Inclusive Care for the Elderly; Health Information Technology Standards and Implementation Specifications'' proposed rule for Part D sponsors, prescribers, and dispensers, when electronically transmitting prescriptions and prescription-related information for covered Part D drugs for Part D eligible individuals, to use a standard in § 170.205(b), which includes the NCPDP SCRIPT standard version. Prescribers, pharmacists, and payers will benefit from the updates to the standards and to the certified criterion through increased standardization and interoperability of electronic prescribing.

9. New Real-Time Prescription Benefit Certification Criterion

We propose to establish a real-time prescription benefit (RTPB) certification criterion in § 170.315(b)(4) based on National Council for Prescription Drug Programs (NCPDP) RTPB standard version 13 and include this certification criterion in the Base EHR definition in § 170.102. We believe including the RTPB certification criterion will markedly increase the use of RTPB tools and promote widespread adoption, which will help to lower drug costs for Medicare beneficiaries. Use of RTBTs enables Medicare providers and enrollees to make cost-informed decisions about prescriptions, and a standardized approach will ensure that critical drug and drug price data is available to providers when they need it.

The proposed certification criterion includes the following standards and functional requirements:

- Incorporate the NCPDP Real-Time Prescription Benefit (RTPB) standard version 13 and vocabulary standards, RxNorm (§ 170.207(d)(1)) and National Drug Codes (§ 170.207(d)(2)), to enable a user to send and receive patient-specific benefit, estimated cost information, and

[295] *https://www.cdc.gov/drugoverdose/pdf/Guidelines_At-A-Glance-508.pdf.*

[296] 45 CFR 162.1002(a)(3).

therapeutic alternatives within workflow at the point of care, specifically standard transactions:

- Mandatory and situational transaction segments and associated data elements for RTPBRequests and RTPBResponse transactions;
- RTPBError transaction;
- Exclusive use of XML format for all transactions; and
- Require use for medications and vaccines covered by a pharmacy benefit.

NCPDP RTPB standard version 13 permits the use of the EDI or XML format for payloads. ONC proposes that a Health IT module certified to the certification criterion must enable a user to perform the specified NCPDP RTPB standard version 13 transactions using the XML format. ONC, similarly, requires that a Health IT Module certified to the ''electronic prescribing'' certification criterion, which uses the NCPDP SCRIPT standard, use the XML format for payloads. Public comments on ONC's RTPB RFI in the HTI–1 NPRM broadly supported use of XML. We do not estimate additional costs to developers to exclusively use XML to implement this certification criterion, as it is broadly supported and required as part of another functionally similar ''electronic prescribing'' certification criterion. The proposed certification criterion also would only require use of NCPDP RTPB standard version 13 to send and receive patient-specific benefit, estimated cost information, and therapeutic alternatives for medication and vaccine products, and would not include required use for medical device products. We do not estimate additional costs to developers to implement the standard and certification criterion in this manner.

Background

ONC analysis of the 2022 American Hospital Association Health Information Technology Supplement indicates that half (50.2%) of hospitals have implemented EHR functionality that integrates health insurer real-time prescription benefit information for all or nearly all payers; another 15.9% have implemented such a functionality for a limited set of payers.[297] However, hospital implementation of RTPB tools does not necessarily translate to widespread prescriber adoption in or out of the hospital. The American Medical Association (AMA) reports that its 2020 member survey of physicians explained RTPB tools to responding physicians and found that only 35.7% had heard of the tool; among those who had heard of it, only 55% actually had access.[298] The AMA survey did find high uptake of RTPB tools among physicians with access, with that group over four times more likely to report use of the RTPB tool than not.[299] Limited adoption may be due to the proprietary and therefore fragmented nature of RTPB tools. The American Health Information Management Association argues that the largest barrier to implementing RTPB is ''not a lack of will, but rather a lack of ability due to technical barriers.'' [300]

Our market research found multiple tools available in the marketplace from health IT software vendors; health plans; and pharmacy benefit managers (PBMs).[301] [302] [303] [304] [305] There is choice in the market for these tools; however, without broadly adopted standards and standardized implementation, use of these tools can become fragmented and such fragmentation can impede interoperability. To realize the overall benefits of RTPB tools—increased patient choice; reduced medication costs and out-of-pocket patient expenses; reduced provider time and effort to identify and prescribe a covered medication; and ease of dispensing by PBMs—technology must be implemented that minimizes disruption to EHR usability, minimizes costs to physicians and hospitals, and ensures accuracy and consistency of pricing and coverage information.[306]

Development and incorporation of these tools into certified health IT is, however, not without cost. As described above, about 2 in 3 hospitals use any type of RTPB tool and, according to one study, less than 1 in 4 physicians uses the tool (far more lack knowledge of or access to one). This may be due to fragmented availability and implementation of tools across EHR vendors. We have no universal assessment of tool adoption and implementation across all EHRs. Information gathered through conversations with several EHR market leaders reveal variation in adoption and implementation. Some have deployed their own tools; some depend on third-party developers to provide these services; and others do not currently deploy a tool to their customers. There's also mixed adoption and perspectives on standard approaches to develop and deploy these tools, with some developers being supportive of tools using the NCPDP RTPB standard and others agnostic.

Furthermore, as finalized in the ''Medicare and Medicaid Programs; Contract Year 2022 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicaid Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly' final rule regulatory impact analysis (86 FR 5864), CMS policy to require entities to implement a RTBT would have costs on providers and payers. These costs are separate from the costs estimated here to adopt the proposed certification criterion but reflect estimated costs for end-users of the technology to implement in a real world setting.

Costs

Dependency on specific health IT vendor or health plan efforts alone to provide these tools may not lead to broader availability and adoption. The proposed certification criterion incorporates the NCPDP RTPB standard version 13, which was piloted successfully in at least one study, and adopts functional requirements that align with implementation of the standard to facilitate interoperability between prescribing systems, plans, and PBMs.[307] The standard was published in October 2021. Since that time, there have been new enhancements added to the standard at the request of end users, resulting in version 13.[308]

We estimate costs to certified health IT developers to incorporate the NCPDP Real-Time Prescription Benefit (RTPB) standard version 13 and vocabulary standards, RxNorm (§ 170.207(d)(1)) and National Drug Codes (§ 170.207(d)(2)) to send and receive mandatory and situational transaction segments and associated data elements for RTPBRequests and RTPBResponse

[297] *https://www.healthit.gov/data/quickstats/hospital-adoption-real-time-benefit-tools.*

[298] *https://councilreports.ama-assn.org/councilreports/downloadreport?uri=/councilreports/n21_cms_report_2.pdf.*

[299] Ibid.

[300] *https://www.ahima.org/media/rrije1di/ahima-onc-hti-1-comments-final.pdf.*

[301] *https://surescripts.com/who-we-serve/ehr-vendors.*

[302] *https://arrivehealth.com/wp-content/uploads/2022/11/Arrive-Health-Physician-Insights-Whats-Needed-to-Improve-Prescribing-Workflows.pdf.*

[303] *https://www.optum.com/content/dam/optum4/resources/pdf/wf2167397_pcs_improving_prescribing_process.pdf.*

[304] *https://www.humana.com/provider/pharmacy-resources/tools/real-time-benefit-tool#:~:text=Real%2DTime%20Benefit%20Check%20(RTBC,your%20electronic%20medical%20record%20representative.*

[305] *https://www.express-scripts.com/corporate/articles/scriptvision-gives-physicians-real-time-access-patient-specific-information.*

[306] Ibid.

[307] *https://ncpdpfoundation.org/pdf/NCPDPFoundationRTPBGrant_FinalReport.pdf.*

[308] *https://ncpdp.org/NCPDP/media/pdf/RTPB-Standard-Implementation-Recommendations-v1-1.pdf?ext=.pdf.*

transactions and the RTPBError transaction.

These tasks have their own levels of effort, and these estimates are detailed in Tables 17 and 18 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 17 shows the estimated labor costs per product to develop the certification criterion. 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 18.

2. We estimate that 208 products certified by 163 developers will be affected by our proposal. These estimates are a subset of the total number of estimated health IT developers and certified products we estimated above.

The estimate of 208 products certified by 163 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. We propose to require Health IT Modules certified to the electronic prescribing certification criterion to certify to the proposed RTPB certification criterion. We, therefore, use the estimated number of developers and products that certify to the ''electronic prescribing'' certification criterion as a proxy for the expected number of developers and products that will certify the proposed RTPB certification criterion. As of the end of 2022, 42% of developers and 40% of products certified to the ''electronic prescribing'' certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

Table 17. Estimated Labor Hours to Develop Real-Time Prescription Benefit Certification Criterion in § 170.315(b)(4)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adopt NCPDP Real-Time Prescription Benefit (RTPB) standard version 13 and all associated transactions.	Transactions include RTPBRequests, RTPBResponse, and RTPBError. Requests include 6 transaction segments and Response includes 5 segments.	500	1000	For the 2015 Certification Edition, new transactions were added to the "electronic prescribing" criterion. It was estimated that it would require 250-400 labor hours to implement each new transaction. We take a similar approach here.
Task 1: Adopt RxNorm vocabulary standard for relevant transaction segments and associated data elements		40	80	RxNorm is widely adopted and is a required vocabulary standard for "electronic prescribing". Mapping using these codes should create little extra effort to implement in certified Health IT Modules.
Task 1: Adopt National Drug Codes vocabulary standard for transaction segments and associated data elements		40	80	NDC is widely adopted and seen as critical for coding drugs. NDC is now a required part of adopting the NCPDP SCRIPT standard as well as the RTPB standard. Mapping using these codes should create little extra effort to implement in certified Health IT Modules.

Table 18. Total Cost to Develop Real-Time Prescription Benefit Certification Criterion [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (208 products)	$15,420,205	$30,840,410
Total (208 products and 163 developers)	$15,420,205	$30,840,410

BILLING CODE 4150–45–C

The cost to a health IT developer to develop the Real-Time Prescription Benefit (RTPB) certification criterion for their Health IT Modules would range from $74,136 to $148,271 per product, on average. Therefore, assuming 208 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $15.4 million to $30.8 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

CMS finalized in the 'Medicare and Medicaid Programs; Contract Year 2022 Policy and Technical Changes to the Medicare Advantage Program, Medicare Prescription Drug Benefit Program, Medicaid Program, Medicare Cost Plan Program, and Programs of All-Inclusive Care for the Elderly' final rule (86 FR 5864) that Part D sponsors implement a real-time benefit tool by January 1, 2023.[309] According to one source, as of the end of 2022, 98% of U.S. prescribers were served by EHRs with access to an available RTBT tool, and over half of prescribers used real-time prescription benefit to access medication pricing. So, although nearly all prescribers have an EHR with an available tool, more than half use it.[310] The proposed certification criterion would incorporate published, adopted standards and functional requirements that promote interoperability and patient choice. Furthermore, the revised certification criterion would provide a standardized implementation for health IT developers to support end-users to meet Medicare Part D requirements finalized in 86 FR 5864 for prescribers to implement a RTPB tool. This certification criterion would enable interoperability between certified health IT, plans, and PBMs, helping deliver on the promising benefits of the real-time ability of providers and their patients to make informed choices about medications and costs.

There are benefits for providers, patients, PBMs, and technology developers, and benefits from implementation of a RTPB tool are likely to manifest via multiple pathways. Standardization can lead to implementation and uptake of RTPB tools, and tool implementation can reduce time and effort and improve the accuracy of information, lead to reduced prescription costs for patients and payers, improve medication adherence, and generate other downstream benefits.

The real-time prescription benefit (RTPB) standard was developed by a multi-stakeholder, consensus-building process led by the National Council for Prescription Drug Programs (NCPDP). A standard format for data exchange is important for all exchange partners to share real-time information about a patient's drug benefit coverage and out-of-pocket cost prior to prescribing and dispensing.[311] By standardizing the data elements and process of exchanging data between an EHR, an intermediary, and a PBM, ''there is significant potential to directly impact the price transparency landscape and reduce out-of-pocket costs for patients.'' [312]

Studies have shown that patients who pay less for their medications overall have higher rates of medication adherence. A review of interventions to improve medication adherence found that reducing out-of-pocket costs to patients can be an effective mechanism.[313] Consistent with this, ONC-affiliated researchers conducted a survey of respondents 65 and older, finding that 20.2% reported cost-related medication non-adherence—most often delaying prescription fills, not filling prescriptions, or skipping doses.[314] The majority of respondents (79.3%) expressed a desire to speak to their physician about the cost of all or some of their medications, with respondents who reported cost-related non-adherence more likely.[315] Reducing prescription copays and formulary decision support have previously been shown to improve medication adherence,[316] [317] suggesting that RTPB tools may also be a useful mechanism. One retrospective study appears to support this, finding that prescriptions placed using RTPB were associated with a higher fill rate (79.8% vs. 71.7%) and lower cancellation rate (9.3% vs. 14.9%).[318] The same researchers found that prescribers using RTPB adjusted days of supply for 44% of medication orders and quantity for 69% of orders, which can support adherence.[319] A cluster-randomized trial of RTPB implementation resulted in 11.2% out-of-pocket savings for patients after controlling for patient and prescriber characteristics; savings were even higher (38.9%) for drugs with the highest out-of-pocket costs.[320] This study, however, did not find a change in the proportion of orders for 90-day supply despite identifying overall cost savings.[321]

An ONC-affiliated research review notes that 86% of providers believe that cost should influence treatment decisions, but barriers to cost conversations include physicians' knowledge of patients' cost burdens and lack of information about insurance coverage and prices.[322] Work by ONC-

[309] *https://www.federalregister.gov/documents/2021/01/19/2021-00538/medicare-and-medicaid-programs-contract-year-2022-policy-and-technical-changes-to-the-medicare.*

[310] *https://surescripts.widen.net/s/mvtqvvf5sd/2022-national-progress-report#page=1.*

[311] *https://ncpdpfoundation.org/pdf/NCPDPFoundationRTPBGrant_FinalReport.pdf.*

[312] Ibid.

[313] *https://www.acpjournals.org/doi/10.7326/0003-4819-157-11-201212040-00538.*

[314] *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2805012.*

[315] Ibid.

[316] *https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/409766.*

[317] *https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/773454.*

[318] *https://www.sciencedirect.com/science/article/abs/pii/S0002934322005289?via%3Dihub* via *https://link.springer.com/article/10.1007/s11606-022-07945-z.*

[319] *https://www.ajmc.com/view/implementation-and-cost-validation-of-a-real-time-benefit-tool.*

[320] *https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2796059.*

[321] Ibid.

[322] *https://journals.sagepub.com/doi/10.1177/10775587221108042?url_ver=Z39.88-*

affiliated researchers has highlighted the desire of patients to have conversations about costs with their prescribers.[323] [324] 89.5% of respondents indicated a desire for physicians to use real-time benefit tools and 89.8% indicated a desire to discuss the estimated prices, with greater interest among those with any cost-related nonadherence.[325] While other tools such as formulary guides exist that can help facilitate cost conversations and lead to savings, that information is not real-time and may not be up to date,[326] and patients may lose confidence in estimates or their providers if the provided information proves to be wrong.[327]

Provider use of tools may provide more informed choices to their patients, and also increase prescribers' efficiencies prescribing and approving products. In a survey of providers commissioned by an RTPB tool, a majority of respondents stated they need to change or manage a prescription order more than 25% of the time after it has been sent to the pharmacy.[328] When one research hospital's health system implemented their RTPB tool, researchers were able to guide prescribers to choose alternatives without prior authorization requirements, convert from drugs covered with restrictions, and/or to convert from drugs not covered to one covered with restrictions.[329] An additional study estimates that avoiding prior authorization is another way in which providers using its RTPB tool save time, estimating approximately 50 minutes of time saved for alternative prescriptions that avoid necessitating a prior authorization.[330]

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit prescribers and patients and improve the quality of health care provided. Data show that RTPB tools are available to nearly all US prescribers through prescribers' EHRs, though only half use the tool itself.[331] The proposed RTPB certification criterion would standardize tools across all EHRs certified to the criterion and establish a baseline of functionality. This may increase use, but the data show the certification criterion may have a negligible effect on the availability of the tools currently. We request comment on quantifiable benefits for this certification criterion.

10. Electronic Health Information (EHI) Export—Single Patient EHI Export Exemption

We propose an exemption policy for certain developers of Health IT Modules certified to the EHI export certification criterion to not support functionality for single patient data export. We believe this voluntary exemption does not create new costs for developers. We are also limited in our understanding of the number of developers to which the exemption policy could apply so cannot estimate any cost savings to developers for this policy. We request comment on any burden associated with this proposed exemption policy and information about the applicability of this proposed policy on developers of certified health IT.

11. Revised End-User Device Encryption Certification Criterion

We propose to revise § 170.315(d)(7) to include a new requirement that Health IT Modules certified to this certification criterion encrypt electronic health information (EHI) stored server-side. To include this new requirement, we propose organizing certification criterion paragraphs in a way that places existing end-user device encryption requirements into § 170.315(d)(7)(i) and adds the new server encryption requirement in § 170.315(d)(7)(ii). Then we propose placing the encryption standard and default settings requirements, that we propose should apply to both the end-user device and server encryption requirements, into § 170.315(d)(7)(iii) and (iv) respectively. Finally, we propose to change § 170.315(d)(7) by renaming it to ''Health IT encryption,'' to better describe the end-user and proposed server-side requirements together.

Costs

This section describes the estimated costs of meeting requirements in the proposed revisions to § 170.315(d)(7), which are detailed in Tables 19 and 20 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 19 shows the estimated labor costs per product to make the proposed updates in § 170.315(d)(7). 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 20.

2. We estimate that 448 products certified by 333 developers will be affected by our proposal. These estimates are a subset of the total estimated number of health IT developers and certified products we estimated above. The estimate of 448 products certified by 333 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(d)(7) and need to meet the proposed requirements. As of the end of 2022, 86% of developers and 86% of products certified § 170.315(d)(7). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[332] 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 $127.82.

2003&rfr_id=ori:rid:crossref.org&rfr_dat=cr_pub%20%200pubmed.

[323] *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2805012.*

[324] *https://agsjournals.onlinelibrary.wiley.com/doi/10.1111/jgs.18226.*

[325] Ibid.

[326] *https://councilreports.ama-assn.org/councilreports/downloadreport?uri=/councilreports/n21_cms_report_2.pdf.*

[327] *https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2805012.*

[328] *https://arrivehealth.com/wp-content/uploads/2022/11/Arrive-Health-Physician-Insights-Whats-Needed-to-Improve-Prescribing-Workflows.pdf.*

[329] *https://ncpdpfoundation.org/pdf/NCPDPFoundationRTPBGrant_FinalReport.pdf.*

[330] *https://www.optum.com/content/dam/optum4/resources/pdf/wf2167397_pcs_improving_prescribing_process.pdf.*

[331] *https://surescripts.widen.net/s/mvtqvvf5sd/2022-national-progress-report#page=1.*

[332] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 19. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(d)(7)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: new requirement in § 170.315(d)(7) for server encryption of EHI that uses the same encryption standard and default setting requirements finalized in § 170.315(d)(7) for end-user device encryption		125	375	In the 2014 Edition Final Rule, adopting the revised § 170.314(d)(7) was estimated to require 100 to 300 labor hours per product. We take a similar approach here while increasing the cost estimate by 25%.

Table 20. Total Cost to for Products and Developers to Meet the Proposed Requirements in § 170.315(d)(7) [2022 dollars]

Activity	Estimated Number of Products	Estimated Cost	
		Lower bound	Upper bound
Task 1: new requirement in § 170.315(d)(7) for server encryption of EHI that uses the same encryption standard and default setting requirements finalized in § 170.315(d)(7) for end-user device encryption	448	$7,157,920	$21,473,760
Total cost for all products (448 products)	**448**	**$7,157,920**	**$21,473,760**

Notes: We used an 86% modifier for the § 170.315(d)(7) certification criterion to estimate the number of products impacted by the Standards for encryption and decryption of electronic health information updates. Estimates reflect the percent of all products that certify to the § 170.210(a) certification criterion through 2022. This estimate is subject to change.

The cost to health IT developers to meet the proposed requirements in § 170.315(d)(7) would range from $15,978 to $47,933 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 448 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $7.2 to $21.5 million. Assuming 333 health IT developers, this would be an average cost per developer ranging from $183,536 to $550,609.

Benefits

Encryption is a ubiquitous feature in modern day technology, and it is widely accepted as a best practice for data protection whenever possible. Since the 2014 Edition Final Rule, encryption technology has continued to advance significantly, and we believe expanding requirements to server-side encryption is critical and beneficial to patients, providers, and developers. Encryption of server-side data prevents unauthorized data access in many

scenarios, including those involving a server breach, theft, or improper disposal. Mitigating these risks using encryption is a best practice for all server developers and, given the unique characteristics of EHI, is especially important for health IT server developers.

EHI is considered one of the most valuable types of personal information for theft because of the breadth of information included in electronic health records and the long shelf life of this information. However, despite its high value, EHI often is not being properly protected, and the problem is getting worse according to data published on the Department of Health and Human Services Office for Civil Rights (OCR) website. Between 2010 and 2022, OCR received 5,144 reports of breaches affecting 500 or more individuals, equating to 394,236,737 individuals.[333] The frequency of breaches affecting 500 individuals or more has increased significantly over the past few years, with almost two such large breaches reported per day in 2022, nearly double the frequency in 2018.[334] These statistics indicate that vulnerabilities and risks exist in EHI technology systems in the United States. While no single solution can fully protect EHI, data breach risks can be mitigated by encryption of data server-side data.

Along with the rising frequency of large data breaches, there is significant and increasing cost associated with health care data breaches. In 2023, the average cost of a health care data breach was $10.93 million, which represents a 53.3% increase from 2020.[335] 57% of organizations pass the costs of these breaches onto consumers.[336] While the benefits of these modifications are not quantifiable at this time, we expect the resulting improvements to help increase health care data security to significantly benefit patients, providers, and developers. Our proposed changes would also prevent many unauthorized data access and protect EHI.

12. Revised Certification Criterion for Encrypt Authentication Credentials

ONC proposes to revise the ''encrypt authentication credentials'' certification criterion in § 170.315(d)(12). Our proposed update revises the certification criterion by replacing our current ''yes'' or ''no'' attestation requirement and instead requiring Health IT Modules that store authentication credentials to protect the confidentiality and integrity of its stored authentication credentials according to October 12, 2021, version of Annex A of the Federal Information Processing Standards (FIPS) 140–2 industry standard or via hashing in accordance with the standard specified in § 170.210(c)(2). We would also change the name of this certification criterion to ''Protect stored authentication credentials,'' to better describe how we are revising the certification criterion.

Costs

The currently adopted ''encrypt authentication credentials'' certification criterion instructs developers to attest ''yes'' or ''no'' that they support encrypting stored authentication credentials. An analysis of the Certified Health IT Product List (CHPL), as of the end of 2022, shows that 66% of developers attested ''yes'' that they support encrypting stored authentication credentials. The proposed revision requires developers that store authentication credentials to protect the confidentiality and integrity of its stored authentication credentials according to the Federal Information Processing Standards (FIPS) 140–2 instead an attestation of its use.

The estimated costs will vary depending on current developer attestations to the ''encrypt authentication credentials'' certification criterion. We assume an overall lower level of burden for developers who attested ''yes'' to support encrypting stored authentication to comply with this revised certification criterion. We separate out the costs for these developers from those that attested ''no'' to support encrypting stored authentication. This section describes the estimated costs of meeting requirements in the proposed revisions to § 170.315(d)(12), which are detailed in Tables 21 to 23 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Tables 21 and 22 shows the estimated labor costs per product to make the proposed updates in § 170.315(d)(12). 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 23.

2. We estimate that 500 products certified by 372 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. The estimate of 500 products certified by 372 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(d)(12) and need to meet the proposed requirements. As of the end of 2022, 96% of developers and 96% of products certified § 170.315(d)(12). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[337] 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 $127.82.

BILLING CODE 4150–45–P

[333] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* These numbers are based on breach reports made to OCR as of May 17, 2024.

[334] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* These numbers are based on breach reports made to OCR as of May 17, 2024.

[335] *https://www.hipaajournal.com/2023-cost-healthcare-data-breach/#:~:text=For%20the%2013th%20year%20in,average%20breach%20cost%20in%202022.*

[336] *https://www.hipaajournal.com/2023-cost-healthcare-data-breach/#:~:text=For%20the%2013th%20year%20in,average%20breach%20cost%20in%202022.*

[337] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 21. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(d)(12) [Developers who currently attest "yes" that they support encrypting stored authentication credentials (66%)]

Task	Lower bound hours	Upper bound hours	Remarks
Task 1: Requiring Health IT Modules that store authentication credentials to protect the confidentiality and integrity of its stored authentication credentials according to the FIPS 140-2 industry standard or via hashing in accordance with the standard specified in § 170.210(c)(2)	0	0	Developers who currently attest "yes" are assumed to meet these basic encrypting stored authentication credentials capabilities.

Table 22. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(d)(12) [Developers who currently attest "no" that they support encrypting stored authentication credentials (34%)]

Task	Lower bound hours	Upper bound hours	Remarks
Task 1: Requiring Health IT Modules that store authentication credentials to protect the confidentiality and integrity of its stored authentication credentials according to the FIPS 140-2 industry standard or via hashing in accordance with the standard specified in § 170.210(c)(2)	0	250	Developers who currently attest "no" may or may not support encrypting stored authentication credentials capabilities in their products. It can be assumed that some may support but choose to attest "no". For others, it is expected to require a low level of effort to meet basic encrypting stored authentication credentials capabilities.

Table 23. Total Cost to for Products and Developers to Meet the Proposed Requirements in § 170.315(d)(12) [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Developers who currently attest "yes"		
Task 1 (330 products)	$0	$0
Developers who currently attest "no"		
Task 1 (170 products)	$0	$5,432,350
Total cost for all products (500 products and 372 developers)	**$0**	**$5,432,350**

Notes: We used a 96% modifier for the § 170.315(d)(12) certification criterion to estimate the number of products impacted by the Standards for encryption and decryption of electronic health information updates. Estimates reflect the percent of all products that certify to the § 170.315(d)(12) certification criterion through 2022. This estimate is subject to change.

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(d)(12) would range from $0 to $31,955 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Therefore, assuming 500 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $0 to $5 million.

Benefits

We believe this updated requirement and updated standard is necessary and important to help best protect health information. The frequency of breaches affecting 500 individuals or more has increased significantly over the past few years, with almost two large breaches reported per day in 2022, nearly double the frequency in 2018.[338] Along with the rising frequency of breaches affecting 500 or more individuals, there is significant and increasing cost associated with health care data breaches. In 2023, the average cost of a health care data breach was $10.93 million, which represents a 53.3% increase from 2020 and 57% of organizations pass the costs of these breaches onto consumers.[339] These statistics indicate that vulnerabilities and risks exist in EHI technology systems in the United States. Properly protecting stored authentication credentials in Health IT Modules is a critical defensive step to help ensure that breached authentication credentials are useless to an attacker.

We believe this proposal would benefit patients, health care providers, and developers. Adopting the, October 12, 2021, version of Annex A of the FIPS Publication 140–2 in § 170.210(a)(3) will help ensure patients' data are protected and cybersecurity risks are mitigated.[340] The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit patients, health care providers, and developers and help prevent exposure to unauthorized persons/entities. Patients, health care providers, and developers will benefit from the updates to the standard and to the certified criterion through revised criterion for encrypt authentication credentials.

13. Health IT Modules Supporting Public Health Data Exchange

a. Proposed Revised Certification Criteria for Health IT Modules Supporting Public Health Data Exchange in § 170.315(f)

§ 170.315(f)(1) Immunization Registries—Bidirectional Exchange

We propose to revise the current certification criterion located in § 170.315(f)(1) ''Transmission to immunization registries'' to reference the most current HL7® Version 2.5.1 Implementation Guide for Immunization Messaging, Release 2.0 to enable systems to respond to incoming, patient-level queries from external systems. Specifically, we propose to update the standard in § 170.205(e)(4) to the HL7 v2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, Published October 2018, which is a compilation of the Release 1.5 version and the Addendum from 2015 referenced in the current Program, and incorporate it by reference in § 170.299. Additionally, we are proposing to update the vocabulary standards in § 170.207(e)(3) and § 170.207(e)(4) referenced in § 170.315(f)(1)(i) to their newest versions.

Additionally, we propose to add a functional requirement in § 170.315(f)(1)(C) to enable certified health IT to respond to incoming patient-level, immunization-specific queries from external systems. We propose a requirement in support of requests for multiple patients' data as a group using an Application Programming Interface in § 170.315(g)(20)(ii). Lastly, we propose

[338] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.* These numbers are based on breach reports made to OCR as of August 25, 2023.

[339] *https://www.hipaajournal.com/2023-cost-healthcare-data-breach/#:~:text=For%20the%2013th%20year%20in,average%20breach%20cost%20in%202022.*

[340] *https://davidhoglund.typepad.com/files/white-paper---fips-in-medical-environments-0919.pdf.*

to revise the name of the certification criterion in § 170.315(f)(1) to ''Immunization registries—Bidirectional exchange'' to more accurately represent the capabilities included in the certification criterion.

Costs

This section describes the estimated costs of meeting the requirements in the proposed updates to § 170.315(f)(1). These tasks have their own level of effort, and these estimates are detailed in Table 31 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 24 shows the estimated labor costs per product to meet the proposed requirements in § 170.315(f)(1). We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will, on average, incur the costs noted in the tables below.

2. We estimate that 177 products certified by 147 developers will be affected by our proposal. These estimates are a subset of the total estimated number of health IT developers and certified products we estimated above. The estimate of 177 products certified by 147 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify to § 170.315(f)(1) certification criterion and need to meet the proposed requirements. As of the end of 2022, 38% of developers and 34% of products certified to § 170.315(f)(1) certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[341] 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 $127.82.

BILLING CODE 4150–45–P

[341] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 24. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(1) Immunization registries – Bidirectional exchange

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Standards update and reference new IG	Health IT Module must enable a user to: (i) create immunization information for electronic transmission and (ii) support request, access, and display in accordance with updated standards in § 170.205(e), § 170.207(e)(3), and § 170.207(e)(4).	0	500	(1) Lower bound assumes health IT product has already implemented the IG. (2) Upper bound assumes health IT product has not yet begun to implement the IG.
Task 2: New functional requirement – *Response*	Health IT module must be able to receive and respond to an incoming patient-level immunization-specific query or request from external systems.	250	1,000	(1) Lower bound assumes health IT already has some technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement
Task 3: New requirement – *Bulk FHIR*	Health IT Module must be able to receive and respond to requests for multiple patients' data as a group using an API in § 170.315(g)(20)(ii).	500	1,000	(1) Lower bound assumes health IT already has some technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement

Table 25. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(1) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: Standards update and reference new IG	$0	$63,910
Task 2: New functional requirement - *Response*	$31,955	$127,820
Task 3: New requirement - *Bulk FHIR*	$63,910	$127,820
Total cost per product	**$95,865**	**$319,550**
Task 1: Standards update and reference new IG	$0	$11,312,070
Task 2: New functional requirement - *Response*	$5,656,035	$22,624,140
Task 3: New requirement - *Bulk FHIR*	$11,312,070	$22,624,140
Total cost for all products (177 products)	**$16,968,105**	**$56,560,350**
Total cost per developer (147 developers)	**$115,429**	**$461,717**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (177 products). Total cost per developer = Total cost for all products / Number of developers (147 developers).

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(1) would range from $95,865 to $319,550 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 177 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $17 to $56.6 million. Assuming 147 health IT developers, this would be an average cost per developer ranging from $115,429 to $384,764.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve by helping remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies. Further, enabling greater flow of health information from EHRs to public health authorities using HL7® FHIR®-based standards could allow public health to reduce burden and streamline data sharing while protecting patient privacy.[342]

The proposed revisions to § 170.315(f)(1), along with the proposed new § 170.315(f)(21) certification criterion that can be adopted by Health IT Modules supporting public health uses cases, would help advance complete, longitudinal immunization histories for individuals. Such comprehensive information would help close gaps that exist today as patients receive care from a variety of settings. This would support EHRs, IISs, and intermediaries in operating from the same foundational functionalities, and keep data moving with the speed of care. If an individual receives a vaccine from a pharmacy, from a community health fair, away from their home State, or at their provider's office, any approved user, regardless of their health IT system, should be able to have access to their complete, accurate vaccine history. According to the American Immunization Registry Association (AIRA), ''the most important value of the IIS comes from providers' ability to query the IIS at the point of care and to locate and use the information about additional immunizations administered elsewhere.'' [343]

The proposed revisions to the certification criterion in § 170.315(f)(1) would help improve interoperability for immunization reporting across the major health IT systems involved and establish a shared technical foundation for health IT systems, with common capabilities related to exchange, receipt, query, and access. The reference and requirement of updated HL7 standards would help systems have more complete data, including demographic data like race and ethnicity, and that they have the functionality to send that data to other certified systems. HL7® message transmission from health care systems to IIS has been shown to improve timeliness and completeness of immunization data over manual entry.[344]

While the benefits of these updates are not quantifiable at this time, we expect the proposed updates to significantly benefit end users of health IT and the patient populations they serve. Specifically, the standards update, and new requirements will enable greater flow of health information from EHRs to public health authorities which would result in increased public health data interoperability between health care and public health and enable better healthcare and public health decision making.

§ 170.315(f)(2) Syndromic Surveillance—Transmission to Public Health Agencies

We propose to revise the current certification criterion located in § 170.315(f)(2) ''Transmission to public health agencies—syndromic surveillance''. We propose to revise the standard in § 170.205(d) (1), which is referenced in § 170.315(f)(2), to reference the most recent IG, HL7 Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1—US Realm Standard for Trial Use, July 2019, and incorporate it by reference in § 170.299. We further propose to minimally change the name of the

[342] *https://www.cdc.gov/surveillance/pdfs/20_319521-D_DataMod-Initiative_901420.pdf.*

[343] AIRA Adult IIS Literature Review (*immregistries.org*), p.23.

[344] Ibid, p.15.

certification criterion in § 170.315(f)(2) to ''Syndromic surveillance—Transmission to public health agencies.''

Costs

This section describes the estimated costs of meeting requirements in the proposed update to § 170.315(f)(2), which are detailed in Table 33 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 26 shows the estimated labor costs per product to make the proposed updates in § 170.315(f)(2). 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 the tables below.

2. We estimate that 141 products certified by 112 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. The estimate of 141 products certified by 112 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(f)(2) and need to meet the proposed requirements. As of the end of 2022, 29% of developers and 27% of products certified § 170.315(f)(2). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[345] 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 $127.82.

Table 26. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(2) Syndromic surveillance – Transmission to public health agencies

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Standards update and reference new IG	Updated standards in § 170.205(d)(2) and § 170.205(d)(4) to reference the HL7 Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1.	0	500	(1) Lower bound assumes health IT product has already voluntarily implemented the HL7 v2.5.1 IG. (2) Upper bound assumes health IT has not yet begun to implement the HL7 v2.5.1 IG.

Table 27. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(2) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: Standards update and reference new IG	$0	$63,910
Total cost per product	**$0**	**$63,910**
Task 1: Standards update and reference new IG	$0	$9,011,310
Total cost for all products (141 products)	**$0**	**$9,011,310**
Total cost per developer (112 developers)	**$0**	**$80,458**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (141 products). Total cost per developer = Total cost for all products / Number of developers (112 developers).

[345] *https://www.bls.gov/oes/current/oes151252.htm.*

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(2) would range from $0 to $63,910 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 141 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $0 to $9 million. Assuming 112 health IT developers, this would be an average cost per developer ranging from $0 to $80,458.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve by helping remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies.

Syndromic surveillance data, when received in a timely manner and in a standard format, helps public health agencies achieve several surveillance goals including identifying emerging conditions or the long-term effects of unplanned mass-events and monitoring infectious disease to predict spikes.[346] The proposed revisions to the certification criterion in § 170.315(f)(2) would provide additional information, such as patients' acuity and comorbidities, for public health agencies to inform assessment of emerging threats to public health and identify possible outbreaks of infectious disease. Additionally, the observation component within the implementation guide now contains additional required elements relevant to public health surveillance that were previously optional including, but not limited to, pregnancy status, travel history, and acuity which aid in public health assessment, particularly in identification of emerging public health threats and the proceeding action. These revisions to the certification criterion in § 170.315(f)(2) would help with more needed data elements being shared with syndromic surveillance programs through use of the current HL7 IG, and that all syndromic surveillance systems can accept and validate incoming data. The new HL7 IG represents ''a more refined and extensible product that can support syndromic surveillance activities across a wider and more diverse range of clinical venues, EHR implementations, and public health authorities.'' [347]

While the benefits of these updates are not quantifiable at this time, we expect the proposed updates to significantly benefit end users of health IT and the patient populations they serve. Specifically, the standards update would enable capture of critical data elements and facilitate public health data interoperability between health care and public health, which will enable better healthcare and public health decision making.

§ 170.315(f)(3) Reportable Laboratory Results—Transmission to Public Health Agencies—and Laboratory Orders—Receive and Validate

We propose to revise the current certification criteria located in § 170.315(f)(3) Transmission to public health agencies—reportable laboratory tests and values/results. The certification criterion currently only includes transmission of lab results and does not cover functions related to the laboratory order. We propose to update the certification criterion to also include functionality for certified health IT to receive, validate, parse, and filter laboratory orders, according to the standard in § 170.205(g)(2). We also propose to update the standard referred to in § 170.205(g)(3) for the transmission of laboratory results.

We propose to adopt the standard for HL7 Version 2.5.1 Implementation Guide: Laboratory Orders (LOI) from EHR, Release 1, STU Release 4—US Realm (LOI) in § 170.205(g)(2) and incorporate it by reference in § 170.299, and to also adopt in § 170.205(g)(3)—and incorporate by reference in § 170.299—the standard for HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface, Release 1 STU Release 4—US Realm (LRI), and to specify the use of the Public Health Profile, in addition to the ELR IG.

We propose to revise § 170.315(f)(3)(i) to reference LRI in addition to the HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm) (ELR). We propose to revise the standards in § 170.207(a), (c), and (m), which are referenced in § 170.315(f)(3)(i) and § 170.315(f)(3)(ii), to reference the latest versions of SNOMED CT®, LOINC®, and UCUM, respectively.

We further propose to add a functional requirement in § 170.315(f)(3)(iii) requiring the ability to receive, validate, parse, and filter reportable laboratory orders according to the standard proposed in § 170.205(g)(2). Additionally, we propose to rename the certification criterion in § 170.315(f)(3) to ''Reportable laboratory results—Transmission to public health agencies—and Laboratory Orders—Receive and validate.''

Costs

This section describes the estimated costs of meeting the requirements in the proposed updates to § 170.315(f)(3). These tasks have their own level of effort, and these estimates are detailed in Table 35 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 28 shows the estimated labor costs per product to meet the proposed requirements in § 170.315(f)(3). 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 the tables below.

2. We estimate that 47 products certified by 39 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. The estimate of 47 products certified by 39 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(f)(3) and need to meet the proposed requirements. As of the end of 2022, 10% of developers and 9% of products certified § 170.315(f)(3). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[348] 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 $127.82.

BILLING CODE 4150–45–P

[346] Overview | NSSP | CDC.

[347] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6606111/.*

[348] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 28. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(3) Reportable laboratory results – Transmission to public health agencies – and Laboratory Orders – Receive and validate

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New requirement that points to specific IG	Adopt the standard for HL7 Version 2.5.1 Implementation Guide: Laboratory Orders (LOI) from EHR, Release 1, STU Release 4 — US Realm (LOI) in § 170.205(g).	500	1,500	(1) Lower bound assumes health IT product has begun to implement HL7 Version 2.5.1 IG. (2) Upper bound assumes health IT product does not support HL7 Version 2.5.1 IG.
Task 2: Standards update and reference new IG	Adopt the standard for HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface, Release 1 STU Release 4 — US Realm (LRI), specifically the Public Health Profile (pgs. 34-38) within the IG, in § 170.205(g)	1,000	1,500	(1) Lower bound assumes health IT product has begun to implement HL7 Version 2.5.1 IG. (2) Upper bound assumes health IT product does not support HL7 Version 2.5.1 IG.
Task 3: Code set update	Revise the standards in § 170.207(a), (c), and (m) which are referenced in § 170.315(f)(3)(i) and § 170.315(f)(3)(ii), to reference the latest versions of SNOMED CT®, LOINC®, and UCUM	0	1,000	(1) Lower bound assumes health IT product has already begun to update standards. (2) Upper bound assumes health IT product has not yet begun to update standards.
Task 4: New functional requirement – *Receive, validate, parse and filter*	Health IT Module must be able to receive, validate, parse and filter reportable laboratory orders according to the standard specified in § 170.205(g)(2).	500	2,500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement. (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement.

Table 29. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(3) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New requirement that points to specific IG	$63,910	$191,730
Task 2: Standards update and reference new IG	$127,820	$191,730
Task 3: Code set update	$0	$127,820
Task 4: New functional requirement	$63,910	$319,550
Total cost per product	**$255,640**	**$830,830**
Task 1: New requirement that points to specific IG	$3,003,770	$9,011,310
Task 2: Standards update and reference new IG	$6,007,540	$9,011,310
Task 3: Code set update	$0	$6,007,540
Task 4: New functional requirement	$3,003,770	$15,018,850
Total cost for all products (47 products)	**$12,015,080**	**$39,049,010**
Total cost per developer (39 developers)	**$308,079**	**$1,001,257**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (47 products). Total cost per developer = Total cost for all products / Number of developers (39 developers).

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(3) would range from $255,640 to $830,830 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 47 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $12 to $39 million. Assuming 39 health IT developers, this would be an average cost per developer ranging from $308,079 to $1,001,257.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, laboratories, public health practitioners) and the patient populations they serve by helping remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed decision making and faster, more coordinated responses to public health threats and emergencies. Laboratory standards are critical not only for health care and public health to be able to exchange and have a common understanding of results with identical meanings that are often represented in different formats, but also for patients who can view test results in their online portals.[349]

The proposed changes to the certification criterion in § 170.315(f)(3) would help increase the data shared between health care providers, laboratories, and public health agencies, and would increase interoperability among the different systems in place at each entity. To encompass all aspects of the laboratory workflow, the proposed requirements in § 170.315(f)(3) to create and transmit laboratory orders according to the LOI IG and receive laboratory results according to the LRI IG align with the proposed updates to § 170.315(a)(2), *Computerized provider order entry—laboratory* and the new proposed requirements in § 170.315(f)(23) for public health agencies to be able to receive electronically transmitted laboratory values/results in their system(s) according to the LRI IG. Together, these proposals will help ensure that laboratory results and orders are sent and received according to the same standards and that all systems involved in the workflow have the same baseline functionality. By requiring systems to receive results and values back electronically (according to national standards), more complete patient information will be available to clinicians throughout the laboratory workflow and for public health action.

With the addition of lab orders to values/results in § 170.315(f)(3), there would be another data source—often that is collected at the point of care from the patient—which would contribute to more complete and accurate demographic information important to understanding and addressing health disparities. Our proposed changes would also provide more complete patient-level information for contact tracing, patient outreach, direct care, and other clinical and public health activities. The use of the LRI IG would provide more specificity than ELR, which can decrease the need for one-off mapping. Additionally, the LRI and LOI IGs could have uses beyond public health reporting, which would reduce implementation and maintenance burden for reporters. Both the LOI and LRI standards have multiple use cases defined in the IGs, allowing for more flexibility, reusability, and scalability.

Standards adoption would aid in getting more complete information to public health agencies, as LOI makes important patient demographic information required, including race, ethnicity, sex, and contact information, as well as Ask at Order Entry questions (AOEs). In one study, COVID electronic laboratory reports were missing data on race more than one-third of the time and data on ethnicity were present less than one-fifth of the time.[350] Missing data in

[349] Development and Implementation of a Standard Format for Clinical Laboratory Test Results | American Journal of Clinical Pathology | Oxford Academic (*oup.com*).

[350] Electronic health information quality challenges and interventions to improve public health surveillance data and practice.—Abstract—Europe PMC

laboratory results transmitted to public health authorities also remains a problem. Having more complete demographic information, enabled by the increased specificity of the LOI and LRI standards, can help improve patient matching, which in turn would improve patient care and the efficiency of care.

While the benefits of many of these modifications are not quantifiable at this time, we expect the proposed changes to help increase the data shared between health care providers, laboratories, and public health agencies, and would increase interoperability among the different systems in place at each entity. Our proposed changes would also provide more complete patient-level information for contact tracing, patient outreach, direct care, and other clinical and public health activities.

§ 170.315(f)(4) Cancer Registry Reporting—Transmission to Public Health Agencies

We propose to modify the requirement for a certified Health IT Module to support creation and submission of cancer case information in § 170.315(f)(4) using at least one of the following standards:

- The cancer FHIR® reporting bundle and accompanying profiles according to the HL7® FHIR® Central Cancer Registry Reporting Content IG in § 170.205(i)(3), with requirement that all data elements indicated as ''mandatory'' and ''must support'' within the IG by the standards and implementation specifications must be supported, and/or
- The HL7 CDA® Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1—U.S. Realm. in § 170.205(i)(2).

We also propose the inclusion of an additional requirement within the cancer registry reporting certification criterion, to include cancer pathology reporting. We propose to adopt the standard HL7® FHIR® Cancer Pathology Data Sharing, 1.0.0—STU1 in § 170.205(i)(4) and incorporate it by reference in § 170.299. We also propose to revise § 170.315(f)(4) to add a requirement to create and transmit cancer pathology laboratory values and results in accordance with the proposed standard referenced in § 170.205(i)(4), Cancer Pathology Data Sharing, 1.0.0—STU1, including support for all ''mandatory'' and ''must support'' data elements within the IG. We also propose minimal changes to the name of this certification criterion to, ''Cancer registry reporting—Transmission to public health agencies.''

Costs

This section describes the estimated costs of meeting the requirements in the proposed updates to § 170.315(f)(4). These tasks have their own level of effort, and these estimates are detailed in Table 37 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 30 shows the estimated labor costs per product to meet the proposed requirements in § 170.315(f)(4). 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 the tables below.

2. We estimate that 42 products certified by 35 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. The estimate of 42 products certified by 35 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(f)(4) and need to meet the proposed requirements. As of the end of 2022, 9% of developers and 8% of products certified § 170.315(f)(4). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[351] 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 $127.82.

BILLING CODE 4150–45–P

[351] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 30. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(4) Cancer registry reporting – Transmission to public health agencies.

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Standards update and reference new IG	Health IT Module must support creation and submission of cancer case information according to (i) Cancer FHIR reporting bundle of HL7 FHIR Central Cancer Registry Reporting Content IG, or (ii) HL7 CDA Release 2 Implementation Guide: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1 – US Realm.	0	0	We assume no cost imposed by this task given that use of the CDA IG is already required in current § 170.315(f)(4). Therefore, this proposal introduces new optionality but does not impose a requirement to adopt the FHIR IG.
Task 2: New requirement that points to specific IG	Health IT Modules must be able to create and transmit cancer pathology laboratory values and results in accordance with the proposed standard referenced in § 170.205(i)(4), Cancer Pathology Data Sharing, 1.00 - STU1, including support for all "mandatory" and "must support" data elements	500	1,500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement. (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement.

Table 31. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(4) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: Standards update and reference new IG	$0	$0
Task 2: New functional requirement that points to specific IG	$63,910	$191,730
Total cost per product	**$63,910**	**$191,730**
Task 1: Standards update and reference new IG	$0	$0
Task 2: New functional requirement that points to specific IG	$2,684,220	$8,052,660
Total cost for all products (42 products)	**$2,684,220**	**$8,052,660**
Total cost per developer (39 developers)	**$76,692**	**$230,076**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (42 products). Total cost per developer = Total cost for all products / Number of developers (39 developers).

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(4) would range from $63,910 to $191,730 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 42 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $2.7 to $8 million. Assuming 35 health IT developers, this would be an average cost per developer ranging from $76,692 to $230,076.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, laboratory technicians, public health practitioners) and the patient populations they serve. Collectively, proposed revisions to existing (f) certification criteria help remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies. Further, enabling greater flow of health information from EHRs to public health authorities using HL7 FHIR-based standards could allow public health to streamline of data sharing while protecting patient privacy.[352]

Adopting FHIR standards for cancer registry reporting would help automate and accelerate reporting to central cancer registries and ensure that cancer data are collected in a complete and consistent manner that would facilitate exchange.[353] Manual and non-standardized data collection can lead to missing or low-quality, non-comparable data, making it difficult to share information needed to facilitate public health surveillance and research. Standards-based reporting to cancer registries supports faster and more accurate reporting, makes the data more useful for secondary purposes, and facilitates bi-directional communication when supplemental data are needed for research or treatment purposes.[354]

An important component of diagnosing cancer, and particularly in understanding how advanced cases are at the point of diagnosis, is cancer pathology reporting. The information included in cancer pathology reports are critical sources of data for cancer registries as the vast majority of cancer cases are diagnosed using methods that generate a pathology report.[355] The proposed updates to the certification criterion in § 170.315(f)(4) for cancer registry reporting would help ensure public health agencies receive standardized, electronic pathology reports, which would be an important addition to more complete and accurate understanding of cancer diagnoses and assessing the stage at diagnosis. The IG leverages structured data capture approaches developed by various stakeholders including the College of American Pathologists, NAACCR, and the IHE SDC on FHIR resources, which is important for promoting interoperability, sustainability, and for scaling standards adoption.[356] The inclusion of electronic transmission of cancer pathology reporting in the Program will result in more complete, accurate diagnostic information being sent, according to a shared standard, to State cancer registries. Such information can better inform cancer staging and aid in targeted programming where it is most needed.

While the benefits of many of these modifications are not quantifiable at this time, we expect the resulting improvements from standards adoption to promote interoperable exchange of more complete and accurate cancer data between health care providers and public health which will allow for better public health decision-making and evaluation of program interventions aimed at cancer prevention and early detection. Health IT users will benefit from the updates to the standard through increased efficiency of reporting (*e.g.,* automation enabled by standardization), which will reduce the time burden of mandatory reporting.

[352] *https://www.cdc.gov/surveillance/pdfs/20_319521-D_DataMod-Initiative_901420.pdf.*

[353] Next Generation of Central Cancer Registries | JCO Clinical Cancer Informatics (*ascopubs.org*).

[354] Ibid.

[355] Using informatics to improve cancer surveillance—PMC (*nih.gov*).

[356] Ibid.

Standardized capture of cancer data will also allow clinicians to more readily identify information needed to make decisions about their patients' care and treatment.[357] Thus, patients will benefit from more complete data being captured and used by clinicians to make decisions about their care. These data can also be used by public health agencies to improve population health by identifying high-risk groups, providing targeted screening, and investigating underlying causes of cancer.[358]

§ 170.315(f)(5) Transmission to Public Health Agencies—Electronic Case Reporting

We propose to revise the certification criterion in § 170.315(f)(5) to require adherence to the HL7 FHIR eCR IG only adopted in § 170.205(t)(1). We propose to maintain in § 170.205(t)(1) adherence to specific aspects of the HL7 FHIR eCR IG to allow for flexibility: the electronic initial case report (eICR) profiles and the RR profile of the HL7 FHIR eCR IG, and the ability to consume and process electronic case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set as specified in the HL7 FHIR eCR IG. We propose that Health IT Modules must enable a user to: create a case report for electronic transmission in accordance with the following:

(A) Consume and process electronic case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code (RCTC) value set as specified in the HL7 FHIR eCR IG in § 170.205(t)(1).

(B) Create a case report consistent with the eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1)

(C) Receive, consume, and process a case report response that is formatted to the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1).

(D) Transmit a case report electronically to a system capable of receiving an electronic case report.

Costs

This section describes the estimated costs of meeting the requirements in the proposed updates to § 170.315(f)(5). These tasks have their own level of effort, and these estimates are detailed in Table 39 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 32 shows the estimated labor costs per product to meet the proposed requirements in § 170.315(f)(5). 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 the tables below.

2. We estimate that a total of 196 products certified by 162 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(f)(5) and need to meet the proposed requirements. The estimate of 196 products certified by 162 developers is derived from the total number of products that were estimated to be affected by updates to the eCR certification criterion in the HTI–1 Final Rule (55 products that were currently certified by 48 developers in 2021 plus 141 new products expected to be certified by 114 developers for the first time).

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[359] 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 $127.82.

[357] Using informatics to improve cancer surveillance—PMC (*nih.gov*).

[358] Ibid.

[359] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 32. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(5) Electronic case reporting – Transmission to public health agencies

Activity	Details	Estimated Labor Hours		Remarks
		Lower bound	Upper bound	
Task 1: Case Report Creation	(1) Enable a user to create a case report for electronic transmission according to eICR profiles of HL7 FHIR eCR IG and (2) Support RCTC value set	0	1,500	(1) Lower bound assumes health IT product has already implemented the FHIR IG. (2) Upper bound assumes health IT product does not support the FHIR IG.
Task 2: Case Report Response Receipt	Health IT Module must be able to consume and process a reportability response according to RR profiles of HL7 FHIR eCR IG.	0	1,500	(1) Lower bound assumes health IT product has already implemented the FHIR IG. (2) Upper bound assumes health IT product does not support the FHIR IG.

Table 33. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(5) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: Standards update for case report creation	$0	$191,730
Task 2: Standards update for case report response receipt	$0	$191,730
Total cost per product	**$0**	**$383,460**
Task 1: Standards update for case report creation	$0	$37,579,080
Task 2: Standards update for case report response receipt	$0	$37,579,080
Total cost for all products (196 products)	**$0**	**$75,158,160**
Total cost per developer (162 developers)	**$0**	**$463,939**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (196 products). Total cost per developer = Total cost for all products / Number of developers (162 developers).

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(5) would range from $0 to $383,460 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 196 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $0 to $75 million. Assuming 162 health IT developers, this would be an average cost per developer ranging from $0 to $463,939.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve. Collectively, proposed revisions to existing (f) certification criteria help remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed

decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies. Further, enabling greater flow of health information from EHRs to public health authorities using HL7 FHIR-based standards could allow public health to take advantage of advanced data science capabilities such as predictive analysis, enhanced surveillance, personalized communications, and streamlining of data sharing while protecting patient privacy.[360]

Important benefits of adopting standards-based requirements for electronic case reporting include improved consistency of reporting specific data elements, increased efficiency of exchange (*e.g.,* by facilitating automated reporting), and greater public health data interoperability between health care and public health. Case reporting provides critical information to track communicable diseases, but manual processes have historically been ''slow, incomplete, and burdensome for healthcare and public health personnel.'' [361] Increasing connectivity through eCR ''can result in more accurate, complete, and timely data to support public health action''.[362] In turn, more timely detection of health-related conditions or events of public concern can result in rapid intervention and lowered disease transmission.[363] [364] More thorough reporting can also improve targeted interventions to improve health of vulnerable populations.[365]

Automated case reporting from healthcare to public health reduces the burden of required reporting for providers while improving the timeliness, accuracy, and completeness of case reports to support public health preparedness and response.[366] [367] One pilot found providers spent 2.4 seconds to transmit cases electronically, compared to 4.22 minutes manually.[368] To the extent case reporting happens automatically, it would also improve clinical care by allowing providers to focus on the medical needs of their patients without having to shift to consider related public health reporting.[369]

Requiring a single standard will help drive the industry and community at large to address issues within the standard and move towards adoption of a common standard for electronic case reporting. The use of FHIR-based solutions encourages more flexibility and reduced burden for set-up and maintenance and aligns with CDC's Public Health Data Strategy. The Public Health Data Strategy prioritizes electronic case reporting, particularly via mechanisms that reduce burden and encourage more complete and timely data exchange.[370] Adopting a common standard for case reporting would ensure case report information can be efficiently exchanged between healthcare and public health in the right format, through the right channel at the right time.[371]

While the benefits of these updates are not quantifiable at this time, we expect the proposed updates to significantly benefit end users of health IT and the patient populations they serve. The standards update and new requirements would result in increased public health data interoperability between health care and public health, which will enable better healthcare and public health decision making. Specifically, standards-based electronic case reporting would enable automatic, complete, accurate data to be reported in real-time to public health agencies which facilitates evidence-based decision-making for public health and reduces burden for health care providers. This would simultaneously support public health response efforts while reducing the time burden for providers to report. Standards-based reporting also streamlines required reporting to multiple jurisdictions and facilitates bi-directional communication between providers and public health.[372]

§ 170.315(f)(6) Antimicrobial Use and Resistance Reporting—Transmission to Public Health Agencies

We propose to revise the current certification criteria located in § 170.315(f)(6) Transmission to public health agencies—antimicrobial use and resistance reporting. We propose to update the standard listed in § 170.205(r) to HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release 3—US Realm for two specific components of the IG, detailed below, and incorporate it by reference in § 170.299. The two required sections updated in the IG are: HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (V5) specific document template in Section 1.1.14; and Antimicrobial Resistance Option (ARO) Summary Report (V3) specific document template in Section 1.1.2, which have already been advanced for voluntary adoption under ONC's Standards Version Advancement Process (SVAP). We are not proposing an update to the Antimicrobial Use (AUP) Summary Report (Numerator and Denominator), currently included in the criteria. We also propose minimal changes to the name of this certification criterion to, ''Antimicrobial use and resistance reporting—Transmission to public health agencies.''

Costs

This section describes the estimated costs of meeting requirements in the proposed update to § 170.315(f)(6), which are detailed in Table 41 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 34 shows the estimated labor costs per product to make the proposed updates in § 170.315(f)(6). We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur the costs in the tables below.

2. The number of products that will update to the revised AUR certification criterion is estimated based on the total number of currently certified products plus the number of new products we expect to certify to the certification criterion. Both estimates are adjusted for attrition. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(f)(6) and need to meet the proposed requirements. As of the end of 2022, 4% of developers and 5% of

[360] Public Health Data Modernization Executive Summary (*cdc.gov*).

[361] *digital-bridge-ecr-evaluation-report-12-32019.pdf* (*aimsplatform.org*).

[362] Ibid.

[363] The Promise of Electronic Case Reporting—PubMed (*nih.gov*).

[364] Public Health Agencies (*aimsplatform.org*).

[365] *digital-bridge-ecr-evaluation-report-12-32019.pdf* (*aimsplatform.org*).

[366] Improving Notifiable Disease Case Reporting Through Electronic Information Exchange-Facilitated Decision Support: A Controlled Before-and-After Trial—PubMed (*nih.gov*).

[367] A Modified Public Health Automated Case Event Reporting Platform for Enhancing Electronic Laboratory Reports with Clinical Data: Design and Implementation Study—PubMed (*nih.gov*).

[368] Piloting Electronic Case Reporting for Improved Surveillance of Sexually Transmitted Diseases in Utah—PMC (*nih.gov*)/.

[369] Public Health Agencies (*aimsplatform.org*).

[370] *Public_Health_Data_Strategy-final-P.pdf* (*cdc.gov*) *Public_Health_Data_Strategy-final-P.pdf* (*cdc.gov*).

[371] Public Health Data Interoperability (*cdc.gov*).

[372] Public Health Surveillance:—PMC (*nih.gov*).

products certified § 170.315(f)(6). Applying this modifier to our total developer and product estimates, we estimate that 26 currently certified products by 15 developers will be affected by our proposal.

In 2023, CMS finalized a requirement that eligible hospitals and critical access hospitals participating in the Medicare Promoting Interoperability Program must begin reporting a new AUR Surveillance measure for Electronic Health Record (EHR) reporting periods in 2024. Due to this new program requirement, we expect more Health IT Modules to certify the AUR certification criterion in the coming year(s). As a proxy for possible future certification of AUR, we used the number of products that are currently certified to § 170.315(f)(3) (Transmission to public health agencies—reportable laboratory tests and values/results) to estimate future certification of the AUR certification criterion. As of 2022, 58% of developers and 67% of products certified to § 170.315(f)(3), but not § 170.315(f)(6). Using these rates, we estimate that 22 developers will newly certify 31 products impacted by this rulemaking.

Overall, we estimate updates to the AUR certification criterion will impact 31 products certified by 22 developers for the first time (''New'') and 26 products already certified by 15 developers (''Current'') for an estimated total of 57 products certified by 37 developers.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[373] 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 $127.82.

BILLING CODE 4150–45–P

[373] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 34. Estimated Labor Hours for New and Currently Certified Products to Meet the Proposed Requirements in § 170.315(f)(6) Antimicrobial use and resistance reporting – Transmission to public health agencies

Activity	Details	Lower bound hours	Upper bound hours	Remarks
New Products				
Task 1: Standards update and reference new IG	Update the standard listed in § 170.205(r) to HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release –3 - US Realm and require updates to two specific components of the IG: (i) HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (V5) specific document template in Section 1.1.14; and (ii) Antimicrobial Resistance Option (ARO) Summary Report (V3) specific document template in Section 1.1.2.	1,000	1,500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement. (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement.
Currently Certified Products				
Task 1: Standards update and reference new IG	Update the standard listed in § 170.205(r) to HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release 3 - US Realm and require updates to two specific components of the IG: (i) HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (V5) specific document template in Section 1.1.14; and (ii) Antimicrobial Resistance Option (ARO) Summary Report (V3) specific document template in Section 1.1.2.	0	1,000	(1) Lower bound assumes health IT product was voluntarily updated through the ONC Standards Version Advancement Process (SVAP) (2) Upper bound assumes health IT product has not yet begun to update standards or adopt new IG.

Table 35. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(6) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Costs per new and currently certified products		
Task 1 [**New products**]: Standards update and reference new IG	$127,820	$191,730
Task 1 [**Currently certified products**]: Standards update and reference new IG	$0	$127,820
Total costs for new and currently certified products		
Task 1 [**New products - 31**]: Standards update and reference new IG	$3,962,420	$5,943,630
Task 1 [**Currently certified products - 26**]: Standards update and reference new IG	$0	$3,323,320
Total cost for all products (57 products)	**$3,962,420**	**$9,266,950**
Total cost per developer* (37 developers)	**$69,516**	**$162,578**

Notes: Costs per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (31 for new products, 26 for currently certified products = 57 for all products). Total cost per developer = Total cost for all products / Number of developers (37 developers). * Assumes 22 developers for new products and 15 developers for currently certified products.

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(6) would range from $127,820 to $191,730 for new products and $0 to $127,820 for currently certified products, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 57 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $4 to $9.3 million. Assuming 37 health IT developers in total (22 developers for new products and 15 developers for currently certified products), this would be an average cost per developer ranging from $69,516 to $162,578.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve. Collectively, proposed revisions to existing (f) certification criteria help remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies.

The monitoring of antimicrobial use and resistance is a vital component of public health reporting. The proposed updates to the certification criterion in § 170.315(f)(6) for antimicrobial use and resistance reporting can help facilitate timely reporting to public health agencies by reducing the burden for health care facilities to report. This in turn will allow prescribers to receive feedback regarding prescribing practices and improve the appropriate use of antimicrobials. Standards adoption can lead to more specific and complete information being shared with public health agencies, allowing for follow-up activities and research to address rising rates of antimicrobial resistance. The updated version includes new and updated reports, templates, and value sets that enable more advanced reports. These new and updated components provide additional contextual and clinical information for public health officials.

While the benefits of many of these modifications are not quantifiable at this time, we expect the updated IG to lead to more specific and complete information being shared with public health agencies, allowing for follow-up activities and research to address rising rates of antimicrobial resistance.

§ 170.315(f)(7) Health Care Surveys—Transmission to Public Health Agencies

We propose to revise the current certification criteria located in § 170.315(f)(7) Transmission to public health agencies—health care surveys. We propose to update the standard for health care survey information for electronic transmission specified in § 170.205(s) to HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1—US Realm and incorporate it by reference in § 170.299. To advance the electronic transmission of health care surveys and include the relevant and needed information to achieve its intent, we propose this version of the standard, as it includes new and updated templates with important context. We also propose to minimally change the name of this certification criterion to, ''Health care surveys—Transmission to public health agencies.''

Costs

This section describes the estimated costs of meeting requirements in the proposed update to § 170.315(f)(7), which are detailed in Table 43 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 36 shows the estimated labor costs per product to make the proposed updates in § 170.315(f)(7). 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 the tables below.

2. We estimate that 52 products certified by 43 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. The estimate of 52 products certified by 43 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(f)(7) and need to meet the proposed requirements. As of the end of 2022, 11% of developers and 10% of products certified § 170.315(f)(7). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[374] 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 $127.82.

Table 36. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(7) Health care surveys – Transmission to public health agencies

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Standards update and reference new IG	Update standard for health care survey information for electronic transmission specified to HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1 - US Realm	500	1,000	(1) Lower bound assumes health IT product has already begun to update standards and adopt new IG. (2) Upper bound assumes health IT product has not yet begun to update standards or adopt new IG.

Table 37. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(7) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: Standards update and reference new IG	$63,910	$127,820
Total cost per product	**$63,910**	**$127,820**
Task 1: Standards update and reference new IG	$3,323,320	$6,646,640
Total cost for all products (52 products)	**$3,323,320**	**$6,646,640**
Total cost per developer (43 developers)	**$77,287**	**$154,573**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (52 products). Total cost per developer = Total cost for all products / Number of developers (43 developers).

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(7) would range from $63,910 to $127,820 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual. Assuming 52 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range

[374] *https://www.bls.gov/oes/current/oes151252.htm.*

from $3.3 to $6.6 million. Assuming 112 health IT developers, this would be an average cost per developer ranging from $77,287 to $154,573.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve. Collectively, proposed revisions to existing (f) certification criteria help remove long-standing barriers to public health data interoperability, which in turn, will improve public health response and the nation's healthcare system, enabling better-informed decision making, more comprehensive data analytics, and faster, more coordinated responses to public health threats and emergencies.

Health care surveys help provide insight to inform policy, research, and quality, and sending them electronically allows for wider representation from hospitals and health care organizations, as well as reduces manual burden on the reporters.[375] Improving the process for electronic collection of survey data, including the use of standards, could make these important surveys easier to administer. Standards adoption will help advance the electronic transmission of health care surveys and include the relevant and needed information to achieve their intent. These additions and updates include, but are not limited to, revised sections for emergency department encounters, patient information sections, gender identity observation, and number of visits over the past 12 months. Such information will provide additional insight on trends in hospitalization, surveillance of symptomology and diagnoses, and demographics that can highlight disparities and better inform interventions.

While the benefits of many of these modifications are not quantifiable at this time, we expect the resulting improvements to interoperable exchange of health information to significantly benefit end users of health IT by making it easy to collect and report data for health care surveys. These updates will ultimately benefit patient populations as they data are used to inform efforts to improve quality of care, allocate health care resources, and eliminate disparities in the provision of health care services.

§ 170.315(f)(8) Birth Reporting—Transmission to Public Health Agencies

We propose a new certification criterion in § 170.315(f)(8), Birth reporting—Transmission to public health agencies. As a part of this new certification criterion, we propose to adopt the HL7 FHIR standard Vital Records Birth and Fetal Death Reporting 1.1.0—STU 1.1 in § 170.205(v) for electronically submitting medical and health information from birth certificate reports to public health agencies.

Costs

This section describes the estimated costs of meeting the proposed requirements in § 170.315(f)(8). Since this new certification criterion is not currently tied to any requirements, we estimate the costs for a single developer to voluntarily certify but do not assess industry wide costs associated with adoption. Thus, we estimate the number of labor hours that would be needed from a Health IT developer to perform each part of the proposed requirements for a given product. The level of effort associated with meeting requirements for a single product is detailed in Table 45 below and is based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 38 shows the estimated labor costs for a Health IT developer to meet the proposed requirements in § 170.315(f)(8) for a single product. 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 the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[376] 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 $127.82.

[375] DHCS—National Health Care Surveys Homepage (*cdc.gov*).

[376] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 38. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(8) Birth reporting – Transmission to public health agencies

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New requirement according to standard	Health IT must enable a user to create composition-provider live birth report for electronic transmission in accordance with the HL7 FHIR standard Vital Records Birth and Fetal Death Reporting 1.1.–0 - STU 1.1	1,000	2,000	(1) Lower bound assumes Health IT Module already has the technical capabilities to meet requirements but has not yet adopted the standard. (2) Upper bound assumes Health IT Module does not have technical capabilities to meet requirements.

Table 39. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(8) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: Standards update and reference new IG	$127,820	$255,640
Total cost per product	**$127,820**	**$255,640**

Notes: Total cost per product = Labor hours x Hourly wage.

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(8) would range from $127,820 to $255,640 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed updates are expected to have a wide range of benefits for end-users of health IT. Currently, health care providers rely on manual and duplicative data entry processes to report live births into State vital records programs. With most U.S. births occur at birthing facilities or in hospital settings, birth reporting typically entails clinicians supplying the medical and health information for the birth certificate to a State web-based Electronic Birth Registration System (EBRS). Typically, non-clinical hospital staff collect the legal and demographic information from the mother through a standardized worksheet, which is then entered into the State EBRS by hospital staff. This information is then sent to the State and a birth certificate is then issued by the State vital records authority. Most of the data necessary to report a live birth is also dually entered into EHRs by providers. As a result, birth reporting processes are duplicative and burdensome for providers and hospital systems. Adopting a standards-based approach to birth reporting would facilitate interoperability between the various systems involved in birth reporting, eliminate duplication of effort associated with entering information into multiple systems, and reduce burden of reporting for providers and hospital systems. Standards-based exchange would also improve the timeliness, accuracy, and completeness of birth reporting data.[377] [378]

While there has been very little uptake of the FHIR standard and associated functionalities by health IT vendors,[379] a pilot study of four Michigan hospitals and their EHRs found increased data completion and accuracy for many data items when births were reported using the FHIR standard and a SMART-on-FHIR app when compared to reports completed manually by hospital staff.[380] This early evidence suggests the standard, when adopted broadly, could aid in timely, more complete and accurate reporting from hospitals with reduced burden on the reporting facilities. While we recognize the burden associated with

[377] Standards for Vital Records (*cdc.gov*).

[378] MN Readiness Assessment Addendum Report September 2015 (*cdc.gov*).

[379] Subsection II–R New Interop Need Table_ HIMSS.pdf (*healthit.gov*).

[380] Final Report submitted to Centers for Disease Control and Prevention In response to Request for Task Order Proposal No. (MI 2020–Q–45799), June 16, 2023.

switching from largely manual processes to electronic, standards-based reporting, we expect significant cost savings from reduced manual data entry into multiple systems to surpass the one-time costs associated with implementation.

While the benefits of this proposal are not quantifiable at this time, we expect the proposed requirements to significantly benefit end users of health IT. Specifically, adopting a standards-based approach to birth reporting would enable consistent capture of critical data elements, facilitate public health data interoperability between health care and public health, and reduce reporting burden for health care providers.

§ 170.315(f)(9) Prescription Drug Monitoring Program (PDMP) Databases—Query, Receive, Validate, Parse, and Filter

We propose to create a new certification criterion in § 170.315(f)(9) Prescription Drug Monitoring Program (PDMP) Data—Query, receive, validate, parse and filter to enable the bidirectional interaction and electronic data exchange between health IT and PDMPs. We propose a new functional certification criterion in § 170.315(f)(9) that would be agnostic to a specific PDMP standard, but would include transport, content, and vocabulary standards where appropriate. We propose to additionally include functional requirements for access controls including access roles and audit logs within this new certification criterion. This certification criterion would enable a user to query a PDMP, including bidirectional interstate exchange, to receive PDMP data in an interoperable manner, to establish access roles in accordance with applicable law, and to maintain records of access and auditable events.

Costs

This section describes the estimated costs of meeting the proposed requirements in § 170.315(f)(9). Since this new certification criterion is not currently tied to any requirements, we estimate the costs for a single developer to voluntarily certify but do not assess industry wide costs associated with adoption. Thus, we estimate the number of labor hours that would be needed from a Health IT developer to perform each part of the proposed requirements for a given product. The level of effort associated with meeting requirements for a single product is detailed in Table 47 below and is based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 40 shows the estimated labor costs for a Health IT developer to meet the proposed requirements in § 170.315(f)(9) for a single product. 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 the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[381] 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 $127.82.

BILLING CODE 4150–45–P

[381] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 40. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(9) Prescription Drug Monitoring Program (PDMP) Data – Query, receive, validate, parse, and filter

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New functional requirement - *Query*	Health IT Module must enable both passive and active bi-directional query of a PDMP, including an interstate exchange query	0	1,000	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement
Task 2: New functional requirement – *Receive*	Health IT Module must enable a user to receive electronic PDMP information	0	500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement
Task 3: New functional requirement – *Validate*	Health IT Module must enable a user to demonstrate the ability to detect valid and invalid electronic PDMP information received	0	500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement
Task 4: New functional requirement – *Parse and filter*	Health IT Module must enable a user to parse and filter electronic PDMP information received and validated	0	500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement

				(2) Upper bound assumes health IT does not have the technical capabilities to meet requirement
Task 5: New functional requirements – *Access controls*	Health IT Module must enable access controls including access roles and recording access including actions for auditable events and tamper-resistance.	0	500	(1) Lower bound assumes health IT already has the technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement

Table 41. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(9) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New functional requirement – Query	$0	$127,820
Task 2: New functional requirement – Receive	$0	$63,910
Task 3: New functional requirement – Validate	$0	$63,910
Task 4: New functional requirement – Parse and filter	$0	$63,910
Task 5: New functional requirements – Access controls	$0	$63,910
Total cost per product	**$0**	**$383,460**

Notes: Total cost per product = Labor hours x Hourly wage.

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(9) would range from $0 to $383,460 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed updates have a wide range of expected benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve. PDMPs are useful tools to help inform decision-making at the point of care and promote safe prescribing practices.[382] However, PDMPs are only useful if providers check the PDMP prior to prescribing controlled substances. Therefore, recent efforts, such as mandated use of PDMPs for prescribers and integrating PDMPs into EHRs,[383] [384] [385] have focused on increasing the frequency of PDMP use and the usability of information contained in them by ensuring that PDMP data are easily accessible in clinical workflows and across State lines.[386] [387] Early evidence suggests efforts to make PDMPs easier to access and use can aid prescribers in making informed clinical decisions and lead to reductions in controlled substance prescriptions for patients.[388]

[382] Prescription Drug Monitoring Programs (PDMPs) | Healthcare Professionals | Opioids | CDC.

[383] *TAG_Mandatory_Enrollment_Use_20200710.pdf* (*pdmpassist.org*).

[384] Prescription Drug Monitoring Programs (PDMPs) | Drug Overdose | CDC Injury Center.

[385] Integrating & Expanding Prescription Drug Monitoring Program Data: Lessons from Nine States (*cdc.gov*).

[386] Leveraging Prescription Drug Monitoring Program (PDMP) Data in Overdose Prevention and Response (*cdc.gov*).

[387] Physicians have Widespread Access to State PDMP Data, but Data Sharing Varies Across States—Health IT Buzz Health IT Buzz.

[388] National Estimates and Physician-Reported Impacts of Prescription Drug Monitoring Program Use | SpringerLink.

While requirements and incentives are in place for providers to access PDMPs, there are no known requirements regarding the capability for health IT to query PDMPs directly, creating a gap in interoperability. There are also no requirements for integrating query information into clinical workflows within health IT systems. These functionalities are critical components to ensuring PDMP data interoperability as State mandates for prescribers to query the PDMP cannot be effective if the technology is not there to support this requirement. A recent study found that the uptick in PDMP use following the adoption of a State mandate requiring clinicians to query the PDMP before prescribing opioids was considerably smaller than the changes resulting from an EHR-integrated PDMP tool making PDMP data easier to access and use.[389] Inclusion of a functional certification criterion to support PDMP data exchange will help ensure that health IT has the functional capabilities required to engage with a PDMP meeting the definitions under Section 5042(a) of the SUPPORT Act.[390] These capabilities include enabling health IT systems to support integration of query into clinical workflows informed by established CDC guidelines for opioid prescribing and to support requirements for the capability to reconcile queried data as discrete data elements (not just as read only). Implementing these functionalities would promote interoperability between health IT and PDMPs and increase providers' access to PDMP data at the point of care.

There is substantial evidence to suggest that integrating query information into clinical workflows within health IT systems would help reduce clinical burden and increase the likelihood that authorized users check the PDMP,[391] as PDMP–EHR integration has been shown to be associated with greater frequency and ease of PDMP use.[392] [393] [394] [395] [396] [397] A 2020 GAO analysis of interviews with physicians and PDMP officials estimated that checking a PDMP database integrated into the EHR takes 2–15 seconds, compared with 3–5 minutes for checking a PDMP database not integrated into the EHR.[398] The same GAO report noted that PDMPs not integrated into the EHR required more than a dozen additional mouse clicks, representing significant time savings for authorized users to check the PDMP.[399] PDMP–EHR integration is widely recognized as a strategy for improving the utility of PDMPs in inpatient and outpatient settings. A 2016 expert panel to define best practices for PDMPs in the emergency department setting recommended that prescription drug monitoring program data should be pushed into hospital EHRs.[400] Recent surveys and semi-structured interviews also found that PDMP–EHR integration was preferred by multi-disciplinary health care providers, who felt that improving the interface and function of the PDMP through integration would increase PDMP use.[401] [402]

In addition to providing benefits to end users of health IT, including prescribers and pharmacists, these requirements would benefit patient populations by increasing the provision of guideline-concordant care, such as checking the PDMP before prescribing opioids to confirm the appropriateness of treatment. One systematic review found that PDMP use influences health care providers' clinical decision-making in relation to the supply of controlled substances, refusal to prescribe or treat, risk mitigation strategies, communication, education and counselling, referrals and care coordination, and stigma.[403] PDMP use has also been shown to be associated with several benefits including reductions in opioid prescribing rates, opioid-related inpatient stays, and opioid-related emergency department visits as well as better care coordination for patients and informed clinical decision-making.[404] [405] [406] PDMP supports which allow for integration and the interoperability of PDMP data can support advancement of patient-centered care that focuses on the specific needs, and safety, of the individual. For example, the viewing of opioid therapies and nonopioid therapies together supports the 2022 CDC Clinical Practice Guideline for Prescribing Opioids, Recommendation 1: ''Nonopioid therapies are at least as effective as opioids for many common types of acute pain. Clinicians should maximize use of nonpharmacologic and nonopioid pharmacologic therapies as appropriate for the specific condition and patient and only consider opioid therapy for acute pain if benefits are anticipated to outweigh risks to the patient. Before prescribing opioid therapy for acute pain, clinicians should discuss with patients the realistic benefits and known risks of opioid therapy.'' [407] The CDC recommends that PDMP data should be reviewed before every opioid prescription for acute, subacute, or chronic pain. Universal application of PDMP queries would mitigate bias and therefore the recommendation is that clinicians should query the PDMP when feasible for all patients rather than differentially based on assumptions about what they will learn about specific patients. EHR integration of PDMP data would increase feasibility of universal application.

While the benefits of many of these modifications are not quantifiable at this time, we expect the resulting improvements to significantly improve data interoperability between health IT systems and PDMPs, which will reduce burden on providers to access the PDMP and improve their access to information

[389] Prescription Drug Monitoring Program Mandates: Impact On Opioid Prescribing And Related Hospital Use—PMC (*nih.gov*).

[390] Report to Congress: State Challenges and Best Practices Implementing PDMP Requirements Under Section 5042 of the SUPPORT Act (*medicaid.gov*).

[391] Leveraging Prescription Drug Monitoring Programs and Health Information Technology for Addressing Substance Use Disorder and Opioid Use Disorder (LPASO) (*healthit.gov*).

[392] National Estimates and Physician-Reported Impacts of Prescription Drug Monitoring Program Use—PubMed (*nih.gov*).

[393] The Impact of a PDMP–EHR Data Integration combined with Clinical Decision Support on Opioid and Benzodiazepine Prescribing Across Clinicians in a Metropolitan Area—PMC (*nih.gov*).

[394] Provider perspectives and experiences following the integration of the prescription drug monitoring program into the electronic health record—Matthew Witry, Barbara St Marie, Jeffrey Reist, 2022 (*sagepub.com*).

[395] Effect of Integrating Access to a Prescription Drug Monitoring Program Within the Electronic Health Record on the Frequency of Queries by Primary Care Clinicians: A Cluster Randomized Clinical Trial—PubMed (*nih.gov*).

[396] Barriers and facilitators to PDMP IS Success in the US: A systematic review—PubMed (*nih.gov*)/.

[397] Provider beliefs on the Barriers and Facilitators to Prescription Monitoring Programs and Mandated Use—PubMed (*nih.gov*).

[398] Prescription Drug Monitoring Programs: Views on Usefulness and Challenges of Programs | U.S. GAO.

[399] Ibid.

[400] Best Practices for Prescription Drug Monitoring Programs in the Emergency Department Setting: Results of an Expert Panel—PubMed (*nih.gov*).

[401] Barriers to Increasing Prescription Drug Monitoring Program . . . : CIN: Computers, Informatics, Nursing (*lww.com*).

[402] Provider beliefs on the Barriers and Facilitators to Prescription Monitoring Programs and Mandated Use—PubMed (*nih.gov*).

[403] How prescription drug monitoring programs influence clinical decision-making: A mixed methods systematic review and meta-analysis—ScienceDirect.

[404] Prescription Drug Monitoring Program Mandates: Impact On Opioid Prescribing And Related Hospital Use—PMC (*nih.gov*).

[405] Integrating & Expanding Prescription Drug Monitoring Program Data: Lessons from Nine States (*cdc.gov*).

[406] National Estimates and Physician-Reported Impacts of Prescription Drug Monitoring Program Use—PubMed (*nih.gov*).

[407] CDC's Clinical Practice Guideline for Prescribing Opioids for Pain | Guidelines | Healthcare Professionals | Opioids | CDC.

needed for clinical decision-making. Reductions in clicks needed to access the PDMP translates to reductions in time in takes staff to access and review PDMP data, which could result in significant time and cost savings for prescribers to access and use PDMP data. Timely access to PDMP data can help improve care coordination for individual patients, but it can also be an important tool for public health surveillance by enabling health departments to identify at-risk communities and provide targeted outreach and intervention.[408] We expect these improvements to benefit both individual patients and communities by enabling prescribers to make informed treatment decisions and equipping public health agencies with the information needed to develop initiatives for safe and appropriate prescribing, prevention and treatment of substance use disorders, and risk-reduction for opioid overdose.[409]

[408] In Brief, Prescription Drug Monitoring Programs: A Guide for Healthcare Providers (*samhsa.gov*).

b. Proposed New Certification Criteria for Health IT Modules Supporting Public Health Data Exchange in § 170.315(f)

§ 170.315(f)(21) Immunization Information—Receive, Validate, Parse, Filter, and Exchange—Response

We propose a new certification criterion for immunization information receipt, validation, parsing, and filtering, as well as exchange and response as a complement to the proposed updated requirements in § 170.315(f)(1). We propose requirements in § 170.315(f)(21) to enable a system to receive, validate, parse, and filter electronic immunization information in accordance with the standard and applicable implementation guide specified in § 170.205(e). We also propose a new functional exchange requirement for the capability to respond to incoming patient-level and/or immunization-specific queries from external systems.

Costs

This section describes the estimated costs for an Immunization information system (IIS) vendor to meet the proposed requirements in § 170.315(f)(21). Since this certification criterion is not currently tied to any requirements, we estimate the costs for a single developer to voluntarily certify but do not assess industry wide costs associated with adoption. While it is common for jurisdictions to customize their IIS to meet their unique needs, here we assess the costs associated with updating the base functionality of an IIS to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from an IIS vendor to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 49 below and are based on the following assumptions:

1. IIS vendors will use the same labor costs and data models. Table 42 shows the estimated labor costs for a vendor to meet the proposed requirements in § 170.315(f)(21) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all IIS vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[410] 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 $127.82.

[410] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 42. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(21) Immunization information – Receive, validate, parse, filter, and exchange – response

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New requirement according to standard – *Receive, validate, parse and filter*	IIS systems must be able to receive, validate, parse and filter incoming data in accordance with the standard and applicable implementation specifications specified in § 170.205(e)	0	1,000	(1) Lower bound assumes IIS already has the technical capabilities to meet requirement (2) Upper bound assumes IIS does not have the technical capabilities to meet requirement
Task 2: New functional requirement – *Exchange - response*	IIS systems must be able to respond to incoming patient-level and/or immunization-specific queries from external systems.	0	1,000	(1) Lower bound assumes IIS already has the technical capabilities to meet requirement (2) Upper bound assumes IIS does not have the technical capabilities to meet requirement

Table 43. Summary of Costs for a Public Health Data System to Meet the Proposed Requirements in § 170.315(f)(21) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New requirement according to standard – Receive, validate, parse, and filter	$0	$127,820
Task 2: New functional requirement – Exchange – response	$0	$127,820
Total cost per system	**$0**	**$255,640**

Notes: Total cost per system = Labor hours x Hourly wage.

The cost to an IIS vendor to meet the proposed requirements in § 170.315(f)(21) would range from $0 to $255,640 per system, on average. This would be a one-time cost to developers per system that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting public health data exchange would benefit public health agencies (PHAs) who rely on timely, actionable data from healthcare partners. While the benefits associated with this proposal are not quantifiable at this time, we expect adoption of these new functional requirements in (f)(21) to improve bidirectional interoperability between healthcare and public health. By including functions performed by public health facing technology within the certification criterion, foundational capabilities will be in place by receiving

technology for bidirectional data exchange, completing a critical component of the immunization exchange workflow.

Functionality for receipt, validation, transmission, query/response, and patient access will enable more users, including those using a variety of health IT systems, to have the most complete and accurate vaccine history for individuals. This functionality can help advance EHRs, IISs, and intermediaries in alignment, with the same foundational functionalities, and that data are moving with the speed of care. If an individual receives a vaccine from a pharmacy, from a community health clinic, away from their home State, or at their provider's office, any approved user, regardless of their health IT system, should be able to have access to their complete, accurate vaccine history. Further, it aligns the technology used by public health officials and immunization programs with the same standard that providers and health care organizations are required to use for transmission, without additional manual effort or manipulation. We believe these proposed requirements, coupled with proposed (g)(20) and updates to (f)(1), can move the nation closer to this ideal state.

§ 170.315(f)(22) Syndromic Surveillance—Receive, Validate, Parse, and Filter

We propose a new certification criterion for the functional requirement to receive, validate, parse, and filter incoming syndromic surveillance information in accordance with the standard and applicable implementation guide specified in § 170.205(d). The transmission of information electronically must be accompanied by the ability for public health technology to receive and validate information according to the same standard and use these standardized data for analysis and to inform next steps. Receipt and validation functions are needed to reduce the need for manual effort or manipulation related to data integration and processing, and to allow for the prompt intake and analysis of information.

Costs

This section describes the estimated costs for a syndromic surveillance system vendor to meet the proposed requirements in § 170.315(f)(22). Since this certification criterion is not currently tied to any requirements, we estimate the costs for a single vendor to voluntarily certify but do not assess industry wide costs associated with adoption. While jurisdictions may customize their systems to meet their unique needs, here we assess the costs associated with updating the base functionality of surveillance systems to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from surveillance system vendors to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 51 below and are based on the following assumptions:

1. Syndromic surveillance system vendors will use the same labor costs and data models. Table 44 shows the estimated labor costs for a developer to meet the proposed requirements in § 170.315(f)(22) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[411] 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 $127.82.

Table 44. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(22) Syndromic surveillance – Receive, validate, parse and filter

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New functional requirements – *Receive, validate, parse and filter*	Syndromic surveillance system must be capable of receiving, validating, parsing and filtering electronic syndrome-based public health surveillance information received and formatted in accordance with the standards specified in § 170.207(d).	0	750	(1) Lower bound assumes system already has the technical capabilities to meet requirement (2) Upper bound assumes system does not have the technical capabilities to meet requirement

[411] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 45. Summary of Costs for a Public Health Data System to Meet the Proposed Requirements in § 170.315(f)(22) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New functional requirement – Receive, validate, parse, and filter	$0	$95,865
Total cost per system	**$0**	**$95,865**

Notes: Total cost per system = Labor hours x Hourly wage.

The cost to a vendor to meet the proposed requirements in § 170.315(f)(22) would range from $0 to $95,865 per system, on average. This would be a one-time cost to developers per system that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting public health data exchange would benefit public health agencies (PHAs) who rely on timely, actionable data from healthcare partners and promote public health data interoperability. Syndromic surveillance information is vital to the monitoring and early detection of potential public health events and can help provide PHAs with the information needed to prevent a threat from becoming a public health emergency. The transmission of information electronically, according to the standard specified in § 170.205(d), must be accompanied by the ability for public health systems to receive and validate information according to the same standard, and use the standardized data for analysis and to inform next steps. Receipt and validation functions would benefit public health agencies by reducing the need for manual effort or manipulation related to data integration and processing and allowing for prompt intake and analysis of information. The pandemic raised the importance of certain data elements being included in the standard to better assess hot spots and inform response, including travel status, pregnancy status, acuity, and admission information—all of which are reflected in the updated version of the standard specified in § 170.205(d).

While the benefits of adopting this new functional requirement are not quantifiable at this time, we expect the resulting improvements to help reduce the time needed to onboard new data sources and make syndromic surveillance able to scale and respond to new public health threats as well as meet daily operational needs. Additionally, it would create a foundational functionality requirement for all syndromic surveillance systems to be able to validate and assess incoming information quickly to identify emerging threats. While receipt is a function that most syndromic surveillance systems can accomplish today, our proposal to certify this functionality would allow for several additional benefits. First, it would include both sending and receiving systems in testing the shared standard, finding issues, and aligning on how to constrain specifications to limit variability. Second, it would advance syndromic surveillance technology on the same path as the systems reporting data to them, to allow all involved systems to grow and align in concert when it comes to data exchange—eliminating the need for manual workarounds or costly third parties to fill the gaps between functionalities. Third, the coordination between sending and receiving systems would compel nationwide upgrades and transitions as needs and use cases evolve and shift.

§ 170.315(f)(23) Reportable Laboratory Test Values/Results—Receive, Validate, Parse, and Filter

We propose a new requirement in § 170.315(f)(23) to enable technology to receive, validate, parse, and filter incoming laboratory tests and results/values according to the standard in § 170.205(g)(3), the HL7® Laboratory Results Interface (LRI) Implementation Guide, or the ELR IG. By requiring Health IT Modules supporting public health data exchange to receive results and values electronically (according to national standards), more complete patient information will be available to clinicians throughout the laboratory workflow and for public health action.

Costs

This section describes the estimated costs for a system vendor to meet the proposed requirements in § 170.315(f)(23). Since this certification criterion is not currently tied to any requirements, we estimate the costs for a single vendor to voluntarily certify but do not assess industry wide costs associated with adoption. While jurisdictions may customize their systems to meet their unique needs, here we assess the costs associated with updating the base functionality of systems to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from vendors to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 53 below and are based on the following assumptions:

1. Vendors will use the same labor costs and data models. Table 46 shows the estimated labor costs for a developer to meet the proposed requirements in § 170.315(f)(23) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[412] 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 $127.82.

[412] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 46. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(23) Reportable laboratory test values/results – Receive, validate, parse, and filter

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New requirement according to standard – *Receive, validate, parse and filter*	System must be able to receive, validate, parse and filter reportable laboratory test results/values according to the HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface, Release 1 STU Release 4 - US Realm (LRI) specified in § 170.205(g)(3) or ELR IG.	500	2,500	(1) Lower bound assumes system already has the technical capabilities to meet requirement. (2) Upper bound assumes system does not have the technical capabilities to meet requirement.

Table 47. Summary of Costs for a Public Health Data System to Meet the Proposed Requirements in § 170.315(f)(23) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New requirement according to standard – Receive, validate, parse, and filter	$63,910	$319,550
Total cost per system	**$63,910**	**$319,550**

Notes: Total cost per system = Labor hours x Hourly wage.

The cost to a vendor to meet the proposed requirements in § 170.315(f)(23) would range from $63,910 to $319,550 per system, on average. This would be a one-time cost to developers per system that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting public health data exchange would benefit public health agencies (PHAs) who rely on timely, actionable data from healthcare partners and laboratories. The proposed requirements would help increase the data shared between health care providers, laboratories, and public health agencies, and would increase interoperability among the different systems in place at each entity. To encompass all aspects of the laboratory workflow, the proposed requirements in § 170.315(f)(23) for public health data systems to receive results and values electronically according to the LRI IG align with the proposed requirements in § 170.315(a)(2) for a user to create and transmit laboratory orders electronically according to the HL7® Laboratory Order Interface (LOI) Implementation Guide and the proposed requirements in § 170.315(f)(3) for Health IT Modules to create and transmit laboratory orders according to the LOI IG and receive laboratory results according to the LRI IG.

Together, these proposals will help ensure that laboratory results and orders are sent and received according to the same standards and that all systems involved in the workflow have the same baseline functionality.

While the benefits of this proposal are not quantifiable at this time, the proposed requirements would help ensure that public health agencies are able to receive electronically transmitted laboratory values/results in their system(s) in a standardized format, resulting in more complete patient information being available for public health action. We expect adoption of the LRI IG, in particular, to enable providers and laboratories to send more complete data to public health agencies that are needed to inform rapid response and assist with contact tracing and patient outreach during outbreaks of infectious disease.

§ 170.315(f)(24) Cancer Pathology Reporting—Receive, Validate, Parse, and Filter

We propose a new certification criterion for receiving and validating incoming cancer pathology reports according to the proposed standard in

§ 170.205(i)(4), Cancer Pathology Data Sharing 1.0.0—STU1. In order for cancer registries to receive, validate, parse and filter these reports according to the standard proposed in § 170.315(f)(4), we propose to include an accompanying requirement for the receipt, validation, parsing, and filtering of cancer pathology reports in § 170.315(f)(24).

Costs

This section describes the estimated costs for a cancer registry vendor to meet the proposed requirements in § 170.315(f)(24). Since this certification criterion is not currently tied to any requirements, we estimate the costs for a single vendor to voluntarily certify but do not assess industry wide costs associated with adoption. While jurisdictions may customize their registries to meet their unique needs, here we assess the costs associated with updating the base functionality of systems to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from cancer registry vendors to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 55 below and are based on the following assumptions:

1. Cancer registry vendors will use the same labor costs and data models. Table 48 shows the estimated labor costs for a vendor to meet the proposed requirements in § 170.315(f)(24) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[413] 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 $127.82.

Table 48. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(24) Cancer pathology reporting – Receive, validate, parse and filter

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New requirement according to standard – Receive, validate, parse and filter	Systems must be able to receive, validate, parse and filter cancer pathology reports in accordance with the standard and applicable implementation specifications in § 170.205(i)(4).	0	1,000	(1) Lower bound assumes cancer registry already has the technical capabilities to meet requirement (2) Upper bound assumes cancer registry does not have the technical capabilities to meet requirement

Table 49. Summary of Costs for a Public Health Data System to Meet the Proposed Requirements in § 170.315(f)(24) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New requirement according to standard – Receive, validate, parse, and filter	$0	$127,820
Total cost per system	**$0**	**$127,820**

Notes: Total cost per system = Labor hours x Hourly wage.

The cost to a vendor to meet the proposed requirements in § 170.315(f)(24) would range from $0 to $127,820 per system, on average. This would be a one-time cost to developers per system that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting public health

[413] *https://www.bls.gov/oes/current/oes151252.htm.*

data exchange would benefit public health agencies (PHAs) who rely on timely, actionable data from healthcare partners and promote public health data interoperability. This proposal would support cancer registries in having the functionality to accept information in the same standard as sending systems, as well as help sending and receiving technology progress at the same rate, with aligned functionality.

CDC's National Program of Cancer Registries has been actively working with State public health agencies and pathology partners, including the College of American Pathologists (CAP), to develop and pilot the FHIR Implementation Guide for cancer pathology reporting. Early results of these pilots demonstrate that use of FHIR by all involved systems will reduce the need for manual intervention and data cleansing, aid in more timely reporting, and include more complete information, including the demographic information needed to confirm reporting is happening within the patient's State of residence, rather than the State of treatment, as well as for patient matching.[414] [415] [416]

While the benefits of this proposal are not quantifiable at this time, we expect the inclusion of receipt, validation, parsing, and filtering of electronic cancer pathology reporting in the Program to result in more complete, accurate diagnostic information being received by State cancer registries. Not only would our proposal support cancer registries in having the functionality to accept information in the same standard as sending systems, but it would help sending and receiving technology progress at the same rate, with aligned functionality. The proposed requirements would also enable cancer registries to receive pathology reports in a structured format rather than narrative form, which would help facilitate use of these data for research, analysis, and intervention.

§ 170.315(f)(25) Electronic Case Reporting—Receive, Validate, Parse, and Filter Electronic Initial Case Reports and Reportability Response; and Create and Transmit Reportability Response

In the HTI–2, we propose requirements in § 170.315(f)(5) for compliance with the HL7 eCR FHIR IG for electronic case reporting from hospitals and providers to public health agencies. We propose a corresponding requirement in § 170.315(f)(25) for technology in place at public health agencies to receive, validate, parse, and filter electronic case reports as well as create and electronically transmit a reportability response (RR) according to the standards referenced in § 170.205(t)(3). This requirement would help advance the technology that receives reported data in alignment with the technology that transmits the reports, adhering to the same foundational functions and standards.

Costs

This section describes the estimated costs for a case surveillance system vendor to meet the proposed requirements in § 170.315(f)(25). Since this certification criterion is not currently tied to any requirements, we estimate the costs for a single developer to voluntarily certify but do not assess industry wide costs associated with adoption. While jurisdictions may customize their systems to meet their unique needs, here we assess the costs associated with updating the base functionality of systems to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from system vendors to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 57 below and are based on the following assumptions:

1. System vendors will use the same labor costs and data models. Table 50 shows the estimated labor costs for a developer to meet the proposed requirements in § 170.315(f)(25) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[417] 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 $127.82.

[414] Pursuing Data Modernization in Cancer Surveillance by Developing a Cloud-Based Computing Platform: Real-Time Cancer Case Collection | JCO Clinical Cancer Informatics (*ascopubs.org*).

[415] Using informatics to improve cancer surveillance—PMC (*nih.gov*).

[416] The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities—PubMed (*nih.gov*).

[417] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 50. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(25) Electronic case reporting – Receive, validate, parse, filter, electronic initial case reports and reportability response; and create and transmit reportability response

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New functional requirement– *Receive, validate, parse and filter*	Technology must be able to receive, validate, parse and filter electronic case reports in accordance with the standard and applicable implementation specifications referenced in § 170.205(t)(2).	500	1,500	(1) Lower bound assumes system already has the technical capabilities to meet requirement (2) Upper bound assumes system does not have the technical capabilities to meet requirement
Task 2: New functional requirement – *Reportability response*	Technology must be able to consume and process a reportability response according to RR profiles of HL7 FHIR eCR IG in § 170.205(t)(2).	500	1,500	(1) Lower bound assumes system already has the technical capabilities to meet requirement (2) Upper bound assumes system does not have the technical capabilities to meet requirement

Table 51. Summary of Costs for a Public Health Data System to Meet the Proposed Requirements in § 170.315(f)(25) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New functional requirement – Receive, validate, parse, and filter	$63,910	$191,730
Task 2: New function requirements – Reportability response	$63,910	$191,730
Total cost per system	**$127,820**	**$383,460**

Notes: Total cost per system = Labor hours x Hourly wage.

The cost to a vendor to meet the proposed requirements in § 170.315(f)(25) would range from $127,820 to $383,460 per system, on average. This would be a one-time cost to developers per system that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting public health data exchange would benefit public

health agencies (PHAs) who rely on timely, actionable data from healthcare partners and promote public health data interoperability. While the benefits of adopting these proposed requirements are not quantifiable at this time, we expect the resulting improvements to reduce burden associated with processing case reports and alleviate the need for manual intervention. Further, these requirements would help advance and align technology that receives reported data with the technology that transmits case reports, adhering to the same foundational functions and standards. Adherence to a single standard, particularly the FHIR IG, will benefit public health agencies by encouraging consistent implementation and promoting greater interoperability compared to referencing multiple standards. Further, the HL7 eCR FHIR IG allows public health agencies to have more control in configuration, including the data elements and frequency of initial case notifications. Upgrading public health facing technology and tools to support APIs and FHIR payload, as included in the HL7 FHIR eCR IG, creates greater flexibility to respond to emergency issues. Improvements in consistent implementation and interoperability would enable PHAs to have an improved picture of where and when disease outbreaks occur. Supporting this alignment allows the industry to advance in harmony and creates a more scalable infrastructure in times of emergency.

Aligning requirements for systems sending and receiving electronic case reports was generally supported by commenters to HTI–1, who suggested that systems receiving electronic case reports should also have to certify to capabilities that align with the requirements in § 170.315(f)(5). One commenter stated that there is little value in requiring the capability to transmit electronic case reporting if public health partners do not have the capabilities to receive data electronically. Some commenters stated that they are prepared to support electronic case reporting but have not been able to do so due to lack of public health capacity to receive it. The proposed requirements would therefore help to create alignment between senders and receivers of case report data and enable bidirectional communication between health care and public health. Such improvements in public health data interoperability are critical to enabling public health agencies to receive complete and accurate case report information in a timely manner in order to identify and monitor cases of nationally notifiable conditions, respond quickly to outbreaks of infectious disease, and informs programs and interventions aimed at reducing the incidence of disease.

While the benefits of this proposal are not quantifiable at this time, we expect adoption of standards-based requirements for electronic case reporting to result in improved consistency of reporting specific data elements to public health, increased efficiency of exchange (*e.g.,* by facilitating automated reporting), and greater public health data interoperability between health care and public health. Increasing connectivity through standards-based, electronic case reporting can help ensure that more complete, accurate, timely data are available to support public health response.[418] [419] In turn, more timely detection of health-related conditions or events of public concern can result in rapid intervention and lowered disease transmission.[420] [421] More thorough reporting can also improve targeted interventions to improve health of vulnerable populations.[422]

§ 170.315(f)(28) Birth Reporting—Receive, Validate, Parse, and Filter

We propose a requirement in § 170.315(f)(28) for the receipt, validation, parsing, and filtering of incoming birth reports according to the FHIR IG for birth reporting in § 170.205(v) and referenced in § 170.315(f)(8) to create alignment between systems sending and receiving birth reports. Inclusion of the FHIR standard in regulation would align the technology receiving birth reports with those sending the reports.

Costs

This section describes the estimated costs for an electronic birth registry system (EBRS) vendor to meet the proposed requirements in § 170.315(f)(28). Since this certification criterion is not currently tied to any requirements, we assess the cost for a single developer to voluntarily certify but do not assess industry wide costs associated with adoption. While jurisdictions may customize their systems to meet their unique needs, here we assess the costs associated with updating the base functionality of EBRS to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from system vendors to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 59 below and are based on the following assumptions:

1. EBRS vendors will use the same labor costs and data models. Table 52 shows the estimated labor costs for a developer to meet the proposed requirements in § 170.315(f)(25) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[423] 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 $127.82.

[418] digital-bridge-ecr-evaluation-report-12-32019.pdf (aimsplatform.org).

[419] Completeness and timeliness of notifiable disease reporting: a comparison of laboratory and provider reports submitted to a large county health department | BMC Medical Informatics and Decision Making | Full Text (*biomedcentral.com*).

[420] The Promise of Electronic Case Reporting—PubMed (*nih.gov*).

[421] Public Health Agencies (*aimsplatform.org*).

[422] *digital-bridge-ecr-evaluation-report-12-32019.pdf* (*aimsplatform.org*).

[423] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 52. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(28) Birth reporting – Receive, validate, parse, and filter.

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New requirement according to standard – *Receive, validate, parse and filter*	EBRS must be able to receive, validate, parse and filter electronic case reports in accordance with the standard and applicable implementation specifications referenced in § 170.205(v)	1,000	2,000	(1) Lower bound assumes EBRS already has the technical capabilities to meet requirement (2) Upper bound assumes EBRS does not have the technical capabilities to meet requirement

Table 53. Summary of Costs for a Public Health Data System to Meet the Proposed Requirements in § 170.315(f)(28) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New functional requirement – Receive, validate, parse, and filter	$127,820	$255,640
Total cost per system	**$127,820**	**$255,640**

Notes: Total cost per system = Labor hours x Hourly wage.

The cost to a vendor to meet the proposed requirements in § 170.315(f)(28) would range from $127,820 to $255,640 per system, on average. This would be a one-time cost to developers per system that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting public health data exchange would benefit public health agencies (PHAs) who rely on timely, actionable data from healthcare partners and promote public health data interoperability. Birth reporting helps inform public health programs, is used for research and surveillance, and is used to produce the birth certificates needed for proof of identification, accessing benefits, and other administrative purposes. However, much of the birth reporting process currently relies on manual data entry and there remains a gap in public health agencies' ability to receive and integrate data within applicable public health technology, particularly for data received used FHIR-based standards.

Requiring that technology receiving birth reports can do so according to the standard specified in § 170.315(f)(8) would create alignment between sending and receiving systems. Inclusion of the ability to receive and validate FHIR within applicable public health technology supporting birth reporting will also provide a baseline set of capabilities that public health technology vendors can build on as additional FHIR-based approaches emerge for public health, including Bulk Import of data and FHIR Questionnaires. The receipt of FHIR for birth records also supports investments being made by CDC to receive FHIR messages downstream through the Data Modernization Initiative.[424] While the benefits of this proposed requirement are not quantifiable at this time, we expect adoption of the FHIR IG for birth reporting to reduce implementation and maintenance burden, and lead to greater consistency and completeness in reported information.

[424] *https://www.cdc.gov/surveillance/data-modernization/technologies/cdc-front-door.html.*

§ 170.315(f)(29) Prescription Drug Monitoring Program (PDMP) Databases—Receive, Validate, Filter, and Parse Prescription Data, Support Query and Exchange

We propose to introduce functional certification criteria certifying the ability of Health IT Modules supporting public health use cases to receive and validate reported PDMP information, and to initiate and respond to queries from providers or other PDMP databases and hubs. To complement our proposal in § 170.315(f)(9) to support certification of health IT used by providers to be capable of requesting data from PDMP databases, we also believe it is important to certify the capability of

public health systems, including PDMP technology, to respond to queries submitted. Our proposal will require that functionality is based on open, consensus-based practices where possible, allowing PDMPs to have the ability to exchange information without undue burden. Additionally, PDMPs should have the capability to support interstate data sharing (or queries) to better inform prescribing practices and monitor drug misuse and diversion. ONC proposes a set of functional certification criteria in § 170.315(f)(29) for receiving and validating reported data and initiating and responding to queries from applicable health IT, including other State PDMPs, to support applicable health IT capabilities required under Section 5042(a) of the Support Act.

Costs

This section describes the estimated costs for a PDMP vendor to meet the proposed requirements in § 170.315(f)(29). Since this certification criterion is not currently tied to any requirements, we assess the cost for a single PDMP developer to voluntarily certify but do not assess industry wide costs associated with adoption. While States may customize their systems to meet their unique needs, here we assess the costs associated with updating the base functionality of systems to meet the above requirements. Thus, we estimate the number of labor hours that would be needed from PDMP vendors to perform each part of the proposed requirements for a given system. Each task is assumed to have its own level of effort, and these estimates are detailed in Table 61 below and are based on the following assumptions:

1. PDMP vendors will use the same labor costs and data models. Table 54 shows the estimated labor costs for a developer to meet the proposed requirements in § 170.315(f)(25) for a single system. We recognize that vendor costs will vary; however, our estimates in this section assume all vendors will incur the costs noted in the tables below.

2. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[425] 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 $127.82.

BILLING CODE 4150–45–P

[425] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 54. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(f)(29) ***Prescription Drug Monitoring Program (PDMP)Databases – Receive, validate, filter, and parse prescription data, support query and exchange***

Activity	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: New functional requirement – *Receive*	PDMP module must enable a user to receive electronic prescription information	0	500	(1) Lower bound assumes PDMP already has the technical capabilities to meet requirement (2) Upper bound assumes PDMP does not have the technical capabilities to meet requirement
Task 2: New functional requirement – *Validate*	PDMP must demonstrate the ability to detect valid and invalid electronic controlled substance medication prescription information received	250	500	(1) Lower bound assumes PDMP already has some of the technical capabilities to meet requirement (2) Upper bound assumes PDMP does not have the technical capabilities to meet requirement
Task 3: New functional requirement – *Parse and filter*	PDMP must enable a user to parse and filter electronic PDMP information received and validated	250	500	(1) Lower bound assumes PDMP already has some of the technical capabilities to meet requirement (2) Upper bound assumes health IT does not have the technical capabilities to meet requirement

Task 4: New functional requirement – *Exchange – response*	PDMP must be able respond to incoming patient-level queries from external system.	0	750	(1) Lower bound assumes PDMP already has the technical capabilities to meet requirement (2) Upper bound assumes PDMP does not have the technical capabilities to meet requirement
Task 5: New functional requirement – *Exchange – Patient access*	PDMP must enable patient access to view electronic controlled substance medication prescription information	500	750	(1) Lower bound assumes PDMP already has some of the technical capabilities to meet requirement (2) Upper bound assumes PDMP does not have the technical capabilities to meet requirement

Table 55. Summary of Costs for Products and Developers to Meet the Proposed Requirements in § 170.315(f)(29) [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1: New functional requirement – *Receive*	$0	$63,910
Task 2: New functional requirement – *Validate*	$31,955	$63,910
Task 3: New functional requirement – *Parse and filter*	$31,955	$63,910
Task 4: New functional requirement – *Exchange – response*	$0	$95,865
Task 5: New functional requirements – *Exchange – Patient access*	$63,910	$95,865
Total cost per product	**$127,820**	**$383,460**

Notes: Total cost per product = Labor hours x Hourly wage.

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed requirements in § 170.315(f)(29) would range from $127,820 to $383,460 per product, on average. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed requirements for Health IT Modules supporting the exchange of PDMP data will help ensure that PDMPs can receive and validate reported PDMP information and initiate and respond to queries from providers or other State PDMPs to better inform prescribing practices and monitor drug misuse and diversion. A lack of consistent interoperability requirements between PDMPs and systems involved in interstate exchange makes such queries burdensome on both the querying and responding systems. Inclusion of a certification criterion in the Program will help alleviate this burden by

supporting PDMP capabilities in alignment with requirements for health IT systems to request and validate data from PDMP databases. These new functional requirements for PDMPs will also help States conform to functionalities specified in Section 5042(a) of the SUPPORT Act to support interjurisdictional query and response, and to receive and validate data into health IT.

New Standardized API for Public Health Data Exchange

We propose a new certification criterion in § 170.315(g)(20) that would establish requirements for a standardized FHIR-based API for public health reporting. This new certification criterion would support ongoing and future development of public health FHIR IGs leveraging a core set of existing, generalizable, and extensible capabilities and standards. The new certification criterion would include FHIR capabilities proposed in § 170.315(j), which are proposed elsewhere in this rule. These certification criteria include FHIR capabilities such as FHIR Subscriptions, CDS Hooks, and SMART Health Cards, as well as requirements for authorization and authentication, among others. Our proposals in § 170.315(g)(20) would also include customized requirements for public health such as compliance with the United States Public Health Profile Library Implementation Guide (US PH Profile Library IG) and support the capability for public health query of patient-level data.

We propose that Health IT Modules certified to § 170.315(g)(20) support generalizable and extensible capabilities and standards to support a public health transition to FHIR. These foundational FHIR capabilities will support transmission of relevant data to public health entities.

Costs

These tasks to develop § 170.315(g)(20) have their own level of effort and these estimates are detailed in Tables 63 to 65 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 56 shows the estimated labor costs per product to develop § 170.315(g)(20). 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 58.

2. We estimate that 130 products certified by 112 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 130 products certified by 112 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products will certify § 170.315(g)(20) and need to meet the proposed requirements. As of the end of 2022, 29% of developers and 25% of products certified the ''standardized API criterion for patient and population services'' and one of three public health certification criteria: (1) ''immunizations''; ''syndromic surveillance''; or ''reportable labs''. Since this is a new certification criterion with novel capabilities, our estimate is based off the best proxy of what developers would certify what products to this certification criterion. We determined that the ''standardized API'' certification criterion was a close proxy to this criterion's capabilities, and we modified that proxy by a product's certification to one of the three above public health certification criteria, which are all probable use cases for public health data exchange this certification criterion is proposed to facilitate. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

Table 56. Estimated Labor Hours to Develop § 170.315(g)(20)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Support for FHIR Release 4 and US Core IG 7.0.0		0	1,000	Many developers support this capability as part of their adoption of the Standardized API for Patient and Population Services
Task 2: Support for US Public Health Library IG		200	500	IG represents about 20% more data elements than US Core IG. Minimum effort to incorporate these elements would be about 20% of the upper bound cost of implementing the US Core IG.
Task 3: Support for Bulk data export		100	600	Task assumes developers would need to support bulk export of US Core and USPHPL data elements. Lower bound assumes developer support US Core bulk data export and needs to develop support for additional USPHPL data elements
Task 4: Functional registration		0	100	Lower bound assumes underlying technology supported as part of other certified APIs
Task 5: Token introspection		0	100	
Task 6: System authentication and authorization		0	100	
Task 7: Adoption of HL7 CDS Hooks FHIR Implementation Guide version 2.0	Adoption of CDS Hooks FHIR Implementation Guide version 2.0 in	0	1,000	See Table 66 in "workflow triggers for decision support interventions"

	§ 170.215(f) as a prerequisite to facilitate API-driven CDS workflow triggers in § 170.315(j)(20)			impact analysis for more information
Task 8: Support for the "patient-view" hook	We believe that the "patient-view" hook has the highest maturity level and that implementers of CDS Hooks can consistently support this hook.	0	150	
Task 9: Adoption of Subscriptions R5 Backport Implementation Guide version 1.1.0 (Backport IG)	Requirements to include: (1) topic-based Subscription support for FHIR R4; (2) support of id-only payload notification bundles; and (3) support of the REST-hook Subscription channel	500	1500	See Table 68 in "Subscriptions" impact analysis for more information.
Task 10: Support R4/B Topic-Based Subscription Profile	Conformance to profile, support for "must support" elements, and use of canonical URL of Subscription Topic	250	500	
Task 11: Support Subscription topics	Adoption of Patient-Update and Encounter-End Subscription topics	100	200	
Task 12: FHIR server support for optional requirements	Support the creation and deletion of Subscription resources in the Capability Statement	50	100	

Table 57. Example Calculation for the Lower Bound Estimated Cost to Products to Perform Task 1 in Table 63 [2022 dollars]

Activity	Estimated labor hours	Developer salary	Projected products
	Upper bound		
Task 1	1,000	$127.82 per hour	130
Example calculation: 500 * $127.82 * 130 products = $16,616,600			

Table 58. Total Cost to Develop § 170.315(g)(20) [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (130 products)	$0	$16,616,600
Task 2 (130 products)	$3,323,320	$8,308,300
Task 3 (130 products)	$1,661,660	$9,969,960
Task 4 (130 products)	$0	$1,661,660
Task 5 (130 products)	$0	$1,661,660
Task 6 (130 products)	$0	$1,661,660
Task 7 (130 products)	$0	$16,616,600
Task 8 (130 products)	$0	$2,492,490
Task 9 (130 products)	$8,308,300	$24,924,900
Task 10 (130 products)	$4,154,150	$8,308,300
Task 11 (130 products)	$1,661,660	$3,323,320
Task 12: (130 products)	$830,830	$1,661,660
Total (130 products and 112 developers)	$19,939,920	$97,207,110

BILLING CODE 4150–45–C

The cost to a health IT developer to develop § 170.315(g)(20) for their Health IT Modules would range from $153,384 to $747,747 per product, on average. Therefore, assuming 130 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $19.9 million to $97.2 million.

Benefits

The proposed updates have a wide range of benefits for end-users of health IT (such as physicians, pharmacists, public health practitioners) and the patient populations they serve. While current standards support simple, single-patient, event-based submission of data from healthcare to public health, adopted technology does not adequately support more complex data exchange use cases, such as bulk exchange of patients who received a specific vaccine. The shift to FHIR is needed to support a wide-scale public health response and adoption of FHIR will reduce burden of implementation and maintenance for data exchange between and among health care organizations, providers, and public health agencies.

Research demonstrated that a trigger to a public health agency—in this instance, a positive lab report—could then be followed by a query back to the EHR, and data relevant to the condition were shared in an electronic case report.[426] This approach aided in more complete case reports, including demographic and clinical information, such as medications, symptoms, and diagnoses, and also resulted in only specific, relevant information being shared with the PHA.

Such an approach would allow proactive surveillance and provide public health authorities with the complete data needed to perform public health outreach and other activities. The direct access to relevant, appropriate data is possible using APIs, rather than passive, inflexible technology that sends pre-defined data sets based on a trigger, or that requires the manual intervention of a clinician. Such FHIR functions, including newer functionalities like FHIR based Subscriptions, will reduce the burden of implementation and

[426] Mishra N, Duke J, Karki S, Choi M, Riley M, Ilatovskiy AV, Gorges M, Lenert L. A Modified Public Health Automated Case Event Reporting Platform for Enhancing Electronic Laboratory Reports With Clinical Data: Design and Implementation Study. J Med internet Res. 2021 Aug 11;23(8):e26388. doi: 10.2196/26388. PMID: 34383669; PMCID: PMC8387889.

maintenance long-term, particularly for public health reporting, as the industry is able to move away from multiple, custom point-to-point connections.

While the benefits of many of these modifications are not quantifiable at this time, we expect the resulting improvements to interoperable exchange of health information to significantly benefit end users of health IT and their patient populations and improve the quality of health care provided. Health IT users will benefit from the new certified criterion through increased standardization and public health data interoperability.

14. Bulk Data Enhancements

We propose to adopt the HL7 FHIR Bulk Data Access (v2.0.0: STU 2) implementation specification (Bulk v2 IG) in § 170.215(d)(2), which would replace the current Bulk v1 implementation guide established as the standard in § 170.215(a)(3). V2.0.0 is for the most part backward compatible with v1 and builds on v1 with additional features (optional parameters including, _elements, Patient, and includeAssociatedData) and filter parameters (_since).

Through adoption of the Bulk v2 IG, we propose to require server support for the ''group-export'' ''OperationDefinition'', which enables developers engaging with § 170.315(g)(10)-certified Health IT Modules to obtain FHIR resources for a group of patients specified through various filter parameters, for testing and certification. Adoption of the ''group-export'' ''OperationDefinition'' for certification also entails adoption of the ''_since'' query parameter, which allows users to export only FHIR resources that have been modified after a specified date and was not required for client or server in v1 but is now required for server in the v2 IG.

Additionally, we propose to require server support for the ''_type'' query parameter, which allows FHIR resources for export to be filtered by resource type and is currently specified as an optional parameter for both server and client.

Costs

These tasks have their own level of effort, and these estimates are detailed in Tables 59 to 61 and are based on the following assumptions.

1. Health IT developers will use the same labor costs and data models. Table 59 shows the estimated labor costs per product to update the new FHIR Bulk Data Access implementation specification and develop server support for the _type query parameter. 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 61.

2. We estimate that 224 products certified by 182 developers will be affected by our proposal. These estimates are a subset of the total estimated number of health IT developers and certified products we estimated above.

The estimate of 224 products certified by 182 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify to the Standardized API certification criterion which adopts the bulk data technical functionality and need to meet the proposed requirements. As of the end of 2022, 43% of developers and 47% of products certified to the Standardized API certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[427] 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 $127.82.

BILLING CODE 4150–45–P

[427] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 59. Estimated Labor Hours to Implement / Meet the New Requirements in § 170.315(g)(10)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adoption of new implementation guide	Adoption of the HL7 FHIR Bulk Data Access (v2.0.0: STU 2) implementation specification (Bulk v2 IG)	0	500	We anticipate the lower bound of hours required for adoption of the new implementation guide to be 0. Through the standards version advancement process (SVAP) established by the Cures Act, developers can move to a newer implementation guide without this being required by a certification program. Therefore, nothing has prevented developers from moving to the new IG already.
Task 2: Server support for _type query parameter		150	250	

Notes: The lower and upper bound hours estimated to complete each task are estimates of labor hours required for each product.

Table 60. Example Calculation for the Lower Bound Estimated Cost to Products to Perform Task 1 in Table 24 [2022 dollars]

Activity	Estimated labor hours	Developer salary	Projected products
	Lower bound		
Task 2: Server support for _type query parameter	150	$127.82 per hour	224
Example calculation: 150 * $127.82 * 224 products = $4,294,752			

Table 61. Total Cost to Implement / Meet the New Requirements in § 170.315(g)(10) [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (224 products)	$ 0	$ 14,315,840
Task 2 (224 products)	$ 4,294,752	$ 7,157,920
Total	$ 4,294,752	$ 21,473,760

BILLING CODE 4150–45–C

The cost to a health IT developer to implement these bulk data enhancements for their Health IT Modules would range from $19,173 to $95,865 per product, on average. Therefore, assuming 224 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $4.29 million to $21.47 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The benefits of adopting support for the new standard for FHIR Bulk Data Access are difficult to quantify. We believe the adoption of the new standards in the Bulk FHIR v2 IG and server support of the optional _ type query parameter would benefit providers and patients, as well as the overall public. Bulk FHIR group export functionalities have a variety of use cases, such as, clinical research, and reporting for clinical quality measures. The group export functionality has already been successfully implemented by many organizations, including in CMS' bulk export APIs for ''data at the point of care,'' in which patients are grouped by provider and care timeframes.[428]

We believe that the standards update to the Bulk FHIR v2 IG would not place significant additional burden on developers. As noted in the proposal, new requirements in the Bulk v2 IG are increments to the v1 IG, and many are out of scope for testing and certification. Adoption of Bulk FHIR group export, including support of the _ since parameter, as well as support for the _ type query parameter is already well underway, and the _ since parameter is even better clarified in the v2 IG. In the same 2020 study, researchers surveyed various companies (including payers, EHR and cloud vendors, research organizations, and developers) implementing SMART/HL7 FHIR Bulk Data to assess the state of the API's implementation.[429] 18 of 19 survey respondents noted that they had implemented (5) or were making progress towards implementing (13) the group export functionality. 17 of 19 respondents indicated that their organization had ''implemented'' or had ''in progress'' the Bulk filter ''_ type'' parameter. Only a slightly smaller portion (16 of 19) had indicated that they had implemented or were in progress of implementing the Bulk filter ''_ since'' parameter. As of 2020 Q2, organizations were already making substantial progress towards adoption, so these additional requirements for certification and testing are not expected to be unusually burdensome. Further, as mentioned in the proposal, by Spring 2023, 73.7% of certified Bulk FHIR modules supported the optional _ type parameter.

Within the same study, survey respondents were asked to indicate hurdles to Bulk FHIR implementation. Major concerns expressed included processing time for data export, choosing breakpoints to divide large data files, granular access to specified FHIR resources, and opportunities for reducing the costs to host data. We believe that these concerns are addressed in the contents of this proposal.

The primary additional functionality offered through server support for the ''group-export'' ''OperationDefinition'' is filtering by date with the ''_ since'' parameter. The _ since parameter is expected to produce efficiency in applications in the context of the previously mentioned use cases, as it

[428] *https://link-springer-com.ezproxyhhs.nihlibrary.nih.gov/chapter/10.1007/978-3-030-91563-6_10.*

[429] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8661398/.*

will allow for incremental data export, reductions in the amount of data transferred, and prevention of duplication of data transferred. As data are updated, FHIR resources modified within a particular timeframe can be exported, preventing the need to repeatedly export a full dataset when data is being followed and repeatedly shared over time. In addition to preventing the recipient of the data from needing to spend valuable time resources sifting through data to identify data of particular interest (based on the specified timeframe) and delete duplicate data that may have already been received through a previous export, limitations on the amount of data exported through use of the _ since parameter can prevent exports from taking up valuable storage on a user's machine when unnecessary data is otherwise included. We expect the same benefit from adoption of the _ type parameter.

Furthermore, we believe our proposals offer opportunities for increased efficiency in these spaces, specifically in contexts where Bulk FHIR group export functionalities are used. Use of the _ since and _ type parameters for group export of FHIR resources is anticipated to lead to improvements in API performance because it allows for a more specified group of resources to be exported, thus limiting the time required for export and improving efficiency. Server support of the _ type parameter for querying in preparation for group export is further expected to have benefits for privacy and security, as specifying FHIR resource types for export limits the risk of exporting sensitive or confidential data, thereby preventing inadvertent harm to patients through exposure of private data. Therefore, these proposals pose an opportunity to address needs indicated in the aforementioned survey.

The group export requirement is anticipated to meet existing needs across Bulk FHIR use cases with respect to limiting the quantity of data exported through additional specification. In one study assessing the feasibility of using of Bulk FHIR queries to get COVID–19 vaccination registry information to public health workers performing patient follow-up after vaccines and to schedule vaccination appointments, the researchers found that the specifications in the current Bulk FHIR standard for patient data export was clunky and not scalable for public health purposes, which in the context of using data to facilitate response to the COVID–19 pandemic would have typically required the export of records for thousands of individuals.[430] Because of this, these researchers found the need to utilize an optional group extension that allowed the specification of particular patient groups for data export. This demonstrates a use case with a practical need for expansion of the standard through adoption of the Bulk v2 IG, and therefore also server support for the ''group-export'' ''OperationDefinition''.

15. New Requirements To Support Dynamic Client Registration Protocol in the Program

We propose to revise the application programming interface (API) certification criterion in § 170.315(g)(10) and the API Conditions and Maintenance of Certification requirements in § 170.404 by adding requirements to support dynamic client registration for patient-facing applications. We propose to adopt several specific sections of the HL7 UDAP Security for Scalable Registration, Authentication, and Authorization 1.0.0 implementation guide to support these revisions to § 170.315(g)(10) and corresponding API Conditions and Maintenance of Certification requirements. This proposal would facilitate an individual's timely access to their health information using an application of their choice by providing a more uniform, standardized, and automated registration pathway for patient-facing applications.

[430] *https://academic.oup.com/jamia/article/30/3/551/6874797.*

Costs

This section describes the estimated costs of meeting requirements in the proposed revisions to § 170.315(g)(10), which are detailed in Tables 62 and 63 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 62 shows the estimated labor costs per product to make the proposed updates in § 170.315(g)(10). 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 63.

2. We estimate that 224 products certified by 182 developers will be affected by our proposal. These estimates are a subset of the total estimated number of health IT developers and certified products we estimated above. The estimate of 224 products certified by 182 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify to § 170.315(g)(10) certification criterion and need to meet the proposed requirements. As of the end of 2022, 47% of developers and 43% of products certified to § 170.315(g)(10) certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91.[431] 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 $127.82.

BILLING CODE 4150–45–P

[431] *https://www.bls.gov/oes/current/oes151252.htm.*

Table 62. Estimated Labor Hours to Meet the Proposed Requirements

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adopt four sections of the HL7 UDAP Security IG v1 for dynamic registration for patient-facing applications	New registration server development (or updates to existing server) to support dynamic client registration	640	800	(1) Lower bound assumes that the developer is making updates to existing server to support dynamic client registration (2) Upper bound assumes new registration server development to support dynamic client registration
Task 2: Support for capabilities and features for the authorization and patient authentication requirements to accommodate dynamically registered apps		250	500	(1) Lower bound estimates hours to keep it running with junior staff. (2) Upper bound estimates small updates.
Task 3: Publication of trust community information and (optional) authenticity verification	New API Maintenance of Certification requirements	20	40	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

Table 63. Total Cost to for Products and Developers to Meet the Proposed Requirements [2022 dollars]

Activity	Estimated Number of Products	Estimated Cost	
		Lower bound	Upper bound
Task 1: Adopt four sections of the HL7 UDAP Security IG v1 for dynamic registration for patient-facing applications	224	$18,324,275	$22,905,344
Task 2: Support for capabilities and features for the authorization and patient authentication requirements to accommodate dynamically registered apps	224	$7,157,920	$14,315,840
Task 3: Publication of trust community information and (optional) authenticity verification	224	$572,634	$1,145,267
Total cost for all products (224 products)	**224**	**$26,054,829**	**$38,366,451**

Notes: We used a 48% modifier for the § 170.315(g)(10) certification criterion to estimate the number of products impacted by the Dynamic Client Registration Protocol updates. Estimates reflect the percent of all products that certify to the § 170.315(g)(10) certification criterion through 2022. This estimate is subject to change.

BILLING CODE 4150–45–C

In addition to the estimated costs, we believe this proposal would create cost savings for certified API developers. API developers currently support a manual app registration process where they must review and confirm all registrations individually. The proposed dynamic registration process would replace a manual verification of each app developer by the certified API developers with a trust framework wherein an app developer with a certification for a given trust framework would be granted automatic registration. The proposed process would reduce burden on certified API developers to verify all registrations individually. Table 64 shows the projected cost savings over a 10-year period to all certified API developers.

We estimate that on average, there would be 50 app registrations per certified product per year. This estimate is based on a study of public app galleries and the number of new apps, on average, that are available to EHR users each year.[432] Because this average is based on public marketing of apps approved for display by EHR vendors, it may underestimate the true number of apps that register, but do not go into production each year. The average may also be overestimated, because it's based on app integrations for market leading EHR vendors and may not be representative of app registrations for smaller EHR vendors. We request comment on this measurement approach and accuracy of the number of app registrations a developer of certified health IT must verify annually.

[432] Barker W., Johnson C., The ecosystem of apps and software integrated with certified health information technology.Journal of the American Medical Informatics Association 28(11), 2021, 1–6.

Table 64. Total Cost Savings for Products and Developers to Meet the Proposed Requirements in § 170.315(g)(10) [2022 dollars]

	App Registrations per Developer	Estimated Cost Savings	
		Lower bound	Upper bound
Time required to approve registrations for each app (hour)		$59.22* (1 hour)	$118.44* (2 hours)
Total estimated cost savings (224 products)	50	$663,264	$1,326,528
Total estimated cost savings (10-year time horizon)	**500**	**$6,632,640**	**$13,265,280**

Note: *Labor category = computer user support specialist (https://www.bls.gov/oes/current/oes151232.htm) + overhead.

The cost to a health IT developer to meet the proposed requirements would range from $116,316 to $171,279 per product, on average. Assuming 224 products overall and a labor rate of $127.82 per hour, we estimate that the total cost for all products would, on average, range from $26 to $38.3 million. The cost savings to a health IT developer to meet the proposed requirements would range from $29,610 to $59,220 per product, on average, over a 10-year time horizon. Assuming 224 products overall and a labor rate of $59.22 per hour, we estimate that the cost savings for all products would, on average, range from $6.6 to $13.3 million, over a 10-year time horizon, resulting in an overall net cost to health IT developers of $19.4 to $25.1 million.

Benefits

We believe this proposal would benefit health care developers and the health IT industry. The proposed updates would streamline the currently manual and non-standardized process for application registration for the § 170.315(g)(10) certification criterion for patient-facing apps. The current manual process creates administrative burden and is difficult to scale when registering for more than one endpoint. With dynamic registration, applications can obtain a certificate that can then be used across all endpoints that support that certificate, taking the industry one step closer to the goal of APIs being usable ''without special effort'' under the Cures Act.

We believe this proposal would create financial benefits to app developers. Current app registration processes are manual, requiring app developers to complete their registration and wait for the certified API developer or API information source to manually verify and approve their registration. The actual process of verification and approval may take minutes, but the wait and backlog of registrations may create undue burden for app developers to successfully register their app to begin testing and development using the EHR's APIs. The proposed registration process, as we detail in the cost savings estimated for certified API developers, reduces this time and automates the registration process with immediate verification. App developers would see direct benefits from this new registration process through time savings due to decreased wait times and uncertainty about verification timelines. Table 65 below shows the estimated benefits for app developers realized from the new proposed registration process.

Table 65. Benefits to App Developers from Proposed Dynamic Client Registration Process in § 170.315(g)(10) [2022 dollars]

		Time required to register for each endpoint (hour)		Total estimated cost per app developer		Total estimated cost for 50 apps per year for 8 years	
Estimated number of endpoints	Hourly wage*	Lower bound	Upper bound	Lower bound	Upper bound	Lower bound	Upper bound
20,000	$59.22	0.25	0.5	$296,100	$592,200	$118,440,000	$236,880,000

Note: *Labor category = computer user support specialist (https://www.bls.gov/oes/current/oes151232.htm) + overhead.

The estimated quantified benefits assume several factors: (1) app registrations may need to be completed for all distinct FHIR electronic endpoints; (2) a computer user support specialist would be needed to complete the process; and (3) benefits will begin to accrue in the third year after this rulemaking is finalized. The estimated

number of endpoints per developer was calculated using public data available through the ONC FHIR API Monitoring System or ''Lantern''.[433] The data are as of the end of 2023 and represent all endpoints available from certified API developers (n = 224). The endpoints were tested by the Lantern system to ensure they were accessible when randomly queried and a conformant FHIR Capability Statement was fetched upon a successful query of the endpoint. We request comment on whether endpoints represent the best proxy for volume of app registrations and if the proposed endpoint calculation is sound. We estimate that the average time for an app developer to register for each endpoint would take from 15 to 30 minutes. We then multiplied the effort for one app developer to register their app for all endpoints by the average number of app registrations per developer per year estimated in Table 64 for 8 years (the number of years after the proposed registration requirements would be implemented by certified API developers.) We estimate financial benefits from $118.4 million to $236.9 million for app developers in the form of time savings and other reduced costs associated with the effort of manual registration to electronic endpoints. We request comment on this proposed approach and, specifically, request comment on the approximate time to complete the registration process.

16. New Certification Criteria for Modular API Capabilities

We propose to include 14 new certification criteria as modular API capabilities in § 170.315(j). These new certification criteria would be available for certification based on certain contexts or other programs requiring the use of the specified certified capabilities. The first eight of these certification criteria are substantially similar to capabilities currently referenced in § 170.315(g)(10)(iii) through (vii) and the three remaining certification criteria are new to the Program.

- § 170.315(j)(1): Functional registration
- § 170.315(j)(2): Dynamic registration
- § 170.315(j)(5): Asymmetric certificate-based authentication for patient access
- § 170.315(j)(6): SMART app launch user authorization
- § 170.315(j)(7): SMART backend services system authentication and authorization
- § 170.315(j)(8): Asymmetric certificate-based system authentication and authorization
- § 170.315(j)(9): SMART patient access for standalone apps
- § 170.315(j)(10): SMART clinician access for EHR launch
- § 170.315(j)(11): Asymmetric certificate-based authentication for B2B user access
- § 170.315(j)(20) and § 170.315(j)(21): Workflow triggers for decision support interventions
- § 170.315(j)(22): Verifiable health records
- § 170.315(j)(23) and § 170.315(j)(24): Subscriptions

The proposed new certification criteria create flexibility to test and certify Health IT Modules and introduce new technical functionalities with synergy with other certification criteria proposed in this rulemaking and already adopted by the Program. For certification criteria § 170.315(j)(1) to (j)(7), these new certification criteria do not increase the level of burden on developers to adopt. Sections 170.315(j)(1) and 170.315(j)(3) to (j)(7) are currently adopted as part of the § 170.315(g)(10) certification criterion and we assume no additional development burden (beyond what has been estimated as part of prior rulemaking where these functionalities were originally adopted and finalized) to adopt these capabilities in this new modular manner. The proposal for ''Dynamic Client Registration'' would be adopted as part of proposed certification criterion § 170.315(j)(2). This proposal is discussed elsewhere in this regulatory impact analysis. We also request comment on a proposed update to functionalities currently adopted as part of the (g)(10) certification criterion and are proposed to be adopted as individual (j) certification criteria, as discussed above. We propose to update the token revocation policy (as adopted in § 170.315(j)(7): User authorization and (g)(10)) to require authorization revocation for users generally (to include users such as clinicians generally as opposed to only patients.) We request on whether this broader revocation policy will require additional effort to implement, as the underlying functionality to enable it for patients should be very similar for users generally. We believe implementing this update should require de minimis effort and appreciate public comment.

Certification criteria § 170.315(j)(20) to (j)(24) propose new technical functionalities. However, this proposed rulemaking does not require adoption of these new certification criteria, specifically. The certification criteria are referenced as conditional or as required functionality for other proposed certification criteria. The impact analyses, below, for these three proposed certification criteria assess the expected level of effort and development tasks required to adopt the new certification criteria, but do not assume required adoption for these certification criteria for any current developers of certified health IT. Where necessary, we reference these development tasks and burden in the related impact analyses of other proposed certification criteria that adopt these new certification criteria and their technical functionalities as necessary functionality to meet their distinct certification requirements.

Workflow Triggers for Decision Support Interventions

We propose to adopt HL7 Clinical Decision Support (CDS) Hooks FHIR Implementation Guide version 2.0 in § 170.215(f) as a mandatory compliance prerequisite to facilitate API-driven workflow triggers for decision support interventions in § 170.315(j)(20) and § 170.315(j)(21). This requirement would establish adoption of a ''hook''-based pattern for initiating clinical decision support, either allowing decision support results to be integrated seamlessly into a provider's EHR workflow or launching an interactive CDS application from within the workflow.

We additionally propose the integration of standards-based interfaces into § 170.315(j)(20), including the requirement for § 170.315(j)(20)-certified Health IT Modules to support the ''patient-view'' hook per the standard specified in § 170.215(f). The patient-view hook enables clinicians to retrieve data for individual patients (*e.g.,* demographics, medical history, pertinent clinical information) as a means of accessing decision support that is customized to an individual patient and more contextually relevant.

Costs

These tasks have their own level of effort, and these estimates are detailed in Table 66 below.

[433] *https://github.com/onc-healthit/onc-open-data/tree/main/lantern-daily-data.*

Table 66. Estimated Labor Hours to Develop Workflow Triggers for Decision Support Interventions § 170.315(j)(20) and § 170.315(j)(21)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adoption of HL7 CDS Hooks FHIR Implementation Guide version 2.0	Adoption of CDS Hooks FHIR Implementation Guide version 2.0 in § 170.215(f) as a prerequisite to facilitate API-driven CDS workflow triggers in § 170.315(j)(20)	0	1,000	First balloted 5 years ago, CDS Hooks is mature but still in trial use. We propose a minimal implementation of the standard and believe this implementation is likely supported and deployed by some developers, but not all in some fashion.
Task 2: Support for the "patient-view" hook	We believe that the "patient-view" hook has the highest maturity level and that implementers of CDS Hooks can consistently support this hook.	0	150	The "patient-view" hook is FHIR maturity model level 5 and has been implemented by several different systems.

Notes: The lower and upper bound hours estimated to complete each task are estimates of labor hours required for each product.

These proposals may also impose some costs and challenges that are not easily quantifiable. While some scholars posit that CDS Hooks are in a state of relative immaturity compared to other HL7 standards, their growing popularity suggests further standards development for CDS Hooks is likely on the horizon. Part of the developing maturity level comes from exploration of new hook definitions for workflow trigger points, security best practices, response analytics, and suggestions for improved interoperability for items like recommended prescriptions.[434] Based on public feedback on ONC's request for information in the HTI–1 Proposed Rule, some commenters expressed concerns for slow real-world adoption of CDS Hooks. Although CDS Hooks is reasonably mature, many developers and other organizations are not using this technology. One review of ''original studies describing development of specific CDS tools or infrastructures'' using FHIR, SMART, CQL, and CDS Hooks published in 2021 found that only 18% used CDS Hooks. These authors note that CDS Hooks are too early in their life cycles to determine their uptake based on the limited number of studies on them.[435]

Considering this, many commenters were partial to certification requirement rollout for specific use cases, such as prior authorization, immunization decision support, evidenced-based treatment decisions and alternatives, etc. Notably, prior authorization was indicated to be a high priority use case. Furthermore, one market leading EHR developer indicated in RFI comments that it does not believe certification of CDS Hooks is necessary to materially advance interoperability and supports allowing market forces to drive adoption. The developer noted they make CDS Hooks available but is utilized by only about 10% of end users, potentially due to its effect of slowing clinician workflows.

There are examples of successful implementations of CDS Hooks, but these implementations are not without challenges. In one study by Dolin et al., the researchers developed a pharmacogenomics CDS service prototype based on the FHIR and CDS Hooks standards.[436] The researchers noted that they were able to meet their goals of deploying a functional prototype but identified some challenges with CDS Hooks. They found that the process for executing an authenticated query request in a system outside of the EHR from a trigger within

[434] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8324242/.*

[435] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8416232/.*

[436] *https://pubmed.ncbi.nlm.nih.gov/30605914/.*

the EHR was very complex and noted constraints on the variety of actionable CDS recommendation types that could be returned from the decision support tool.

One randomized control trial assessed the cost of using CDS Hooks to clinician end users. CDS Hooks was shown to be more burdensome to end-users, requiring many clicks and a greater level of effort than other EHR prompts. Based on a cluster RCT in an emergency department using Epic, single-click prompts like ordering HIV screening laboratory tests take less effort and clicks than CDS Hooks. Single-click app launching occurs with some CDS Hooks; for example, the Epic EHR uses CDS Hooks for pop-up alerts. However, single-click launching does not happen for all Epic prompts, including Storyboard prompts (patient summaries that are always displayed in the EHR for an individual patient). Instead of a single click, the user must click on the Storyboard prompt and then eventually access the hyperlink to the hook. Accessing the hyperlink is nonintuitive to most users, which is why the researchers in this study requested Epic to have a single-click for CDS Hooks in the Storyboard prompt.[437] These challenges faced by end-users suggest that there may be room for growth in CDS Hooks implementations.

Benefits

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit clinician end users and improve the quality of health care provided. Clinicians will benefit from the updates to the standard and to the certified criterion through increased standardization and interoperability of CDS Hooks technology. Certified use of CDS Hooks is expected to facilitate more patient-specific results from clinical decision support tools, assisting providers in a more patient-centric approach to care. Further, we believe that the ''patient-view'' hook proposed to be required for modular certification is the most mature, as supported by public comment, and that current implementers of CDS Hooks will be able to implement this with limited additional challenge.

Based on public feedback on ONC's request for information in the HTI–1 Proposed Rule, commenters were generally more supportive of certification criteria for adoption of the v2.0 specification of FHIR CDS Hooks, as opposed to v1.0. Many also preferred ONC supporting narrow certification criteria related to a particular user guide, as we have specified in this proposal. Specifically, we propose to require just the ''patient-view'' hook for modular certification. We believe the nature of our proposal addresses some of these concerns. Further, the ''patient-view'' hook was among the hooks recommended by commenters to use as part of the certification requirements. Given commenter concerns for use-case specific guidance, we propose support for the ''patient-view'' hook, specifically, given its broad applicability across use cases. We expect the ability to acquire modular certification per in § 170.315(j)(20) through the ''patient-view'' hook because it is use-case agnostic.

Although many argue that adoption is growing slowly for CDS Hooks, based on comments received as part of the HTI–1 Proposed Rule RFI, one commenter expressed their support for modular certification of this technology, noting the belief that it is significantly developed and mature, as well as citing the fact that the CMS Interoperability and Prior Authorization Proposed Rule is dependent on this technology (a large-scale implementation example).

Based on public feedback on ONC's request for information in the HTI–1 Proposed Rule, commenters were generally supportive of the utility of CDS Hooks and believed the specification to be mature. Based on the literature, use of CDS Hooks appears to offer utility to patients and providers. In a randomized control trial of CDS Hooks' feasibility to increase use of SMART on FHIR apps, researchers found that CDS Hooks may lead to reduction in usability issues with SMART on FHIR apps.[438] This would likely create better access to clinical care recommendations on its own, in addition to more complex decision logic due to the use of an external CDS engine through CDS Hooks services that could then be implemented using native EHR CDS approaches. These improvements in CDS could subsequently improve care decisions and patient outcomes. Another likely benefit of CDS Hooks is time savings from interoperability because (similar to SMART on FHIR apps), CDS Hooks can be shared across EHR platforms and health systems.

Beyond the opportunity for clinical decision support tools to facilitate reduced cognitive load and timesaving for providers, another anticipated benefit of CDS Hooks is that it gives clinicians using CDS tools the option to utilize these tools only when needed.[439] Relatedly, use of CDS Hooks allows decision support results to be accessed at any time during a patient's care, and not only when the results of an ordered lab are received. This is expected to benefit patients by reducing the risk of adverse health events and preventing duplication of lab tests. Due to resulting increases in care efficiency, this is also expected to lead to notable cost-savings for health systems utilizing the CDS Hooks tool.

In one RCT trial, researchers aimed to assess the feasibility of using CDS Hooks to increase SMART on FHIR app utilization. The researchers found that, since the same logic is used for CDS Hooks and SMART on FHIR apps, developer burden can be reduced because CDS Hooks use FHIR as their data model and exchange standard like SMART on FHIR. Morgan et al., advise that to justify the significant time and resources EHR developers must invest in building the hook, development should focus on single-click prompts where the end-user burden is most likely to benefit (however, developer effort is not quantified in this RCT).[440] CDS Hooks largely addresses this concern, as it uses a hyperlink to SMART on FHIR app that allows users to launch the app in a single click.[441]

Verifiable Health Records

We propose in § 170.315(j)(22) that Health IT Modules demonstrate support for creating verifiable SMART Health Cards per the standard in § 170.215(g) and that records are made available to users through these cards. SMART cards allow patients to carry verifiable, portable healthcare data that can easily be shared with a provider via QR code. SMART cards are a form of patient-held records intended to advance interoperability and improve patients' ability to share their healthcare data for treatment in light of challenges with provider-to-provider data exchange.

Costs

From a development perspective, costs are anticipated to be minimized, as code necessary to implement the technology is based on open standards, and components are substitutable. However, these tasks have their own level of effort, and these estimates are detailed in Table 67 below:

[437] Ibid.

[438] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9382378/.*

[439] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7233102/.*

[440] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9382378/.*

[441] Ibid.

Table 67. Estimated Labor Hours to Develop Verifiable Health Records § 170.315(j)(22)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adopt SMART Health Cards standard and make verifiable records available to users	Health IT Module should show support for creating verifiable health records according to the § 170.215(g) SMART Health Card Standard	0	500	We assume some developers have already adopted this standard and made verifiable records available to users through their participation in VCI (https://vci.org/about) and other related efforts. VCI participating organizations and members include current developers of certified health IT. Our proposal for verifiable health records does not exceed these prior implementations of the standard and its use.

Notes: These labor hours are estimated specifically for products certified through f1 certification criteria but not through g10 certification criteria. Hours reflect anticipated labor required per individual product.

The cost to adopt the SMART Health Cards standard and make verifiable records available to users is difficult to estimate given the current state of SMART Health Card implementations. Beyond the cost of development, some additional concerns with certification have been expressed by major Health IT developers and policy organizations. The public was asked to provide comment on ONC's ''SMART Health Links Request for Information'' in the HTI–1 Proposed Rule, and several major developers and EHR companies responded with their feedback. Many commenters indicated that they were supportive of the advancement of SMART Health Cards but not of related certification, citing the current lack of maturity of the technology as well as the lack of necessity for certification in high-value use cases, noting that the market should be left to fuel the demand for this technology. One market leading EHR expressed its opposition to certification of SMART Health Cards due to a perceived lack of standards maturity, need for a clear use case, and need for greater adoption by patients. One commenter highlighted that the focus needs to first be on defining use cases of this technology; importantly, there are no known implementations of SMART Health Cards beyond the public health (particularly, the COVID–19 pandemic) use case. One market leading EHR expressed additional concerns about certification of SMART Health Cards in the context of an unfolding landscape in which privacy concerns that must be considered may not yet be identifiable, noting that ''ensuring trusted and secure links to such cards raises challenges that need to be fully addressed to ensure appropriately authorized users to access the highly sensitive PHI.'' In general, commenters had interest in this technology and its uses being better defined before moving towards certification. To summarize, companies expressed concerns about rushing into certification of SMART Health Cards when use cases still need to be defined, and thus demand is not present, and given unidentified security concerns that might be exposed with more adoption fueled naturally by market demand.

We anticipate some additional challenges in adopting this technology that were not included in the comments

discussed above.[442] Tradeoffs exist between privacy and the strength of identity binding for SMART Health Cards technology, so developers may face challenges ensuring the safety of individuals' health information while binding cards to a real-world identity. SMART Health Cards also rely on the establishment of ''trust frameworks'' so that clinicians who are presented a QR code with patient data can verify that this record is from a trustworthy source. This may be difficult in the future as multiple frameworks with differing goals launch.

Benefits

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit providers and patients and improve the quality of health care provided. Providers and patients will benefit from the updates to the standard and to the certified criterion through increased standardization and interoperability of patient health data through a verifiable form of patient-held records.

During the COVID–19 pandemic, 12 IT companies (led by Microsoft and Oracle) came together to form the Vaccination Credential Initiative (VCI), which used the SMART Health Cards specification to allow patients to hold verifiable COVID–19 vaccination records or ''passports.'' [443] Of note, a few of the companies and organizations that provided comment to the request for information in ONC's HTI–1 Proposed Rule were involved in this effort. Likely due to the recency of the COVID–19 pandemic and the kick-off of such efforts, there is little in the literature that assesses the performance of these verifiable records. However, the vaccine passports are thought to have created a sense of validity of COVID–19 vaccine records at a time when many paper records were being falsified.

Because of the low levels of current adoption of SMART Health Cards in use cases beyond the COVID–19 public health emergency, tangible improvements in health outcomes due to the use of SMART Health Cards (if any exist) are unknown. However, we anticipate many benefits from the adoption and certification of this technology. First, SMART Health Cards offer an opportunity to engage patients in the self-management of their own health data, which is expected to lead to improved outcomes due to the resulting improvements in patient-provider communication and availability of verifiable patient-held records. This may particularly benefit patients with serious chronic conditions, as these individuals may be more likely to adopt personal use of patient-held records, such as SMART Health Cards.[444] Despite ONC's ongoing efforts for and clear improvements with respect to interoperability in the healthcare sector, we acknowledge that interoperable exchange of healthcare data is not perfect, and providers generally do not have all of a patient's diagnostic and treatment history. Use of patient-held health records (of which SMART Health Cards are an example) prevents information asymmetry with provider and improved communication with provider as a result, which we expect to enable providers to make more informed and effective treatment decisions.[445] Patient engagement has improved with improvements in Health IT, and we expect the adoption of SMART Health Cards (a technology that fosters patient engagement by placing control over records sharing into the hands of the patient) to lead to improved patient outcomes.[446] One systematic review of the impact of Health IT on ''patient engagement and behavior change'' published in 2016 found encouraging results. Assessing 170 studies in total, the researchers found that 4 in 5 showed improved patient engagement and nearly 9 in 10 found improvements in patient behavior due to continuing advancements in health information technology.[447] When additional technologies are provided that allow patients to become more engaged, patients may be more invested in better personal health-decision making.

Patient control over their data sharing through adoption of SMART Health Cards technology offers further opportunities to respect patient preferences in the sharing of sensitive information by preventing the over-sharing of data. Based on a recent Pew study involving focus groups of patients, individuals are interested in most of their health information being shareable between providers but are less comfortable of more sensitive data being shared (*e.g.* data points relating to substance misuse, behavioral and mental health, and social needs).[448] Some participants expressed concern that stigmatizing information may fuel discrimination, which is expected to negatively affect care outcomes and patient comfort with seeking care. SMART Health Cards offer patients the opportunity to share verifiable records with their providers very easily but also preserves the element of choice, thus respecting patient preferences in the continuity of their care and offering opportunities to prevent the sharing of data that is deemed irrelevant for care.

Subscriptions

We propose that Health IT Modules certified to § 170.315(j)(23) and § 170.315(j)(24) demonstrate support for FHIR-based API subscriptions according to the HL7 FHIR Subscriptions Framework. We specifically propose the adoption of the Subscriptions R5 Backport Implementation Guide version 1.1.0 (Backport IG) in § 170.215(h)(1) as a baseline standard conformance requirement in § 170.315(j)(23) and § 170.315(j)(24). FHIR Subscriptions allow a server to notify a user when information has been added or altered within a record, as well as offers the ability to submit a payload with a notification. We further propose the following requirements for certification of a Health IT Module in § 170.315(j)(23) and § 170.315(j)(24):

1. Conformance to the ''R4/B Topic-Based Subscription'' profile detailed in the as specified in the Backport IG. This includes the need to demonstrate support for ''must support'' elements.

2. Adoption of both the Patient-Update and Encounter-Create Subscription topics as minimum requirements for server support.

3. Conformance to the R4 ''Server CapabilityStatement'' included in the Backport IG.

a. Server support of create, update and delete interactions for Subscription resources (create and delete are currently optional).

4. Server support of id-only payload notification bundles.

5. At a minimum, support of the REST-hook Subscription channel as a means of notifying subscribers of the availability of new results.

Costs

These tasks have their own level of effort, and these estimates are detailed in Table 68 below:

[442] *https://docs.google.com/presentation/d/1Ib8lxZWgJ8IIq7NEzbV4_R5s1nRD3pEv/present?slide=id.p5.*

[443] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9759417/.*

[444] *https://academic.oup.com/jamia/article/18/4/515/736676.*

[445] *https://www-sciencedirect-com.ezproxyhhs.nihlibrary.nih.gov/science/article/pii/S0738399103001848#aep-section-id31.*

[446] *https://medinform.jmir.org/2016/1/e1/.*

[447] *https://medinform.jmir.org/2016/1/e1/.*

[448] *https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2020/03/patients-seek-better-exchange-of-health-data-among-their-care-providers.*

Table 68. Estimated Labor Hours to Develop Subscriptions § 170.315(j)(23) and § 170.315(j)(24)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adoption of Subscriptions R5 Backport Implementation Guide version 1.1.0 (Backport IG)	Requirements to include: (1) topic-based Subscription support for FHIR R4; (2) support of id-only payload notification bundles; and (3) support of the REST-hook Subscription channel	500	1500	
Task 2: Support R4/B Topic-Based Subscription Profile	Conformance to profile, support for "must support" elements, and use of canonical URL of Subscription Topic	250	500	
Task 3: Support Subscription topics	Adoption of Patient-Update and Encounter-Create Subscription topics	100	200	
Task 4: FHIR server support for optional requirements	Support the creation and deletion of Subscription resources in the Capability Statement	50	100	

Notes: The lower and upper bound hours estimated to complete each task are estimates of labor hours required for each product.

We acknowledge that these costs may be difficult to estimate given the current state of FHIR Subscription implementations ONC requested public comment in a ''FHIR Subscriptions Request for Information'' in the HTI–1 Rule proposal, and some commenters expressed concern for cost. One commenter specifically indicated a concern for costs to implement and a need for more information on relevant use cases, given a current lack of real-world implementations of FHIR Subscriptions according to the specifications in the R5 Backport IG. Further, we do not know the extent to which costs and benefits may balance one another. Subscriptions are intended to provide active event notifications to users immediately when data in a record is updated or changed.[449] However, academic literature on this topic does not currently reflect concrete benefits of this notification service. We request comment on these cost estimates, in particular the burden hours and necessary tasks to develop this functionality.

[449] *https://build.fhir.org/ig/HL7/fhir-subscription-backport-ig/.*

Benefits

The benefits of these modifications are not quantifiable at this time, but we expect the resulting improvements to interoperable exchange of health information to significantly benefit patients, providers, and health care workers and improve the quality of health care provided. Currently, patient access and decision support applications need to periodically poll § 170.315(g)(10)-certified APIs to check for updates to patient records. Using the HL7 FHIR Subscriptions Framework, these apps can receive notifications when relevant updates are available.

This means that patient apps and decision support apps can have more timely, real-time access to the latest records, ensuring that they always have the most up-to-date information. The current API polling model requires applications to make requests to the server, even when there are no updates available. This can result in unnecessary network traffic and resource utilization. Using HL7 FHIR Subscriptions, applications receive notifications when updates are available, and can use these notifications to make server queries to receive patient record updates, reducing the overall network traffic and resource usage. Provider applications can similarly benefit by receiving real-time notifications to update decision support modules and other supporting services.

Public health reporting can also be supported with the HL7 FHIR Subscriptions Framework. Currently, implementers seeking to support projects like electronic case reporting must configure one-off solutions to support case report triggers in their EHR systems. While the triggering criteria can be standards-based using value sets like the electronic case reporting Reportable Conditions Trigger Code, the process for sending notifications currently relies on non-standardized or manual solutions. Support for the HL7 FHIR Subscriptions Framework will enable systems to readily support a variety of standards-based public health reporting and will provide the baseline functionality required for future public health implementation guides to be developed that will help ensure that vital public health information is timely and available when needed. Additionally, since the HL7 FHIR Subscriptions Framework is based in HL7 FHIR, the servers and applications are able to use a standardized language to communicate the criteria used for triggering subscription notifications.

FHIR Subscriptions have a maturity level of 3 (on a 5-point Likert scale) and is currently in Trial Use. Although it's been deemed ready for use in production systems, it has not seen widespread use in production.[450] According to the HL7 website, this would mean that the ''FMM2 + the artifact has been verified by the work group as meeting the Conformance Resource Quality Guidelines; has been subject to a round of formal balloting; and has at least 10 distinct implementer comments recorded in the tracker drawn from at least 3 organizations resulting in at least one substantive change.'' [451] HL7's website further states that subscribers (in this case, developers) typically would not need to implement many channel types, so it is unlikely that these developers would spend a significant portion of time with trial and error.[452] We specifically propose to require support only for the REST-hook channel for modular certification in § 170.315(j)(22). We note in the proposal that this channel uses the RESTful model, is used extensively in the FHIR standard, and is considered the lowest bar for implementation. Given these points, we believe the burden to developers who wish to achieve modular certification in § 170.315(j)(22) to be minimized. As a note, no academic literature has been found that assesses end-user burden of event notifications/Subscriptions R5 Backport IG.

Although the literature does not highlight clear, quantifiable benefits of FHIR Subscription services, we anticipate FHIR Subscriptions to ease interorganizational transactions through the functionality to transmit a payload along with a notification, as well as to reduce the burden of reporting across several public health use cases. Subscriptions are expected to be relevant in clinical, public health, administrative, and research use cases, and we believe Subscriptions will play a role in automating case and health care survey reporting in these contexts, thus reducing provider burden.

The public was asked to provide comments on ONC's FHIR subscriptions request for information in the HTI–1 rule proposal, and responses were considered in the development of proposals pertaining to FHIR subscriptions in HTI–2. Commenters generally noted that the FHIR version R5 Backport IG as a better option for implementation guidance than the R4B IG. Feedback received also included recommendations to start with small defined use cases and a subset of topics thought to be most beneficial. We have specifically proposed support for two Subscription topics—Patient-Update and Encounter-Create, which can be implemented easily through canonical URLs. Our proposals align with these recommendations to begin with a simplified and clearly specified approach to adoption required for modular certification.

17. Multi-Factor Authentication Certification Criterion

ONC proposes to revise the ''multi-factor authentication'' (MFA) certification criterion in § 170.315(d)(13) and accordingly update the privacy and security (P&S) certification framework in § 170.550(h). The proposed update would revise our MFA certification criterion by replacing our current ''yes'' or ''no'' attestation requirement with a specific requirement to support multi-factor authentication and configuration for three certification criteria: ''view, download, transmit to 3rd party'' (§ 170.315(e)(1)); ''standardized API for patient and population services'' (§ 170.315(g)(10)) (for ''patient facing'' access); and ''electronic prescribing'' (§ 170.315(b)(3)). We believe these updates match industry best practices for information security, particularly for important authentication use cases in health IT. Finally, we propose to remove references to § 170.315(d)(13) in § 170.550(h)(3) for all certification criteria except for § 170.315(e)(1), (g)(10), and (b)(3).

Costs

The currently adopted MFA certification criterion instructs developers to attest ''yes'' or ''no'' that they support multi-factor authentication. An analysis of the Certified Health IT Product List (CHPL), as of the end of 2022, shows that 43% of developers (comprising 44% of products required to comply with the certification criterion) attested ''yes'' that they support multi-factor authentication. These results do not confirm our priors, when ONC finalized the ONC Cures Act Final Rule, that most, if not nearly all developers and products, would support MFA. The proposed revision requires most of the developers who must comply with the current adopted certification criterion with actual MFA functionality versus an attestation of its use.

The proposed revised certification criterion will require developers who certify ''view, download, transmit to 3rd party'' (§ 170.315(e)(1)); ''standardized API for patient and population services'' (§ 170.315(g)(10)) (for ''patient facing'' access); and ''electronic prescribing'' (§ 170.315(b)(3)) to comply with the revised certification criterion. Similar to developers and products overall that must meet the MFA certification criterion, 43% of these developers of these products that meet any of these three certification criteria attested ''yes'' that they support multi-factor authentication.

The proposed revisions include:

- Revise § 170.315(d)(13)(i) to require Health IT Module support for authentication, through multiple elements of the user's identity, according to industry recognized standards.
- Revise § 170.315(d)(13)(ii) to require that Health IT Modules provide

[450] *https://build.fhir.org/subscriptions.html.*

[451] *https://build.fhir.org/versions.html#maturity.*

[452] *https://build.fhir.org/subscriptions.html.*

functionality that allows users (*e.g.,* providers and patients) to configure, enable and disable these multi-factor authentication capabilities.

- Revise § 170.550(h)(3) to require compliance for § 170.315(d)(13) for § 170.315(e)(1), § 170.315(g)(10), and § 170.315(b)(3). No other certification criteria will require compliance to § 170.315(d)(13).

The estimated costs will vary depending on current developer attestations to the MFA certification criterion. We assume an overall lower level of burden for developers who attested ''yes'' to support MFA to comply with this revised certification criterion. We separate out the costs for these developers from those that attested ''no'' to support MFA.

These tasks have their own level of effort and these estimates are detailed in Tables 69 to 71 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Tables 69 and 70 shows the estimated labor costs per product to modify the ''multi-factor authentication'' (MFA) certification criterion in § 170.315(d)(13). 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 71.

2. We estimate that 323 products certified by 252 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 323 products certified by 252 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products will need to certify the revised § 170.315(d)(13) certification criterion and need to meet the proposed requirements. As of the end of 2022, 96% of developers and 96% of products certified § 170.315(d)(13). The proposed modification to the certification criterion revises the certification criteria that must comply with this certification criterion to § 170.315(e)(1), § 170.315(g)(10), and § 170.315(b)(3) alone. As of the end of 2022, 65% of developers and 62% of products certified § 170.315(e)(1), § 170.315(g)(10), or § 170.315(b)(3). We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by and need to comply with the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

Table 69. Estimated Labor Hours to Modify Multi-factor Authentication § 170.315(d)(13) [Developers who currently attest "yes" that they support MFA (43%)]

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Authentication, through multiple elements of the user's identity, according to industry recognized standards		0	0	Developers who currently attest "yes" are assumed to meet these basic MFA capabilities.
Task 2: Allows users (e.g., providers and patients) to configure, enable and disable these multi-factor authentication capabilities		0	0	

Table 70. Estimated Labor Hours to Modify Multi-factor Authentication § 170.315(d)(13) [Developers who currently attest "no" that they support MFA (57%)]

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Authentication, through multiple elements of the user's identity, according to industry recognized standards		0	250	Developers who currently attest "no" may or may not support MFA in their products. It can be assumed that some may support but choose to attest "no". For others, it is expected to require a low level of effort to meet basic MFA capabilities.
Task 2: Allows users (e.g., providers and patients) to configure, enable and disable these multi-factor authentication capabilities		0	250	

Table 71. Total Cost to Modify Multi-factor Authentication § 170.315(d)(13) [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Developers who currently attest "yes"		
Task 1 (139 products)	$0	$0
Task 2 (139 products)	$0	$0
Developers who currently attest "no"		
Task 1 (184 products)	$0	$5,879,720
Task 2 (184products)	$0	$5,879,720
Total (323 products and 252 developers)	$	$11,759,440

The cost to a health IT developer to modify the ''multi-factor authentication'' certification criterion for their Health IT Modules would range from $0 to $36,407 per product, on average. Therefore, assuming 323 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $0 to $11.8 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed updates will improve information security and access. We believe our proposal helps improve security by increasing support of MFA. This is because it is unlikely that an unauthorized individual or entity will be able to succeed in proving one's identity when more than one authentication factor is used. The MFA certification criterion, as adopted through the ONC Cures Act Final Rule, required an attestation to promote transparency and encourage health IT developers who were not using MFA to do so. In that rule we articulated expected benefits that adopting MFA would reduce the likelihood that authentication credentials would be compromised and would eliminate an unnecessary use of IT resources and could directly reduce providers' operating/support costs, which would reduce their administrative and financial burden.

At the time, we believed supporting MFA to be an established best practice among industry developers, including health IT developers, but we did not have access to published literature that detailed how health IT developers were already supporting MFA industry-wide, but we believed the majority of health IT developers, or around 80%, were taking such actions. We assumed that building this functionality was in the future project plans for the remaining 20% because, as noted previously, adopting these capabilities is an industry best practice. We believed that health IT developers that had not yet adopted these capabilities were likely making financial investments to get up to speed with industry standards. We believed our proposal would motivate

these health IT developers to speed their implementation process. We also did not attribute a monetary estimate to this potential benefit because our rule is not a direct cause of health IT developers adopting these capabilities.

The Program data for MFA attestations tell us that less than half of developers attested ''yes'' that they support MFA, far less than the 80% we assumed support MFA in our prior rulemaking. The attestation alone does not confirm support of MFA, but the data does tell us the attestation alone may be insufficient to enforce this information security best practice across certified health IT. Ensuring Health IT Modules use industry best practice to protect health information will benefit the security of patient health information and prevent malicious access to authentication credentials. This proposed revision further motivates certified health IT developers to develop this information security for their products. The benefits of these modifications are not quantifiable at this time, and we welcome comment on how to quantify these benefits, if any.

18. Revised Computerized Provider Order Entry—Laboratory Criterion

We propose to update the ''computerized provider order entry—laboratory'' certification criterion in § 170.315(a)(2) to require enabling a user to create and transmit laboratory orders electronically according to the standard specified in § 170.205(g)(2), the HL7® Laboratory Order Interface (LOI) Implementation Guide. We further propose to update § 170.315(a)(2) to require technology to receive and validate laboratory results according to the standard specific in § 170.205(g)(3), the HL7® Laboratory Results Interface (LRI) Implementation Guide. Ensuring that systems creating laboratory orders can transmit orders and receive associated results and values electronically, according to national standards, will create more complete patient information available to clinicians throughout the laboratory workflow.

Costs

This section describes the estimated cost of meeting the requirements in the proposed updates to § 170.315(a)(2). These tasks have their own level of effort, and these estimates are detailed in Tables 72 and 73 below and are based on the following assumptions:

1. Health IT developers will experience the assumed average costs of labor and data model use. Table 72 shows the estimated labor costs per product to meet the proposed requirements in § 170.315(a)(2). We recognize that health IT developer costs will vary; however, our estimates in this section assume all health IT developers will incur, on average, the costs noted in Table 73.

2. We estimate that 302 products certified by 33 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above. The estimate of 302 products certified by 33 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify § 170.315(a)(2) and § 170.315(f)(3) (Transmission to public health agencies—reportable laboratory tests and values/results) need to meet the proposed requirements. As of the end of 2022, 62% of developers and 58% of products certified § 170.315(a)(2) and 10% of developers and 9% of products certified to § 170.315(f)(3). We applied these modifiers to our total developer and product estimate, after removing duplicates as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

Table 72. Estimated Labor Hours to Meet the Proposed Requirements in § 170.315(a)(2)

Computerized provider order entry – Laboratory

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Create and transmit laboratory orders according to § 170.205(g)(2) standard	Enabling a user to create and transmit laboratory orders electronically according to the standard specified in § 170.205(g)(2), the HL7® Laboratory Order Interface (LOI) Implementation Guide	500	1000	In the 2015 Edition Health IT Certification Criteria, it was estimated that it would require 50-100 preparation hours to implement § 170.315(a)(2). We take a similar approach here.
Task 2: Receive and validate laboratory results according to § 170.205(g)(3) standard	Require technology to receive and validate laboratory results according to the standard specified in § 170.205(g)(3), the HL7® Laboratory Results Interface (LRI) Implementation Guide	500	1000	In the 2015 Edition Health IT Certification Criteria, it was estimated that it would require 50-100 preparation hours to implement § 170.315(a)(2). We take a similar approach here.

Table 73. Total Cost to Products and Developers to Meet the Proposed Requirements in § 170.315(a)(2) [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1: Create and transmit laboratory orders according to § 170.205(g)(2) standard	$19,300,820	$38,601,640
Task 2: Receive and validate laboratory results according to § 170.205(g)(3) standard	$19,300,820	$38,601,640
Total cost per product	$127,820	$255,640
Total cost for all products (302 products)	$38,601,640	$77,203,280
Total cost per developer (33 developers)	$989,786	$1,979,571

Notes: We used a 58% modifier for the § 170.315(a)(2) certification criterion to estimate the number of products impacted by the Computerized provider order entry – Laboratory updates. Estimates reflect the percent of all products that certify to the § 170.315(a)(2) certification criterion through 2022. This estimate is subject to change. Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (302 products). Total cost per developer = Total cost for all products / Number of developers (33 developers).

The cost to products and developers to meet the proposed requirements in creating and transmitting laboratory orders according to § 170.205(g)(2) standard would range from $63,910 to $127,820 per product, on average. The products and developers to meet the proposed requirements in receive and validating the laboratory results according to § 170.205(g)(3) standard would also range from $63,910 to $127,820 per product. Therefore, assuming 302 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $39 million to $77 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

We believe this proposal would benefit health care providers, patients, and the industry. The updates to these specifications, and the inclusion of the receipt of orders in § 170.315(f)(3), as well as the receipt of results in § 170.315(a)(2), ensure that functions throughout the lifecycle of the laboratory order, from entry, to result, to reporting to public health agency, is covered by electronic requirements with the associated national standard. We believe these proposed updates will enhance the completeness of critical patient information that are made available to clinicians, laboratory, and public health agency receiving the laboratory results. Addressing the current gaps in patient information is critical as we strive to improve health equity as well as contact tracing and patient outreach to slow down the spread of infectious diseases.

A typical interface between a laboratory information system and electronic health record can cost between $5,000 to $50,000 and take up to six months to implement.[453] The expense and complexity of these interfaces and implementation efforts are primarily due to a lack of consistent application of industry standards for laboratory result reporting. The LOI and LRI Implementation Guides address variability and customization that was possible in Electronic Laboratory Reporting (ELR) by providing an unambiguous specification for ambulatory lab reporting, significantly decreasing the need for mapping or unique configuration for each interface. These implementation guides also have uses beyond public health reporting where hospitals and other users could re-use existing orders and results interfaces used for non-public health purposes for public health purposes instead of needing to implement a new specification.

[453] *https://www.politico.com/story/2015/02/data-fees-health-care-reform-115402.*

The LRI IG outlines multiple use cases, allowing for flexibility and scalability while reducing implementation and maintenance burden for the users. It also includes details such as formatting time stamp that will help reduce the need for standardization afterwards. The LOI IG has the potential to support inter-organizational care, improve care delivery, and clinical outcomes.

Although the benefits of these modifications are not quantifiable at this time, we expect the resulting improvements to interoperable exchange of health information to significantly benefit health care providers, laboratories, and public health agencies and improve the quality of health care provided. Public health initiatives will benefit from the proposed changes through increased standardization and interoperability of laboratory computerized provider order entry.

19. Revised Standardized API for Patient and Population Services Criterion To Align With Modular API Capabilities

As part of our overall proposal, we propose to revise the structure of the regulation text in § 170.315(g)(10) for clarity as well as phrasing consistency with other proposed API certification criteria in this proposed rule (*e.g.,* the proposed applicable § 170.315(j) certification criteria). We do not believe

this revision will create additional development effort as many of the functional requirements for Health IT Modules remain the same. We request comment on additional burden and level of effort for the proposed revisions.

We, however, propose new functional requirements for § 170.315(g)(10) beyond these revisions to regulation text and describe them and their estimated burden, below:

Patient and User Authorization Revocation

This would require a Health IT Module's authorization server to be able to revoke and must revoke an authorized application's access at a user's direction within 1 hour of the request. This is distinct from the existing patient authorization revocation requirement currently in § 170.315(g)(10)(vi) which requires support for revocation of a patient's authorization but does not require support for revocation of a clinician's authorization. We propose introducing this requirement to support revocation for both patient and clinician authorizations to enable clinicians to have greater control over their authorizations for applications to access patient data. We believe the underlying functionality to support user authorization revocation is very similar to the current adopted functionality of patient access revocation, and do not estimate additional burden to support both revocation functionalities. We request comment on additional burden to support this revocation functionality.

Alignment With Proposed (j) Certification Criteria (1)–(7)

We propose to add a new category of certification criteria to § 170.315(j) titled ''Modular API capabilities.'' The § 170.315(j) certification criteria, if finalized, would allow for specific API certification requirements to be demonstrated independently or in different combinations through the Program (when meeting all of § 170.315(g)(10)'s requirements would not be applicable). Technology updates to the Standardized API certification criterion are considered to be minimal, as the applicable new (j) certification criteria are already supported by Health IT Modules certified to the certification criterion and believe they would not require additional development effort. We request comment on additional burden to support alignment of the certification criterion with the proposed certification criteria § 170.315(j)(1) through § 170.315(j)(7).

Support for Workflow Triggers for Decision Support Interventions

We propose to require support for workflow triggers for decision support interventions under proposed § 170.315(g)(10)(iv). We propose that the Health IT Module must support capabilities in § 170.315(j)(20) (where we have proposed to adopt the ''workflow triggers for decision support interventions'' certification criterion) to enable workflow triggers to call decision support services, including support for ''patient-view'' and ''order-sign'' CDS Hooks according to at least one of the versions of the implementation specification adopted in § 170.215(f)(1).

Support for Verifiable Health Records (j)(22)

We propose support for the issuance of verifiable health records as specified by the requirements in proposed § 170.315(j)(22) be supported. We propose requiring support for verifiable health records in the § 170.315(g)(10) certification criterion to support the ability for patients to access their immunization and infectious disease-related laboratory test information in a format that is easily portable and verifiable by third parties.

Costs

The tasks and estimated cost to revise § 170.315(g)(10) to support verifiable health records are detailed in Tables 74 to 75 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 74 shows the estimated labor costs per product to revise § 170.315(g)(10) to support verifiable health records. 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 75.

2. We estimate that 224 products certified by 182 developers will be affected by our proposal. These estimates are a subset of the total estimated number of health IT developers and certified products we estimated above. The estimate of 224 products certified by 182 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products certify to the § 170.315(g)(10) certification criterion and need to meet the proposed requirements. As of the end of 2022, 47% of developers and 43% of products certified to § 170.315(g)(10) certification criterion. We applied this modifier to our total developer and product estimate as an overall estimate of the number of developers and products impacted by the proposed modifications to the certification criterion.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

[454] Estimate derived from a prototype implementation of SMART on FHIR, in which four EHR vendors completed necessary work with one or two software engineers in under 2 months without previously implementing any portion of the FHIR API. Source: SMART on FHIR: a standards-based, interoperable apps platform for electronic health records—PMC (*nih.gov*).

[455] Please reference the impact analysis for verifiable health records for more information about the costs and benefits of adopting the SMART Health Cards standard.

Table 74. Estimated Labor Hours to Revise § 170.315(g)(10) Standardized API for Patient and Population Services

Task 1: Patient access via SMART cards	Health IT Module must enable patient access to immunization information stored in certified health IT using SMART Health Cards in § 170.315(j)(22).	0	500	(1) Lower bound assumes health IT product already enables patient access to SMART Health Cards as described in the impact analysis for § 170.315(j)(22). (2) Upper bound assumes health IT product does not yet enable patient access to SMART Health Cards as described in the impact analysis for § 170.315(j)(22).[454,455]
Task 2: Adoption of HL7 CDS Hooks FHIR Implementation Guide version 2.0	Adoption of CDS Hooks FHIR Implementation Guide version 2.0 in § 170.215(f) as a prerequisite to facilitate API-driven CDS workflow triggers in § 170.315(j)(20)	0	1,000	First balloted 5 years ago, CDS Hooks is mature but still in trial use. We propose a minimal implementation of the standard and believe this implementation is likely supported and deployed by some developers, but not all in some fashion.
Task 3: Support for the "patient-view" hook	We believe that the "patient-view" hook has the highest maturity level and that implementers of CDS Hooks can consistently support this hook.	0	150	The "patient-view" hook is FHIR maturity model level 5 and has been implemented by several different systems.
Task 4: Support for the "order-sign" hook	We believe that the "order-sign hook has the highest maturity level and that implementers of CDS Hooks can consistently support this hook.	0	150	The "order-sign" hook is FHIR maturity model level 5 and has been implemented by several different systems.

BILLING CODE 4150–45–C

Table 75. Summary of Costs for Products and Developers to Revise § 170.315(g)(10) Standardized API for Patient and Population Services [2022 dollars]

Activity	Estimated Costs	
	Lower bound	Upper bound
Task 1	$0	$63,910
Task 2	$0	$127,820
Task 3	$0	$19,173
Task 4	$0	$19,173
Total cost per product	**$0**	**$230,076**
Task 1	$0	$14,315,840
Task 2	$0	$28,631,680
Task 3	$0	$4,294,752
Task 4	$0	$4,294,752
Total cost for all products (224 products)	**$0**	**$51,537,024**

Notes: Total cost per product = Labor hours x Hourly wage. Total cost for all products = Labor hours x Hourly wage x Number of products (177 products). Total cost per developer = Total cost for all products / Number of developers (147 developers).

The cost to meet the proposed requirements to revise the ''standardized API for patient and population services'' certification criterion to support verifiable health records would range from $0 to $230,076 per product, on average. Therefore, assuming 224 products overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $0 to $51.5 million.

Benefits

Requiring Health IT Modules to enable patient access to immunization information stored in certified health IT using SMART Health Cards in § 170.315(j)(22) provides several benefits to both patients and providers. SMART Health Cards provide an easy way to store vaccination history and test results for personal records and enable patients to easily share their status with an organization when needed. SMART Health Cards empower patients by providing secure access to their electronic health information.[456]

The SMART Health Card framework has been used, for example, to deploy Digital Vaccine Records (DVR) for vaccine verification which contain name, date of birth, vaccination dates, and vaccine manufacturer, much like the COVID–19 vaccination paper card.[457] This makes it more convenient for individuals to show proof of vaccination by downloading their DVR rather than maintaining a paper card. In August of 2021, the California Department of Public Health required all hospital visitors to show proof of vaccination or a negative test result within 72 hours. Two physicians/clinical informatics scholars from University of California San Diego shared their experience that hospital visitors expressed their appreciation for the ease and accessibility of the digital cards, especially if they did not have their paper vaccine cards. The digital cards also made the validation process easier for staff who were checking vaccination status. Thus, SMART Health Cards also have several benefits to hospitals and health care providers. For instance, SMART Health Cards enable accurate identification of patients who receive care, can help expedite admissions processes, decrease medical errors, and reduce healthcare costs.[458] Further, enabling patient access to SMART Health Cards would increase patient access to electronic health information, which enables individuals to make more informed decisions about their health and care.

Clinicians will benefit from the updates to the certified criterion through increased standardization and interoperability of CDS Hooks technology. Certified use of CDS Hooks is expected to facilitate more patient-specific results from clinical decision support tools, assisting providers in a more patient-centric approach to care. Based on public feedback on ONC's request for information in the HTI–1 Proposed Rule, commenters were generally more supportive of certification criteria for adoption of the v2.0 specification of FHIR CDS Hooks, as opposed to v1.0. Many also preferred ONC supporting narrow certification criteria related to a particular user guide, as we have specified in this proposal. Further, we believe that the ''patient-view'' and ''order-sign'' hooks proposed to be required for certification are the most mature, as supported by public comment, and that current implementers of CDS Hooks will be able to implement this with limited additional challenge. We believe the nature of our proposal addresses some of these concerns. Further, the ''patient-view'' and ''order-sign'' hooks were among the hooks recommended by commenters to use as part of the certification requirements. Given commenter concerns for use-case specific guidance, we propose support for the ''patient-view'' and ''order-sign'' hooks, specifically, given their broad applicability across use cases.

Support for Subscriptions—Server (j)(23)

We propose support for subscriptions as a server according to the requirements specified in § 170.315(j)(23). This is to support the distinct proposal for subscriptions for public health use cases as proposed in this rule at section titled ''Health IT Modules Supporting Public Health Data Exchange.'' We believe, as noted in the impact analysis for the ''Standardized

[456] Smart-Cards-in-Healthcare-FAQ-Series-Smart-Cards-and-Patients.pdf (*securetechalliance.org*).

[457] *https://www.mcpdigitalhealth.org/article/S2949-7612(23)00008-1/fulltext.*

[458] Smart-Cards-in-Healthcare-FAQ-Series-Smart-Cards-and-Healthcare-Providers.pdf (*securetechalliance.org*).

API for Public Health Data Exchange'' certification criterion in § 170.315(g)(20), that Health IT Modules that will need to adopt the new § 170.315(g)(20) certification criterion already supports the § 170.315(g)(10) certification criterion. And, as we propose that § 170.315(g)(20) support the proposed § 170.315(j)(23) certification criterion, revisions to § 170.315(g)(10) to support § 170.315(j)(23) should be minimal, as support for § 170.315(j)(23) should already be built into updates for these Health IT Modules. We request comment on additional burden to support this functionality.

20. Patient, Provider, and Payer APIs

We have proposed a set of certification criteria for payer data exchange, beneficiary access, and network information APIs in § 170.315(g)(30) through (36) that aim to complement and advance the policies that CMS has developed to increase patient, provider, and payer access to information. If health IT developers (including those that support payers or are part of a payer) were to seek testing and certification to these proposed certification criteria, we believe that they would be better positioned to support more effective exchange of clinical, coverage, and prior authorization information and would help ensure that technology used to satisfy the CMS requirements has been tested for conformance with widely available industry standards designed to support interoperability for each use case. These proposed certification criteria reference a set of API implementation specifications based upon the HL7® FHIR® Release 4 base standard. The new certification criteria also incorporate FHIR capabilities proposed in § 170.315(j), which are proposed elsewhere in this rule. These certification criteria include FHIR capabilities such as CDS Hooks and requirements for authorization and authentication, among others.

The proposed certification criteria would enable users of certified health IT to meet requirements for payers and providers in the CMS regulations, specifically, CMS API requirements at the following: Patient Access API (85 FR 25558), Provider Access API (87 FR 76254), Payer-to-Payer API (87 FR 76243), Prior Authorization and Requirements Discovery (PARDD) API (87 FR 76285), and the Provider Directory API (85 FR 25559). We propose to adopt and reference the same required and recommended implementation specifications within the certification criteria.

Costs

The proposed certification criteria are:

- § 170.315(g)(30) Beneficiary access
- § 170.315(g)(31) Payer to provider exchange (provider)
- § 170.315(g)(32) Payer to provider exchange (payer)
- § 170.315(g)(33) Payer to payer exchange
- § 170.315(g)(34) Prior authorization (provider)
- § 170.315(g)(35) Prior authorization (payer)
- § 170.315(g)(36) Network information

Certification criteria (g)(30), (g)(32), (g)(33), (g)(35), and (g)(36) adopt and reference the same required and recommended implementation specifications from the CMS requirements. For the purposes of this impact analysis, we assume that health IT developers (including those that support payers or are part of a payer) who elect to test and certify their Health IT Modules to any one of these four certification criteria face no additional costs beyond those estimated in the CMS regulatory impact analysis for these API requirements. We assume the same level of effort estimated by CMS. Furthermore, the certification criteria provide a predictable and transparent method of health IT developers to test and certify that their modules meet the CMS API requirements, providing entities required to meet these API requirements a way to demonstrate conformance to their users.

Certification criteria (g)(31) and (g)(34) enable bi-directional exchange and transfer of data between payer systems (who must meet CMS API requirements) and provider systems who receive information from payer systems to inform patient care and facilitate prior authorization. These two certification criteria do not implement CMS requirements (which only affect payer systems), but if adopted by health IT developers can further enable interoperability between payer and provider systems. The effort to test and certify these two certification criteria goes beyond the requirements to meet CMS API requirements, however, no policy in this proposed rule requires adoption of these certification criteria. We see these as optional certification criteria that may be voluntarily adopted by health IT developers to further interoperability. The impact analysis, below, estimates costs for a single Health IT Module to adopt the certification criteria: ''Payer to provider exchange (provider)'' and ''Prior authorization (provider)''. The impact analysis assumes no additional costs for health IT developers to adopt ''Beneficiary Patient access'', ''Payer to provider exchange (payer)'', ''Payer to payer exchange'', ''Prior authorization (payer)'', and ''Network information''.

The proposed certification criteria: ''Payer to provider exchange (provider)'' and ''Prior authorization (provider)'' have their own level of effort and these estimates are detailed in Tables 76 to 79 below and are based on the following assumptions:

Health IT developers will use the same labor costs and data models. Tables 76 and 77 shows the estimated labor costs per product to develop ''Payer to provider exchange (provider)'' and ''Prior authorization (provider)''. 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 Tables 78 and 79.

According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

Table 76. Estimated Labor Hours to Develop § 170.315(g)(31)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adopt HL7 FHIR Da Vinci Payer Data Exchange (PDex) Implementation Guide: Version STU 1.0.0		500	1,000	Lower bound assumes developer has implemented this or prior IG versions but will require development time to implement as directed.
Task 2: Adoption of HL7 CDS Hooks FHIR Implementation Guide version 2.0		0	1,000	See the workflow triggers for decision support intervention impact analysis for further information about development effort to meet § 170.315(j)(20).
Task 3: Support for the "patient-view" hook		0	150	See the workflow triggers for decision support intervention impact analysis for further information about development effort to meet § 170.315(j)(20).
Task 4: Support for "appointment-book"hook		75	150	

Table 77. Estimated Labor Hours to Develop § 170.315(g)(34)

Task	Details	Lower bound hours	Upper bound hours	Remarks
Task 1: Adopt HL7 FHIR Da Vinci—Coverage Requirements Discovery (CRD) Implementation Guide: Version STU 1.0.0	Support the request and exchange of information that supports the identification of coverage requirements	500	1,000	Lower bound assumes developer has implemented this or prior IG versions but will require development time to implement as directed.
Task 2: Support for all "SHOULD" requirements described in the "Resource summary" section of the "CRD Client CapabilityStatement"		0	40	Lower bound assumes developer has implemented this or prior IG versions but will require development time to implement as directed.
Task 3: Support for the SMART App Launch Framework "confidential app" profile		0	80	
Task 4: Adoption of HL7 CDS Hooks FHIR Implementation Guide version 2.0		0	1,000	See the workflow triggers for decision support intervention impact analysis for further information about development effort to meet § 170.315(j)(20).
Task 5: Support for "appointment-book," "encounter-start," "encounter-discharge," "order-dispatch," "order-select," and "order-sign" hooks		450	900	
Task 6: HL7 FHIR Da Vinci—Documentation Templates and Rules (DTR) Implementation Guide: Version STU 1.0.0	Support the ability to exchange and execute rules to ensure that prior authorization documentation requirements are met	500	1,000	Lower bound assumes developer has implemented this or prior IG versions but will require development time to implement as directed.
Task 7: HL7 FHIR Da Vinci—Prior Authorization Support (PAS) Implementation Guide: Version STU 1.1.0	Ability of the API to create and send prior authorization requests and to receive prior authorization responses	500	1,000	Lower bound assumes developer has implemented this or prior IG versions but will require development time to implement as directed.

BILLING CODE 4150–45–C

Table 78. Total Cost to Develop § 170.315(g)(31) for 1 product [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (1 product)	$63,910	$127,820
Task 2 (1 product)	$0	$127,820
Task 3 (1 product)	$0	$19,173
Task 4 (1 product)	$9,587	$19,173
Total (1 product and 1 developer)	$73,497	$293,986

Table 79. Total Cost to Develop § 170.315(g)(34) for 1 product [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (1 product)	$63,910	$127,820
Task 2 (1 product)	$0	$5,113
Task 3 (1 product)	$0	$10,226
Task 4 (1 product)	$0	$127,820
Task 5 (1 product)	$57,519	$115,038
Task 6 (1 product)	$63,910	$127,820
Task 7 (1 product)	$63,910	$127,820
Total (1 products and 1 developer)	$249,249	$641,656

The cost to a health IT developer to develop criteria ''payer to provider exchange (provider)'' and ''prior authorization (provider)'' for their Health IT Modules would range from $323,000 to $936,000 per product, on average. Individually, the cost to develop ''payer to provider exchange (provider)'' would be $73,500 to $294,000 per product and ''prior authorization (provider)'' would be $249,000 to $642,000 per product.

Benefits

Payers and providers have both adopted electronic prior authorization and it has increased from 12% to 28% from 2018 to 2022.[459] Phone and fax is largely used by payers to manage prior authorizations and the peer-to-peer review process for denial appeals.[460] Prior authorization poses a large financial and administrative burden on clinicians prescribing medication.[461] A recent survey found that physicians spent 1 hour per week on average, nursing staff spent about 13 hours per week on average, and clerical staff spent about 6 hours per week on average completing prior authorization activities.[462] Another survey found that individual manual prior authorization took about 20 minutes, portal prior authorization took 12 minutes, and electronic prior authorization took 9 minutes. Another survey which had 1,147 responses from 100,000 providers found that most providers spent up to 5 hours per week on prior authorization submissions. There was no difference in the amount of time it took to complete manual prior authorizations compared to electronic prior authorizations.[463]

Prior authorization decisions can cause patient distress, make untreated symptoms last longer, and delay diagnosis. In 2020, the CAQH estimated that the cost to providers of a manual prior authorization approval was $10.92 per claim, while the cost to payers was $3.32 per claim. In 2018, the Cleveland Clinic estimated the cost to providers was $12 per claim. A policy paper for The Hamilton Project calculated that staff time is approximately 25 hours per week in resolving 37 prior authorization adjudications at $20 per hour, which equals $14 per claim as a cost to medical staff.[464]

One possible benefit to standardization of prior authorization is a shorter decision time on prior authorizations. Based on a survey of 1,147 responses from 100,000 providers, physicians and researchers from University of Nebraska Medical Center found it took health plans less time to submit decisions electronically, though providers had similar challenges with electronic prior authorizations as they did with manual prior authorizations.[465]

There are several pilots underway to test the prior authorization API, as well as other tools. One pilot, led by Regence, used the HL7 FHIR standard to automate prior authorization. Using the SmartAuth app integrated with the Epic EHR, they were able to automatically populate policy criteria and automatically extract clinicals from the EHR. They were able to make immediate

[459] *https://www.caqh.org/sites/default/files/2022-caqh-index-report%20FINAL%20SPREAD%20VERSION.pdf.*

[460] *https://ascopubs.org/doi/full/10.1200/EDBK_100036.*

[461] *https://www.sciencedirect.com/science/article/pii/S1551741118301542?via%3Dihub.*

[462] *https://onlinelibrary.wiley.com/doi/full/10.1111/ctr.14964.*

[463] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10332446/.*

[464] *https://www.hamiltonproject.org/wp-content/uploads/2023/01/Cutler_PP_LO.pdf.*

[465] *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10332446/.*

determinations on over 90% of the requests with nearly all determined that prior authorization was not required. Whereas, without the use of the app and automated process, providers might wait hours or days just to find out prior authorization is not required. In some cases, prior authorization was automatically processed, enabling an immediate decision to prescribe or suggest a treatment. This was all enabled using an API built using the FHIR standard.

Setting a standard, electronic method to facilitate payer and provider exchange and the prior authorization of certain treatments and medications can reduce overall time and effort for payers and providers alike. A standard, uniform process can also be replicated across many IT systems, ensuring reliable interoperability between systems and more certainty to providers that they can electronically submit a prior authorization to a payer and receive a response congruent with their technology and workflow. A piecemeal system where providers may need to follow different procedures and processes for different payers increases burden on providers and administrators and reduces their time to treat and manage patients.

CMS in their final rule, ''Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program'', assessed the overall benefit and level of effort to standardize prior authorization and payer exchange.[466] CMS estimates, over a ten-year period, that physician groups and hospitals could face reduced costs of $15.3 billion if they adopted this technology to standardize prior authorization. We believe that these proposed certification criteria would provide a reliable and transparent testing and certification process for the functionalities proposed by CMS to facilitate data exchange and prior authorization, helping to enable these expected benefits for technology users. As stated earlier, these proposed certification criteria adopt the standards and functionality proposed by CMS and we assume that testing and certifying these certification criteria would not exceed the level effort estimated by CMS. We also believe that these certification criteria, if voluntarily adopted by developers, would help ensure that the technology are developed and deployed in a standard, uniform way, culminating into the expected savings to physician groups and hospitals estimated by CMS in their rulemaking.

21. Insights

We propose to update the Insights condition of certification to incorporate updates and revisions based on proposed changes to certification requirements in this proposed rulemaking that affect the Insights measures finalized in HTI–1. The proposed updates to the Insights condition of certification include: (1) updates to the ''Individuals' access to electronic health information through certified health IT'' Insights measure; (2) updates to the ''C–CDA medications, allergies, and problems reconciliation and incorporation through certified health IT'' Insights measure; and (3) new requirements for developers of certified health IT to list the clients and their publicly available identifiers (*e.g.,* NPI) who were included in the measurement of submitted Insights measures.

Estimated Labor Hours To Meet Updated ''Individuals' Access to Electronic Health Information Through Certified Health IT'' Measure for Insights

In the HTI–1 Final Rule, the ''Individuals' access to electronic health information through certified health IT'' measure and related metrics only counts individuals' access of their EHI when measuring access to EHI.[467] We request comment on whether the changes proposed related to revising the definition of counting access to EHI to include both individuals and individuals' authorized representatives accessing their EHI (rather than just individuals alone) would have an incremental increase (or decrease) in burden compared to what was estimated in the HTI–1 Final Rule. The HTI–1 Final Rule regulatory impact analysis found that it would cost between $170,000 and $354,000 per developer to implement this measure.

We believe it would be beneficial to developers of certified health IT to make ONC's patient access measure consist with the CMS Promoting Interoperability (PI) Measure for patient access (''Provide Patients Electronic Access to Their Health Information''), which counts both patients and their authorized representatives for measuring patient access for access using portals or apps.

We expect that the proposed changes would not impact or potentially reduce burden associated with implementing this measure as previously estimated in the HTI–1 Final Rule as it now aligns with how CMS operationalizes this measure; however, we request comment on this.

Estimated Labor Hours To Meet Updated ''C–CDA Reconciliation and Incorporation Through Certified Health IT'' Measure for Insights

The ''C–CDA medications, allergies, and problems reconciliation and incorporation through certified health IT'' measure was finalized in the HTI–1 Final Rule and is now proposed to be renamed as ''C–CDA reconciliation and incorporation through certified health IT''.[468] The prior HTI–1 Final Rule regulatory impact analysis found that it would cost between $402,000 and $1,117,000 per developer to implement this measure.

We request comment on the incremental burden associated with updating the measure to align with updates to the certification criterion § 170.315(b)(2). Specifically, we are requesting comment on the potential increase in burden associated with updating the metric to include additional data classes that are proposed (in one proposal 6 data classes, in another proposal all data classes associated with USCDI v4). We are also requesting comment on the additional incremental costs associated with dividing the metrics according to the use of the three processes that make up the definition for ''any method'' so that it aligns with the updates being proposed to § 170.315(b)(2) related to automatic reconciliation and incorporation capabilities.

Estimated Labor Hours To Meet Provider Listing Requirements for Insights

The Insights condition of certification, as finalized in the HTI–1 Final Rule,

[466] *https://www.federalregister.gov/documents/2024/02/08/2024-00895/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-advancing-interoperability.*

[467] *https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and.*

[468] *https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and.*

allows developers of certified health IT to select specific end-users to submit data for measurement of applicable Insights measures, due to known constraints with developers' ability to get data needed to inform Insights measures from their clients' systems. ONC granted flexibility to developers in how they calculate their measures, given this reality. We propose to update the Insights condition to include an additional requirement for developers who submit any Insights measure to include a list of the clients included in the measurement of the submitted measure(s). This will enable further analysis of the measures to determine representativeness of clients included in measurements.

Costs

The tasks associated with proposed requirement to provide client information have their own level of effort and these estimates are detailed in Tables 80 and 81 below and are based on the following assumptions:

1. Health IT developers will use the same labor costs and data models. Table 80 shows the estimated labor costs per product to modify their technology to collect the requested or measures. 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 81.

2. We estimate that 176 products certified by 59 developers will be affected by our proposal. These estimates are a subset of the total estimated health IT developers and certified products we estimated above.

The estimate of 176 products certified by 59 developers is derived as follows. We estimate that, in total, 387 health IT developers will certify 521 health IT products impacted by this rulemaking. However, not all these developers and products must meet the Insights condition of certification and need to meet the proposed requirements. In the HTI–1 Final Rule we estimated the number of developers and products that would be required to meet the Insights condition of certification, based on thresholds designed to capture insightful measures from the developers of certified health IT with the largest market share, excluding developers who server fewer than 50 hospitals or 500 clinicians and who certify a criterion with an applicable Insights measure.

3. According to the May 2022 BLS occupational employment statistics, the mean hourly wage for a ''Software Developer'' is $63.91. 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 $127.82.

BILLING CODE 4150–45–P

Table 80. Estimated Labor Hours to Modify Technology to Meet Proposed Insights Requirements [2022 dollars]

Task	Details	Lower Bound Hours	Upper Bound Hours	Remarks
Task 1: Data extract to pull list of clients whose data is included for Insights reporting	List of hospitals for products used in inpatient setting and clinicians for products used in outpatient setting	0	150	Lower bounds assume health IT developer already pulled the list to report the percentages required for HTI-1. Upper bound assumes the developer used a different approach to address reporting the percentages for HTI-1.
Task 2: Link national identifiers to list of clients whose data is included for Insights Reporting	Link national identifier (in the case of hospital CCN and for other providers, national provider identifier) to the list of clients	25	100	Lower bound assumes this national identifier data is available within clients' systems that developers have access to for the purpose of Insights reporting Upper bound assumes that other methods (e.g., algorithm) are needed to link the client list data to their national identifier
Task 3: Audit data to assess accuracy and completeness	Match list with national identifiers to external data source such as CMS NPPES NPI Registry, and	25	50	Lower bound assumes matches are found for most of the providers on the list

	review matched results for completeness and accuracy (e.g., by provider type)			Upper bound assumes some reconciliation and correction are needed to address in accuracies and missing data
Task 4: Create final files in ONC submission template	Put file in format requested by ONC for submission	2	8	Lower bound assumes current file format is close to the format requested by ONC Upper bound assumes file format is substantially different than format requested by ONC

Table 81. Total Cost to Modify Technology to Meet Proposed Insights Requirements [2022 dollars]

Activity	Estimated Cost	
	Lower bound	Upper bound
Task 1 (59 developers)	$0	$1,131,207
Task 2 (59 developers)	$188,535	$754,138
Task 3 (59 developers)	$188,535	$377,039
Task 4 (59 developers)	$15,083	$60,331
Total (176 products and 59 developers)	$392,152	$2,322,745

BILLING CODE 4150–45–C

The cost to a health IT developer to meet the proposed Insights requirements for their Health IT Modules would range from $6,647 to $39,369 per developer, on average. Therefore, assuming 59 developers overall and a labor rate of $127.82 per hour, we estimate that the total cost to all health IT developers would, on average, range from $392,00 to $2.3 million. This would be a one-time cost to developers per product that is certified to the specified certification criterion and would not be perpetual.

Benefits

The proposed update to the Insights Condition of Certification will enable more granular analysis and utility of the submitted Insights measures. The additional data will enable richer comparisons of measures across developers, creating greater value from the measures. The level of effort is low and could be programmed for successive reporting years.

22. Trusted Exchange Framework and Common Agreement℠

This regulation does not establish the requirements for the Trusted Exchange Framework and Common Agreement℠ (TEFCA℠), but instead outlines the application requirements an Applicant QHIN must submit in order to be Designated as a QHIN, and the requirements that an entity would attest to meeting as a participant in the TEFCA networks. We estimate that an Applicant QHIN would spend on average an hour to complete the application process. We estimate that an average Qualified Health Information Network™ (QHIN™) would spend at most one hour to complete the attestation process. We consider the effort to be de minimis.

We do not assess the burden of a QHIN to appeal a Recognized Coordinating Entity® (RCE™) decision as part of their participation in the TEFCA networks, as this proposed rulemaking creates the appeals process for QHINs but does not require it. Furthermore, appeals follow RCE decisions related to QHIN participation in the TEFCA networks, not ONC decisions. We, therefore, do not assess the burden of the appeals process as part of this proposed rulemaking's impact analysis.

Total Annual Cost Estimate

We estimate that the total annual cost for this proposed 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 result in $431.1 million. The total undiscounted perpetual cost over a 10-year period for this proposed rule (starting in year two), based on the cost estimates outlined above, would result in $398.1 million. We estimate the total costs to health IT developers to be $829.2 million.

We assume costs to health IT developers will stagger based on the timeline for developers to meet specific requirements. All requirements are expected to be met by the end of the third year after the rule is final, so all estimated costs will be incurred within that timeframe. Because many of the new requirements will necessitate immediate work to begin developing new technology, we estimate that 50% of total costs will come in the first year the rule is finalized. We estimate that the remaining 50% of total costs will come in the second and third year after the rule is finalized. Most of the new requirements must be met at the end of the second year after the rule is finalized and so a larger portion of the remaining costs are estimated for Year 2, while fewer requirements must be met in the third year after the rule is finalized. This cost breakdown is shown in Table 83.

Total Annual Benefit Estimate

We estimate the total annual benefit across all entities for this proposed rule beginning in Year 3, when the associated policies are required to be implemented and expected benefits to be realized, would be on average $22.2 million. We estimate the total benefits across all entities to be $177.6 million. This breakdown is shown in Table 83.

Total Annual Net Benefit

We estimate the total undiscounted perpetual annual net benefit for this proposed rule (starting in year three), based on the estimates outlined above, would result in a net benefit of $75.4 million.

b. Accounting Statement and Table

When a rule is considered significant under Section 3(f)(1) under Executive Order 12866 and E.O. 14094, we are required to develop an accounting statement indicating the classification of the expenditures associated with the provisions of the proposed rule. Monetary annual effects are presented as discounted flows using 3% and 7% factors in Table 82 below. We are not able to explicitly define the universe of all costs but have provided an average of likely costs of this proposed rule as well as a high and low range of likely costs.

Table 82 EO 12866 Summary Table. **(2022 dollars)**

	Primary (3%)	Primary (7%)
Present Value of Quantified Costs	$790,961,390.45	$744,748,749.67
Present Value of Quantified Benefits	$146,941,101.23	$115,824,623.61
Present Value of Net Benefits	$(644,020,289.21)	$(628,924,126.06)
	Primary (3%)	Primary (7%)
Annualized Quantified Costs	$92,724,804.51	$106,035,467.14
Annualized Quantified Benefits	$17,225,979.74	$16,490,820.66
	Primary (3%)	Primary (7%)
Annualized Net Quantified Benefits	$(75,498,824.77)	$(89,544,646,47)

Table 83. EO 12866 Summary Table Non-Discounted Flows. (2022 dollars)

	Total Costs	Total Benefits
Year 1	$431,091,278.98	$-
Year 2	$295,817,695.34	$-
Year 3	$102,267,903.24	$22,207,500.00
Year 4	$-	$22,207,500.00
Year 5	$-	$22,207,500.00
Year 6	$-	$22,207,500.00
Year 7	$-	$22,207,500.00
Year 8	$-	$22,207,500.00
Year 9	$-	$22,207,500.00
Year 10	$-	$22,207,500.00
Total	$829,176,877.55	$177,660,000.00

D. 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.[469]

The entities that are likely to be directly affected by the requirements in this proposed rule requirements are health IT developers. We note that the proposed updates and clarifications to the reasonable and necessary activities that do not constitute information blocking would 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. We refer readers to section IV for our information blocking-related proposals and welcome comments on their impacts on small entities.

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 proposed in this proposed rule most likely fall under the North American Industry Classification System (NAICS) code 541511 ''Custom Computer Programming Services.'' [470]

OMB advised that the Federal statistical establishment data published for reference years beginning on or after January 1, 2022, should be published using the 2022 NAICS United States codes.[471]

The SBA size standard associated with this NAICS code is set at $34 million annual receipts or less. There is enough data generally available to establish that between 75% and 90% 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% of health IT developers that have had Complete EHRs and/or Health IT Modules certified to the 2011 Edition have less than 51 employees.

We estimate that the proposed requirements in this proposed rule would 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 proposed the minimum number of requirements necessary to accomplish our primary policy goal of enhancing interoperability. Further, as discussed in this RIA above, there are very few appropriate regulatory or non-regulatory alternatives that could be developed to lessen the compliance burden associated with this proposed rule because at least a few of the proposals are derived directly from legislative mandates in the Cures Act.

We do not believe that the proposed requirements of this proposed rule would create a significant impact on a substantial number of small entities, but request comment on whether there are small entities that we have not identified that may be affected in a significant way by this proposed rule. Additionally, the Secretary proposes to certify that this proposed rule would not have a significant impact on a substantial number of small entities.

E. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has federalism implications. Nothing in this proposed rule imposes substantial direct compliance costs on State and local governments, preempts State law, or otherwise has federalism

[469] The SBA references that annual receipts mean ''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.

[470] *https://www.sba.gov/sites/sbagov/files/2023-06/TableofSizeStandards_EffectiveMarch17-29, 2023pdf.*

[471] *https://www.sba.gov/article/2022/feb/01/guidance-using-naics-2022-procurement.*

implications. We are not aware of any State laws or regulations that are contradicted or impeded by any of the proposals in this proposed rule. We welcome comments on this assessment.

F. 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 $183 million in 2024. While the estimated potential cost effects of this proposed rule reach the statutory threshold, we do not believe this proposed rule imposes unfunded mandates on State, local, and Tribal governments, or the private sector. We welcome comments on these conclusions.

List of Subjects

45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health information technology, Health insurance, Health records, Hospitals, Incorporation by reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and record keeping requirements, Public health, Security.

45 CFR Part 171

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health care provider, Health information exchange, Health information technology, Health information network, Health insurance, Health records, Hospitals, Privacy, Reporting and record keeping requirements, Public health, Security.

45 CFR Part 172

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Healthcare, Health information technology, Health insurance, Health records, Hospitals, Laboratories, Medicaid, Medicare, Privacy, Public health, Security.

For the reasons set forth in the preamble, HHS proposes to amend 45 CFR subtitle A, subchapter D, 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.

(a) The standards, implementation specifications, and certification criteria adopted in this part apply to health information technology and the testing and certification of Health IT Modules.

(b) If any provision of this part is held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or circumstance, it shall be construed to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

■ 3. Amend § 170.102 by:

■ a. Revising and republishing the definition of ''Base EHR''; and

■ b. Adding definitions for ''Business day or Business days'', ''Imaging link'', and ''Serious risk to public health or safety'' in alphabetical order.

The revisions, additions, and republications read as follows:

§ 170.102 Definitions.

* * * * *

Base EHR means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to healthcare quality;

(iv) To exchange electronic health information with, and integrate such information from other sources; and

(3) Has been certified to the certification criteria adopted by the Secretary in—

(i) Section 170.315(a)(1), (2), or (3); (a)(5) and (14), (b)(1), (c)(1), and (g)(7), (9), (10); and (h)(1) or (2);

(ii) Section 170.315(a)(9) or (b)(11) for the period up to and including December 31, 2024; and

(iii) Section 170.315(b)(11) on and after January 1, 2025.

(iv) Section 170.315(b)(3) and 170.315(b)(4) on and after January 1, 2028;

(v) Section 170.315(g)(20) on and after January 1, 2028;

(vi) Section 170.315(g)(31) on and after January 1, 2028; and

(vii) Section 170.315(g)(34) on and after January 1, 2027.

Business day or *Business days* means Monday through Friday, except the legal public holidays specified in 5 U.S.C. 6103 and any day declared to be a holiday by Federal statute or Executive order.

* * * * *

Imaging link means technical details which enable the electronic viewing or retrieval of one or more images over a network.

* * * * *

Serious risk to public health or safety means a single event or phenomenon or a recurring series of events or phenomena that by the nature and the fact of its occurrence endangers the life or safety of one or more individuals (as defined in 45 CFR 160.103). Such events and phenomena, when caused or contributed to by health information technology certified as a Health IT Module or as part of a certified Health IT Module (as defined in this section), are non-conformities to the ONC Health IT Certification Program requirements. This would be true even in situations where such certified Health IT Modules pass laboratory or in-the-field testing protocols for conformance to specific standards adopted in subpart B or criteria adopted in subpart C of this part. This definition includes, but is not limited to, the following:

(1) Erasure, other destruction, or truncation of some or all of one or more clinical data entries or of one or more points of metadata needed to maintain and demonstrate the integrity of the clinical data points (excluding erasure, destruction, or truncation commanded by a system administrator or user).

(2) Corruption of clinical data in one or more elements of any patient or patients' data through the certified health information technology's operation or interaction with other technology resulting in:

(i) Comingling or conflation of separate patients' information in a single record or user-interface display or screen, such that the comingled or conflated data appears to the end user to be a single patient's information.

(ii) Display of multiple patients' information on a single user interface screen or display without accurate

indication to the end user of which data pertains to which patient.

(iii) Attributing clinical documentation entered by an end user to a different patient than the patient whose record is identified to the end user as the destination of the documentation during the user's data entry.

(iv) Failure to accurately record and maintain the semantic meaning of documentation entries.

(v) Substitution of documentation entries from sources not selected or authorized by a user (excluding as a result of accurately executed, intentionally automated functions known to and approved by the user or user organization).

(3) Loss of clinical order data integrity, such as:

(i) Changes in numerical values for a prescription or treatment dose, frequency, quantity, or concentration that are not commanded by a user (excluding intentionally automated, accurate unit conversions).

(ii) Changes in a drug name, class, active ingredients, dose, form, or route of administration not commanded by a user (excluding intentionally automated, accurate substitution of nonproprietary names for brand names of the same drug or biologic).

(iii) Erroneously indicating to a clinician entering, or other user(s) reviewing, orders that an order has been sent when it has not been sent.

(iv) Failure to send orders to the recipient or destination designated by a human end user or by accurate, intentional automation of a health care provider's standard routing based on order characteristics.

(v) Failure to accurately execute an authorized user's command to delete, cancel, or discontinue a medication, treatment, or other clinical order.

(vi) Persistently listing a medication or treatment order as current or active after it was cancelled or otherwise intentionally discontinued.

(4) Creation, revision, update, or deletion of one or more data points within a patient record or of an entire record, other than as commanded by an authorized user or through accurate execution of an intentionally automated data feed or capture process.

(5) Failure to accurately execute authorized user commands to create, revise, update, or delete clinical notes or other documentation within a patient's record.

(6) Failure to maintain accurate logs of revisions or edits to any data within a patient record, including but not limited to accurate attribution of each revision to the human user or automated process making the change.

■ 4. Amend § 170.205 by:
■ a. Adding paragraph (a)(1);
■ b. Revising paragraph (a)(6);
■ c. Adding paragraph (d)(1);
■ d. Revising paragraph (d)(2) and (4);
■ e. Adding paragraph (e)(1);
■ f. Revising paragraph (e)(4);
■ g. Revising and republishing paragraph (g);
■ h. Revising paragraphs (h)(2) and (3);
■ i. Adding paragraphs (i)(3) and (4);
■ j. Revising paragraph (k)(1);
■ k. Removing and reserving paragraph (k)(2);
■ l. Revising paragraphs (k)(3) and (r)(1);
■ m. Adding paragraph (r)(2);
■ n. Revising (s)(1);
■ o. Adding paragraph (s)(2);
■ p. Revising paragraph (t)(2); and
■ q. Adding paragraph (v).

The additions, revisions, and republication read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

* * * * *

(a) * * *

(1) *Standard.* HL7® CDA® R2 Implementation Guide: Consolidated CDA (C–CDA) Templates for Clinical Notes, Edition 3—US Realm (C–CDA Edition 3) (incorporated by reference, see § 170.299).

* * * * *

(6) *Standard.* HL7® CDA® R2 Implementation Guide: C–CDA Templates for Clinical Notes STU Companion Guide, Release 4.1—US Realm (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(d) * * *

(1) *Standard.* HL7 Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1—US Realm Standard for Trial Use (incorporated by reference in § 170.299).

(2) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2027 for the purposes of the certification criteria in § 170.315(f).

* * * * *

(4) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). Implementation specifications. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings, Release 2.0, April 21, 2015 (incorporated by reference in § 170.299) and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015; Erratum to the CDC PHIN 2.0 Messaging Guide, April 2015 Release for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2027.

(e) * * *

(1) *Standard.* HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, 2018 Update (incorporated by reference in § 170.299).

* * * * *

* * * * *

(4) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). Implementation specifications. HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5 (incorporated by reference in § 170.299) and HL7 Version 2.5.1 Implementation Guide for Immunization Messaging (Release 1.5)—Addendum, July 2015 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2028.

* * * * *

(g) *Electronic transmission of laboratory results to public health agencies*—(1) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). Implementation specifications. HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm) (ELR) (incorporated by reference in § 170.299) with Errata and Clarifications, (incorporated by reference in § 170.299) and ELR 2.5.1 Clarification Document for EHR Technology Certification, (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2028.

(2) *Standard.* HL7 Version 2.5.1 Implementation Guide: Laboratory Orders Interface (LOI) from EHR, Release 1, STU Release 4—US Realm (incorporated by reference in § 170.299).

(3) *Standard.* HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface (LRI), Release 1 STU Release 4—US Realm (incorporated by reference in § 170.299).

(h) * * *

(2) *Standard.* HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I)—US Realm, STU 5.3 with errata (incorporated by reference in § 170.299).

(3) *Standard.* CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting, Implementation Guide for 2024, Version 1.1 (incorporated by reference in § 170.299).

(i) * * *

(3) *Standard.* HL7 FHIR Central Cancer Registry Reporting Content IG, 1.0.0—STU 1 (incorporated by reference in § 170.299).

(4) *Standard.* HL7 FHIR Cancer Pathology Data Sharing, 1.0.0—STU1 (incorporated by reference in § 170.299).

* * * * *

(k) * * *

(1) *Standard* HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture (QRDA III), Release 1—US Realm (ANSI/HL7 Normative Release 1) (incorporated by reference in § 170.299).

(2) [Reserved]

(3) *Standard.* CMS Implementation Guide for Quality Reporting Document Architecture Category III, Eligible Clinicians Programs, Implementation Guide for 2024, Version 1.1 (incorporated by reference in § 170.299).

* * * * *

(r) * * *

(1) *Standard.* The following sections of HL7 Implementation Guide for CDA® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2027. Technology is only required to conform to the following sections of the implementation guide:

(i) For the time period up to and including December 31, 2025, HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 (pages 69–72);

(ii) For the time period up to and including December 31, 2025, Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1 (pages 54–56); and

(iii) Antimicrobial Use (AUP) Summary Report (Numerator and Denominator) specific document template in Section 2.1.1.2 (pages 56–58).

(2) *Standard.* The following sections of HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release 3—U.S. Realm (incorporated by reference in § 170.299). Technology is only required to conform to the following sections of the implementation guide:

(i) HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator);

(ii) Antimicrobial Resistance Option (ARO) Summary Report (Denominator); and,

(iii) Antimicrobial Use (AUP) Summary Report (Numerator and Denominator).

(s) * * *

(1) *Standard.* HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, HL7 Draft Standard for Trial Use, Volume 1—Introductory Material and HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, HL7 Draft Standard for Trial Use, Volume 2—Templates and Supporting Material (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2027.

(2) *Standard.* HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1—US Realm (incorporated by reference in § 170.299).

(t) * * *

(2) *Standard.* HL7 CDA® R2 Implementation Guide: Public Health Case Report—the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1—US Realm (HL7 CDA eICR IG) (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2028.

* * * * *

(v) *Public health—birth reporting*—(1) *Standard.* HL7 FHIR Vital Records Birth and Fetal Death Reporting 1.1.0—STU 1.1 (incorporated by reference in § 170.299).

(2) [Reserved]

■ 5. Amend § 170.207 by:
■ a. Revising paragraph (a)(1);
■ b. Adding (a)(2);
■ c. Revising paragraphs (a)(4) and (c);
■ d. Revising and republishing paragraphs (d) and (e);
■ e. Revising paragraphs (f)(1) and (2);
■ f. Removing and reserving paragraph (f)(3);
■ g. Revising paragraphs (m)(1), (n)(1) introductory text, and (n)(2) and (3);
■ h. Revising and republishing paragraphs (o) and (p); and
■ i. Revising paragraphs (r)(1) and (s)(1).

The revisions, additions, and republications read as follows:

§ 170.207 Vocabulary standards for representing electronic health information.

(a) * * *

(1) *Standard.* SNOMED CT®, U.S. Edition, March 2022 Release (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(2) *Standard.* SNOMED CT®, U.S. Edition, September 2023 Release (incorporated by reference in § 170.299).

* * * * *

(4) *Standard.* IHTSDO SNOMED CT®, U.S. Edition, September 2015 Release (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

* * * * *

(c) * * *

(1) *Standard.* Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, a universal code system for identifying health measurements, observations, and documents produced by the Regenstrief Institute, Inc., February 16, 2022 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(2) *Standard.* Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.76, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (incorporated by reference in § 170.299).

(3) *Standard.* Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

* * * * *

(d) *Medications*—(1) *Clinical drugs*—(i) *Standard.* RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, July 5, 2022 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(ii) *Standard.* RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, December 4, 2023, Full Monthly Release (incorporated by reference in § 170.299).

(iii) *Standard.* RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, September 8, 2015 Release (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

(2) *Standard.* The code set specified at 45 CFR 162.1002(b)(2) as referenced in 45 CFR 162.1002(c)(1) for the time period on or after October 1, 2015.

(3) [Reserved]

(e) *Immunizations*—(1) *Standard.* HL7® Standard Code Set CVX—Vaccines Administered, dated through June 15, 2022 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(2) *Standard.* National Drug Code Directory (NDC)—Vaccine NDC Linker,

dated July 19, 2022 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(3) *Standard.* HL7 Standard Code Set CVX—Vaccines Administered, updates through August 17, 2015 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

(4) *Standard.* National Drug Code Directory (NDC)—Vaccine NDC Linker, updates through August 17, 2015 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026

(5) *Standard.* CDC National Center of Immunization and Respiratory Diseases (NCIRD) Code Set (CVX)—Vaccines Administered, updates through September 29, 2023 (incorporated by reference in § 170.299).

(6) *Standard.* National Drug Code Directory (NDC)—Vaccine NDC Linker, updates through November 6, 2023 (incorporated by reference in § 170.299).

(f) * * *

(1) *Standard.* The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15.

(i) The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997. The adoption of this standard expires on January 1, 2026.

(ii) U.S. Office of Management and Budget's Statistical Policy Directive No. 15: Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity (SPD 15), as revised, March 29, 2024.

(2) *Standard.* CDC Race and Ethnicity Code Set:

(i) CDC Race and Ethnicity Code Set Version 1.0 (March 2000) (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

(ii) CDC Race and Ethnicity Code Set Version 1.2 (July 08, 2021) (incorporated by reference, see § 170.299).

* * * * *

(m) * * *

(1) *Standard.* The Unified Code of Units of Measure, Revision 1.9 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

* * * * *

(n) * * *

(1) *Standard.* Birth sex must be coded in accordance with HL7® Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference, see § 170.299), up until the adoption of this standard expires January 1, 2026, attributed as follows:

* * * * *

(2) *Standard.* Sex must be coded in accordance with, at a minimum, at least one of the versions of SNOMED CT® codes specified in paragraph (a) of this section.

(3) *Standard.* Sex for Clinical Use must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section.

(o) *Sexual orientation and gender information*—(1) *Standard.* Sexual orientation must be coded in accordance with, at a minimum, at least one of the versions of SNOMED–CT® U.S. Edition codes specified in paragraph (a) of this section for paragraphs (o)(1)(i) through (iii) of this section and HL7 Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference, see § 170.299), up until the adoption of this standard expires on January 1, 2026, for paragraphs (o)(1)(iv) through (vi) of this section, attributed as follows:

(i) *Lesbian, gay, or homosexual.* 38628009

(ii) *Straight or heterosexual.* 20430005

(iii) *Bisexual.* 42035005

(iv) *Something else, please describe.* NullFlavor OTH

(v) *Don't know.* NullFlavor UNK

(vi) *Choose not to disclose.* NullFlavor ASKU

(2) *Standard.* Gender identity must be coded in accordance with, at a minimum, at least one of the versions of SNOMED–CT® U.S. Edition codes specified in paragraph (a) of this section for paragraphs (o)(2)(i) through (v) of this section and HL7® Version 3 Standard, Value Sets for AdministrativeGender and NullFlavor (incorporated by reference in § 170.299), up until the adoption of this standard expires January 1, 2026, for paragraphs (o)(2)(vi) and (vii) of this section, attributed as follows:

(i) *Male.* 446151000124109

(ii) *Female.* 446141000124107

(iii) *Female-to-Male (FTM)/Transgender Male/Trans Man.* 407377005

(iv) *Male-to-Female (MTF)/Transgender Female/Trans Woman.* 407376001

(v) *Genderqueer, neither exclusively male nor female.* 446131000124102

(vi) *Additional gender category or other, please specify.* NullFlavor OTH

(vii) *Choose not to disclose.* NullFlavor ASKU

(3) *Standard.* Sexual Orientation and Gender Identity must be coded in accordance with, at a minimum, the at least one of the versions of SNOMED CT® U.S. Edition codes specified in paragraph (a) of this section.

(4) *Standard.* Pronouns must be coded in accordance with, at a minimum, at least one of the versions of LOINC codes specified in paragraph (c) of this section.

(p) *Social, psychological, and behavioral data*—(1) *Financial resource strain.* Financial resource strain must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with the LOINC® code 76513–1 and LOINC® answer list ID LL3266–5.

(2) *Education.* Education must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with LOINC® code 63504–5 and LOINC® answer list ID LL1069–5.

(3) *Stress.* Stress must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with the LOINC® code 76542–0 and LOINC® answer list LL3267–3.

(4) *Depression.* Depression must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with LOINC® codes 55757–9, 44250–9 (with LOINC® answer list ID LL361–7), 44255–8 (with LOINC® answer list ID LL361–7), and 55758–7 (with the answer coded with the associated applicable unit of measure in at least one of the versions of the standard specified in paragraph (m) of this section).

(5) *Physical activity.* Physical activity must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with LOINC® codes 68515–6 and 68516–4. The answers must be coded with the associated applicable unit of measure in at least one of the versions of the standard specified in paragraph (m) of this section.

(6) *Alcohol use.* Alcohol use must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with LOINC® codes 72109–2, 68518–0 (with LOINC® answer list ID LL2179–1), 68519–8 (with LOINC® answer list ID LL2180–9), 68520–6 (with LOINC® answer list ID LL2181–7), and 75626–2 (with the answer coded with the associated applicable unit of measure in at least one of the versions of the

standard specified in § paragraph (m) of this section).

(7) *Social connection and isolation.* Social connection and isolation must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with the LOINC® codes 76506–5, 63503–7 (with LOINC answer list ID LL1068–7), 76508–1 (with the associated applicable unit of measure in the standard specified in § 170.207(m)(2)), 76509–9 (with the associated applicable unit of measure in at least one of the versions of the standard specified in paragraph (m) of this section), 76510–7 (with the associated applicable unit of measure in at least one of the versions of the standard specified in paragraph (m)), 76511–5 (with LOINC answer list ID LL963–0), and 76512–3 (with the associated applicable unit of measure in at least one of the versions of the standard specified in paragraph (m) of this section).

(8) *Exposure to violence (intimate partner violence).* Exposure to violence: Intimate partner violence must be coded in accordance with, at a minimum, at least one of the versions of LOINC® codes specified in paragraph (c) of this section and attributed with the LOINC® code 76499–3, 76500–8 (with LOINC® answer list ID LL963–0), 76501–6 (with LOINC® answer list ID LL963–0), 76502–4 (with LOINC® answer list ID LL963–0), 76503–2 (with LOINC® answer list ID LL963–0), and 76504–0 (with the associated applicable unit of measure in at least one of the versions of the standard specified in paragraph (m) of this section).

* * * * *

(r) * * *

(1) *Standard.* Crosswalk: Medicare Provider/Supplier to Healthcare Provider Taxonomy, April 2, 2015 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

* * * * *

(s) * * *

(1) *Standard.* Public Health Data Standards Consortium Source of Payment Typology Code Set Version 5.0 (October 2011) (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

* * * * *

■ 6. Amend § 170.210 by revising paragraph (a)(2), adding paragraph (a)(3), and removing and reserving paragraph (f) to read as follows:

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

* * * * *

(a) * * *

(2) *General.* Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2, October 8, 2014 (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2026.

(3) *General.* Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2, October 12, 2021 (incorporated by reference in § 170.299).

* * * * *

■ 7. Amend § 170.213 by revising paragraph (b) and adding paragraph (c) to read as follows:

§ 170.213 United States Core Data for Interoperability.

* * * * *

(b) *Standard.* United States Core Data for Interoperability (USCDI) Version 3 (v3), October 2022 Errata, (incorporated by reference in § 170.299). The adoption of this standard expires on January 1, 2028.

(c) *Standard.* United States Core Data for Interoperability (USCDI) Version 4 (v4), October 2023 Errata, (incorporated by reference in § 170.299).

■ 8. Amend § 170.215 by:

■ a. Revising paragraph (b)(1)(ii);

■ b. Adding paragraphs (b)(1)(iii) and (b)(2);

■ c. Revising paragraphs (c)(1) and (2);

■ d. Adding paragraph (c)(3);

■ e. Revising paragraphs (d)(1); and

■ f. Adding paragraphs (d)(2) and (f) through (o).

The revisions and additions read as follows:

§ 170.215 Application Programming Interface Standards.

* * * * *

(b) * * *

(1) * * *

(ii) *Implementation specification.* HL7® FHIR® US Core Implementation Guide STU 6.1.0 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(iii) *Implementation specification.* HL7 FHIR® US Core Implementation Guide, Version 7.0.0—STU7, (incorporated by reference, see § 170.299).

(2) *Implementation specification.* HL7 FHIR® US Public Health Profiles Library Implementation Guide. US Public Health Profiles Library 1.0.0—STU1 (incorporated by reference in § 170.299).

(c) * * *

(1) *Implementation specification.* HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2026.

(2) *Implementation specification.* HL7® SMART App Launch Implementation Guide Release 2.0.0 (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(3) *Implementation specification.* HL7® SMART App Launch Implementation Guide Release 2.2.0—STU 2.2 (incorporated by reference, see § 170.299).

(d) * * *

(1) *Implementation specification.* HL7® FHIR® Bulk Data Access (Flat FHIR) (v1.0.0—STU 1) (incorporated by reference, see § 170.299). The adoption of this standard expires on January 1, 2028.

(2) *Implementation specification.* HL7® FHIR® Bulk Data Access IG 2.0.0—STU 2, (incorporated by reference, see § 170.299).

* * * * *

(f) *API-based workflow triggers.* The following are applicable for purposes of initiating calls to decision support services or initiating interactions that can be presented to users synchronously in their workflows.

(1) *Implementation specification.* HL7® CDS Hooks Release 2.0 (incorporated by reference in § 170.299).

(2) [Reserved]

(g) *Verifiable health records.* The following are applicable for purposes of issuing verifiable and sharable health information and health records.

(1) *SMART Health Cards Framework*—(i) *Implementation specification.* HL7® FHIR® SMART Health Cards Framework version 1.4.0 (incorporated by reference in § 170.299).

(ii) [Reserved]

(2) *Vaccination and Testing*—(i) *Implementation specification.* SMART Health Cards: Vaccination and Testing Implementation Guide Version 1.0.0—STU 1 (incorporated by reference in § 170.299).

(ii) [Reserved]

(h) *API-based event notifications.* The following are applicable for the purposes of supporting proactive notifications from a server to a client when new information has been added or existing information has been updated.

(1) *FHIR Subscriptions: Implementation specification.* HL7® FHIR® Subscriptions R5 Backport Implementation Guide Version 1.1.0—Standard for Trial Use (incorporated by reference in § 170.299).

(2) [Reserved]

(i) [Reserved]

(j) *Prior authorization*—(1) *Coverage requirements discovery*—(i) *Implementation specification.* HL7 FHIR® Da Vinci—Coverage Requirements Discovery (CRD) Implementation Guide, Version 2.0.1—STU 2 (incorporated by reference in § 170.299).

(ii) [Reserved]

(2) *Prior authorization documentation*—(i) *Implementation specification.* HL7 FHIR® Da Vinci—Documentation Templates and Rules (DTR) Implementation Guide: Version 2.0.1—STU 2 (incorporated by reference in § 170.299).

(ii) [Reserved]

(3) *Prior authorization submission*—(i) *Implementation specification.* HL7 FHIR Da Vinci—Prior Authorization Support (PAS) FHIR Implementation Guide: Version 2.0.1—STU 2 (incorporated by reference in § 170.299).

(ii) [Reserved]

(k) *Payer data exchange*—(1) *Blue button*—(i) *Implementation specification.* HL7 FHIR Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) Implementation Guide: Version 2.0.0—STU 2 (incorporated by reference in § 170.299).

(ii) [Reserved]

(2) *Payer data exchange*—(i) *Implementation specification.* HL7 FHIR® Da Vinci Payer Data Exchange (PDex) Implementation Guide: Version 2.0.0 STU—2.0.0 (incorporated by reference in § 170.299).

(ii) [Reserved]

(l) [Reserved]

(m) *Drug formulary*—(1) *Implementation specification.* HL7 FHIR® Da Vinci—Payer Data Exchange (PDex) US Drug Formulary Implementation Guide, Version 2.0.1—STU2 (incorporated by reference in § 170.299).

(2) [Reserved]

(n) *Directory information*—(1) *Implementation specification.* HL7 FHIR® Da Vinci payer Data Exchange (PDex) Plan Net Implementation Guide: Version 1.1.0—STU1.1 US (incorporated by reference in § 170.299).

(2) [Reserved]

(o) *API functions using digital certificates.* The following is applicable for purposes of API functions secured using digital certificates, including dynamic client registration.

(1) *Implementation specification.* HL7 FHIR® Unified Data Access Profiles (UDAP™) Security for Scalable Registration, Authentication, and Authorization Implementation Guide Release 1.0.0—STU 1 US (incorporated by reference in § 170.299).

(2) [Reserved]

■ 9. Amend § 170.299 by:

■ a. Revising paragraphs (d)(14) and (15);

■ b. Adding paragraph (d)(20);

■ c. Revising paragraphs (e)(4) and (5);

■ d. Redesignating paragraphs (f) through (s) as paragraphs (g) through (t), respectively;

■ e. Adding new paragraph (f);

■ f. Revising newly redesignated paragraphs (h)(14) and (20);

■ h. Removing and reserving newly redesignated paragraphs (h)(21) and (24);

■ i. Adding paragraphs (h)(41) through (64);

■ j. Adding paragraphs (m)(3) and (5), and (n)(7);

■ k. Revising newly redesignated paragraph (q)(7); and

■ l. Adding paragraphs (s)(10) and (11).

The revisions and additions read as follows:

§ 170.299 Incorporation by reference.

* * * * *

(d) * * *

(14) CDC National Center of Immunization and Respiratory Diseases (NCIRD) Code Set (CVX)—Vaccines Administered, updates through September 29, 2023, IBR approved for § 170.207(e).

(15) National Drug Code Directory (NDC)—Vaccine NDC Linker, updates through November 6, 2023, IBR approved for § 170.207(e).

* * * * *

(20) HL7 Version 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5, 2018 Update, IBR approved for § 170.205(e).

(e) * * *

(4) CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting, Implementation Guide for 2024, Version 1.1, August 31, 2023, IBR approved for § 170.205(h).

(5) CMS Implementation Guide for Quality Reporting Document Architecture Category III, Eligible Clinicians Programs, Implementation Guide for 2024, Version 1.1, November 22, 2023, IBR approved for § 170.205(k).

* * * * *

(f) Computational Health Informatics Program, Boston Children's Hospital, 300 Longwood Avenue Boston, MA 02115, phone: (617) 355–6000, website: *https://www.childrenshospital.org/research/programs/computational-health-informatics-program-research.*

(1) SMART Health Cards Framework version 1.4.0, June 15, 2023, IBR approved for § 170.215(g).

(2) [Reserved]

* * * * *

(h) * * *

(14) HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture (QRDA III), Release 1—US Realm (ANSI/HL7 Normative Release 1), September 2021, IBR approved for § 170.205(k).

* * * * *

(20) HL7 CDA® R2 Implementation Guide: Quality Reporting Document Architecture—Category I (QRDA I)—US Realm, STU 5.3 with errata, December 2022, IBR approved for § 170.205(h).

* * * * *

(41) HL7 FHIR® Da Vinci—Coverage Requirements Discovery (CRD) Implementation Guide, Version 2.0.1—STU 2, January 8, 2024, IBR approved for § 170.215(j).

(42) HL7 FHIR® Da Vinci—Documentation Templates and Rules (DTR) FHIR Implementation Guide, Version 2.0.1—STU 2, January 11, 2024, IBR approved for § 170.215(j).

(43) HL7 FHIR® Da Vinci—Prior Authorization Support (PAS) FHIR Implementation Guide, Version 2.0.1—STU 2, December 1, 2023, IBR approved for § 170.215(j).

(44) HL7 FHIR® Consumer Directed Payer Data Exchange (CARIN IG for Blue Button®) Implementation Guide, Version 2.0.0—STU 2, November 28, 2022, IBR approved for § 170.215(k).

(45) HL7 FHIR® Da Vinci Payer Data Exchange (PDex) Implementation Guide, Version 2.0.0—STU 2, January 6, 2024, IBR approved for § 170.215(k).

(46) HL7 FHIR® Da Vinci—Payer Data Exchange (PDex) US Drug Formulary Implementation Guide, Version 2.0.1—STU2, December 1, 2023, IBR approved for § 170.215(m).

(47) HL7 FHIR® Da Vinci Payer Data Exchange (PDex) Plan Net Implementation Guide, Version 1.1.0—STU1.1 US, April 4, 2022, IBR approved for § 170.215(n).

(48) HL7 FHIR® Bulk Data Access IG 2.0.0—STU 2, November 26, 2021, IBR approved for § 170.215(d).

(49) HL7 FHIR® US Public Health Profiles Library Implementation Guide. US Public Health Profiles Library 1.0.0—STU1, October 4, 2023, IBR approved for § 170.215(b).

(50) HL7 FHIR® Subscriptions R5 Backport Implementation Guide Version 1.1.0—Standard for Trial Use, January 11, 2022, IBR approved for § 170.215(h).

(51) HL7® CDS Hooks Release 2.0, August 23, 2022, IBR approved for § 170.215(f).

(52) HL7 Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1—US Realm Standard for Trial Use, July 2019, IBR approved for § 170.205(d).

(53) HL7 Version 2.5.1 Implementation Guide: Laboratory Orders (LOI) from EHR, Release 1, STU Release 4—US Realm, December 3, 2013, IBR approved for § 170.205(g).

(54) HL7 Version 2.5.1 Implementation Guide: Laboratory Results Interface (LRI), Release 1 STU Release 4—US Realm, July 16, 2012, IBR approved for § 170.205(g).

(55) HL7 FHIR® Central Cancer Registry Reporting Content IG, 1.0.0—STU 1, December 21, 2023, IBR approved for § 170.205(i).

(56) HL7 FHIR® Cancer Pathology Data Sharing, 1.0.0—STU1, August 18, 2023, IBR approved for § 170.205(i).

(57) HL7 CDA® R2 Implementation Guide: Healthcare Associated Infection (HAI) Reports, Release 3—US Realm, December 2, 2020. IBR approved for § 170.205(r)(2).

(58) HL7 CDA® R2 Implementation Guide: National Health Care Surveys (NHCS), R1 STU Release 3.1—US Realm, January 6, 2022, IBR approved for § 170.205(s).

(59) HL7 FHIR® Vital Records Birth and Fetal Death Reporting 1.1.0—STU 1.1, October 10, 2023, IBR approved for § 170.205(v).

(60) HL7 FHIR® SMART Health Cards: Vaccination and Testing Implementation Guide Version 1.0.0—STU 1 Release, December 27, 2023, IBR approved for § 170.215(g).

(61) HL7 FHIR® SMART App Launch Implementation Guide, Release 2.2.0—STU 2.2, April 30, 2024, IBR approved for § 170.215(c).

(62) HL7 FHIR® Unified Data Access Profiles (UDAP™) Security for Scalable Registration, Authentication, and Authorization Implementation Guide, Release 1.0.0—STU 1 US, September 27, 2022, IBR approved for § 170.215(o).

(63) HL7 FHIR® US Core Implementation Guide, Version 7.0.0—STU7, May 8, 2024, IBR approved for § 170.215(b).

(64) HL7 CDA® R2 Implementation Guide: Consolidated CDA (C–CDA) Templates for Clinical Notes, Edition 3—US Realm (C–CDA Edition 3), May 18, 2024, IBR approved for § 170.205(a).

* * * * *

(m) * * *

(3) Annex A: Federal Information Processing Standards (FIPS) Publication 140–2, Security Requirements for Cryptographic Modules, October 8, 2014, IBR approved for § 170.210(a).

* * * * *

(5) Annex A: A Federal Information Processing Standards (FIPS) Publication 140–2, Security Requirements for Cryptographic Modules, October 12, 2021, IBR approved for § 170.210(a).

(n) * * *

(7) United States Core Data for Interoperability (USCDI), Version 4 (v4), October 2023 Errata, IBR approved for § 170.213(c).

* * * * *

(q) * * *

(7) Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.76, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc., September 18, 2023, IBR approved for § 170.207(c).

(s) * * *

(10) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), U.S. Edition, September 2023 Release, IBR approved for § 170.207(a).

(11) RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, December 4, 2023, Full Monthly Release, IBR approved for § 170.207(d).

* * * * *

■ 10. Amend § 170.315 by:

■ a. Revising and republishing paragraphs (a) and (b);

■ b. Revising paragraph (c)(4)(iii);

■ c. Revising and republishing paragraphs (d) through (g); and

■ d. Adding paragraph (j).

The revisions, republications, and addition read as follows:

§ 170.315. ONC Certification Criteria for Health IT.

* * * * *

(a) *Clinical*—(1) *Computerized provider order entry—medications.* (i) Enable a user to record, change, and access medication orders.

(ii) *Optional.* Include a ''reason for order'' field.

(2) *Computerized provider order entry—laboratory.* For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (a)(2)(i) of this section, or the requirements specified in paragraph (a)(2)(ii) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph (a)(2)(ii) of this section.

(i) Enable a user to record, change, and access laboratory orders—the Health IT Module may include a ''reason for order'' field; or

(ii) Enable a user to:

(A) Record, change, and access laboratory orders—the Health IT Module may include a ''reason for order'' field;

(B) Create and transmit laboratory orders electronically according to the standard specified in § 170.205(g)(2); and

(C) Receive and validate laboratory results according to the standard specific in § 170.205(g)(3).

(3) *Computerized provider order entry—diagnostic imaging.* (i) Enable a user to record, change, and access diagnostic imaging orders.

(ii) *Optional.* Include a ''reason for order'' field.

(4) *Drug-drug, drug-allergy interaction checks for CPOE*—(i) *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.

(ii) *Adjustments.* (A) Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.

(B) Limit the ability to adjust severity levels in at least one of these two ways:

(*1*) To a specific set of identified users.

(*2*) As a system administrative function.

(5) *Patient demographics and observations.* (i) Enable a user to record, change, and access patient demographic and observations data including race, ethnicity, preferred language, sex, sex parameter for clinical use, sexual orientation, gender identity, name to use, pronouns, and date of birth.

(A) *Race and ethnicity.* (*1*) Enable each one of a patient's races to be recorded in accordance with, at a minimum, at least one of the standards specified in § 170.207(f)(2) and whether a patient declines to specify race.

(*2*) Enable each one of a patient's ethnicities to be recorded in accordance with, at a minimum, at least one of the standards specified in § 170.207(f)(2) and whether a patient declines to specify ethnicity.

(*3*) Aggregate each one of the patient's races and ethnicities recorded in accordance with paragraphs (a)(5)(i)(A)(*1*) and (*2*) of this section to the categories in at least one of the standards specified in § 170.207(f)(1).

(B) *Preferred language.* Enable preferred language to be recorded in accordance with the standard specified in § 170.207(g)(2) and whether a patient declines to specify a preferred language.

(C) *Sex.* Enable sex to be recorded in accordance with the standard specified in § 170.207(n)(1) for the period up to and including December 31, 2025; or § 170.207(n)(2).

(D) *Sexual orientation.* Enable sexual orientation to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(1) for the period up to and including December 31, 2025; or § 170.207(o)(3), as well as whether a patient declines to specify sexual orientation.

(E) *Gender identity.* Enable gender identity to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(2) for the period up to and including December 31, 2025; or § 170.207(o)(3), as well as whether a patient declines to specify gender identity.

(F) *Sex parameter for clinical use.* Enable at least one sex parameter for clinical use to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(n)(3). Conformance with paragraph (a)(5)(i)(F) of this section is required by January 1, 2026.

(G) *Name to use.* Enable at least one preferred name to use to be recorded. Conformance with paragraph (a)(5)(i)(G) of this section is required by January 1, 2026.

(H) *Pronouns.* Enable at least one pronoun to be recorded in accordance with, at a minimum, the version of the standard specified in § 170.207(o)(4). Conformance with paragraph (a)(5)(i)(H) of this section is required by January 1, 2026.

(ii) *Inpatient setting only.* Enable a user to record, change, and access the preliminary cause of death and date of death in the event of mortality.

(6)–(8) [Reserved]

(9) *Clinical decision support (CDS)*— (i) *CDS intervention interaction.* Interventions provided to a user must occur when a user is interacting with technology.

(ii) *CDS configuration.* (A) Enable interventions and reference resources specified in paragraphs (a)(9)(iii) and (iv) of this section to be configured by a limited set of identified users (*e.g.,* system administrator) based on a user's role.

(B) Enable interventions:

(*1*) Based on the following data:

(*i*) Problem list;

(*ii*) Medication list;

(*iii*) Allergy and intolerance list;

(*iv*) At least one demographic specified in paragraph (a)(5)(i) of this section;

(*v*) Laboratory tests; and

(*vi*) Vital signs.

(*2*) When a patient's medications, allergies and intolerance, and problems are incorporated from a transition of care/referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(iii) *Evidence-based decision support interventions.* Enable a limited set of identified users to select (*i.e.,* activate) electronic CDS interventions (in addition to drug-drug and drug-allergy contraindication checking) based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(*1*)(*i*) through (*vi*) of this section.

(iv) *Linked referential CDS.* (A) Identify for a user diagnostic and therapeutic reference information in accordance at least one of the following standards and implementation specifications:

(*1*) The standard and implementation specifications specified in § 170.204(b)(3).

(*2*) The standard and implementation specifications specified in § 170.204(b)(4).

(B) For paragraph (a)(9)(iv)(A) of this section, technology must be able to identify for a user diagnostic or therapeutic reference information based on each one and at least one combination of the data referenced in paragraphs (a)(9)(ii)(B)(*1*)(*i*), (*ii*), and (*iv*) of this section.

(v) *Source attributes.* Enable a user to review the attributes as indicated for all CDS resources:

(A) For evidence-based decision support interventions under paragraph (a)(9)(iii) of this section:

(*1*) Bibliographic citation of the intervention (clinical research/guideline);

(*2*) Developer of the intervention (translation from clinical research/guideline);

(*3*) Funding source of the intervention development technical implementation; and

(*4*) Release and, if applicable, revision date(s) of the intervention or reference source.

(B) For linked referential CDS in paragraph (a)(9)(iv) of this section and drug-drug, drug-allergy interaction checks in paragraph (a)(4) of this section, the developer of the intervention, and where clinically indicated, the bibliographic citation of the intervention (clinical research/guideline).

(vi) *Expiration of criterion.* The adoption of this criterion for purposes of the ONC Health IT Certification Program expires on January 1, 2025.

(10)–(11) [Reserved]

(12) *Family health history.* Enable a user to record, change, and access a patient's family health history in accordance with the familial concepts or expressions included in, at a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a).

(13) [Reserved]

(14) *Implantable device list.* (i) Record Unique Device Identifiers associated with a patient's Implantable Devices.

(ii) Parse the following identifiers from a Unique Device Identifier:

(A) Device Identifier; and

(B) The following identifiers that compose the Production Identifier:

(*1*) The lot or batch within which a device was manufactured;

(*2*) The serial number of a specific device;

(*3*) The expiration date of a specific device;

(*4*) The date a specific device was manufactured; and

(*5*) For an HCT/P regulated as a device, the distinct identification code required by 21 CFR 1271.290(c).

(iii) Obtain and associate with each Unique Device Identifier:

(A) A description of the implantable device referenced by at least one of the following:

(*1*) The ''GMDN PT Name'' attribute associated with the Device Identifier in the Global Unique Device Identification Database.

(*2*) The ''SNOMED CT® Description'' mapped to the attribute referenced in paragraph (a)(14)(iii)(A)(*1*) of this section.

(B) The following Global Unique Device Identification Database attributes:

(*1*) ''Brand Name'';

(*2*) ''Version or Model'';

(*3*) ''Company Name'';

(*4*) ''What MRI safety information does the labeling contain?''; and

(*5*) ''Device required to be labeled as containing natural rubber latex or dry natural rubber (21 CFR 801.437).''

(iv) Display to a user an implantable device list consisting of:

(A) The active Unique Device Identifiers recorded for the patient;

(B) For each active Unique Device Identifier recorded for a patient, the description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section; and

(C) A method to access all Unique Device Identifiers recorded for a patient.

(v) For each Unique Device Identifier recorded for a patient, enable a user to access:

(A) The Unique Device Identifier;

(B) The description of the implantable device specified by paragraph (a)(14)(iii)(A) of this section;

(C) The identifiers associated with the Unique Device Identifier, as specified by paragraph (a)(14)(ii) of this section; and

(D) The attributes associated with the Unique Device Identifier, as specified by paragraph (a)(14)(iii)(B) of this section.

(vi) Enable a user to change the status of a Unique Device Identifier recorded for a patient.

(15) *Social, psychological, and behavioral data.* Enable a user to record, change, and access the following patient social, psychological, and behavioral data:

(i) *Financial resource strain.* Enable financial resource strain to be recorded in accordance with the standard specified in § 170.207(p)(1) and whether a patient declines to specify financial resource strain.

(ii) *Education.* Enable education to be recorded in accordance with the standard specified in § 170.207(p)(2) and whether a patient declines to specify education.

(iii) *Stress.* Enable stress to be recorded in accordance with the standard specified in § 170.207(p)(3) and whether a patient declines to specify stress.

(iv) *Depression.* Enable depression to be recorded in accordance with the standard specified in § 170.207(p)(4) and whether a patient declines to specify depression.

(v) *Physical activity.* Enable physical activity to be recorded in accordance with the standard specified in § 170.207(p)(5) and whether a patient declines to specify physical activity.

(vi) *Alcohol use.* Enable alcohol use to be recorded in accordance with the standard specified in § 170.207(p)(6) and whether a patient declines to specify alcohol use.

(vii) *Social connection and isolation.* Enable social connection and isolation to be recorded in accordance the standard specified in § 170.207(p)(7) and whether a patient declines to specify social connection and isolation.

(viii) *Exposure to violence (intimate partner violence).* Enable exposure to violence (intimate partner violence) to be recorded in accordance with the standard specified in § 170.207(p)(8) and whether a patient declines to specify exposure to violence (intimate partner violence).

(b) *Care coordination*—(1) *Transitions of care*—(i) *Send and receive via edge protocol.* (A) Send transition of care/referral summaries through a method that conforms to the standard specified in § 170.202(d) and that leads to such summaries being processed by a service that has implemented the standard specified in § 170.202(a)(2); and

(B) Receive transition of care/referral summaries through a method that conforms to the standard specified in § 170.202(d) from a service that has implemented the standard specified in § 170.202(a)(2).

(C) *XDM processing.* Receive and make available the contents of a XDM package formatted in accordance with the standard adopted in § 170.205(p)(1) when the technology is also being certified using an SMTP-based edge protocol.

(ii) *Validate and display*—(A) *Validate C–CDA conformance—system performance.* Demonstrate the ability to detect valid and invalid transition of care/referral summaries received and formatted in accordance with the standards specified in § 170.205(a)(3) through (5) for the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates. This includes the ability to:

(*1*) Parse each of the document types.

(*2*) Detect errors in corresponding ''document-templates,'' ''section-templates,'' and ''entry-templates,'' including invalid vocabulary standards and codes not specified in the standards adopted in § 170.205(a)(3) through (5).

(*3*) Identify valid document-templates and process the data elements required in the corresponding section-templates and entry-templates from the standards adopted in § 170.205(a)(3) through (5).

(*4*) Correctly interpret empty sections and null combinations.

(*5*) Record errors encountered and allow a user through at least one of the following ways to:

(*i*) Be notified of the errors produced.

(*ii*) Review the errors produced.

(B) *Display.* Display in human readable format the data included in transition of care/referral summaries received and formatted according to the standards specified in § 170.205(a)(3) through (5).

(C) *Display section views.* Allow for the individual display of each section (and the accompanying document header information) that is included in a transition of care/referral summary received and formatted in accordance with the standards adopted in § 170.205(a)(3) through (5) in a manner that enables the user to:

(*1*) Directly display only the data within a particular section;

(*2*) Set a preference for the display order of specific sections; and

(*3*) Set the initial quantity of sections to be displayed.

(iii) *Create.* Enable a user to create a transition of care/referral summary formatted in accordance with the standard specified in § 170.205(a)(3) through (5) using the Continuity of Care Document, Referral Note, and (inpatient setting only) Discharge Summary document templates that includes, at a minimum:

(A) *USCDI.* (*1*) The data classes expressed in the standards in § 170.213 and in accordance with § 170.205(a)(4) and (5) and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section for the time period up to and including December 31, 2025, or

(*2*) The data classes expressed in the standards in § 170.213 and in accordance with § 170.205(a)(4) and (6) and paragraphs (b)(1)(iii)(A)(*3*)(*i*) through (*iii*) of this section, 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).

(B) *Encounter diagnoses.* Formatted according to at least one of the following standards:

(*1*) The standard specified in § 170.207(i).

(*2*) At a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a).

(C) *Additional data.* Cognitive status.

(D) *Additional data.* Functional status.

(E) *Ambulatory setting only.* The reason for referral; and referring or transitioning provider's name and office contact information.

(F) *Inpatient setting only.* Discharge instructions.

(G) *Patient matching data.* First name, last name, previous name, middle name (including middle initial), suffix, date of birth, current address, phone number, and sex. The following constraints apply:

(*1*) *Date of birth constraint*—(*i*) *Year, month, and day.* The year, month and day of birth must be present for a date of birth. The technology must include a null value when the date of birth is unknown.

(*ii*) *Optional.* When the hour, minute, and second are associated with a date of birth the technology must demonstrate that the correct time zone offset is included.

(*2*) *Phone number constraint.* Represent phone number (home, business, cell) in accordance with the standards adopted in § 170.207(q)(1). All phone numbers must be included when multiple phone numbers are present.

(*3*) *Sex constraint.* Represent sex with at least one of the versions of the standards adopted in § 170.207(n).

(H) On and after January 1, 2028, imaging links.

(2) *Clinical Information Reconciliation and Incorporation*—For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements in paragraphs (b)(2)(i), (ii), (iii) and (vii) of this section; or the requirements in paragraphs (b)(2)(iv), (v), (vi) and (vii) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements in paragraphs (b)(2)(iv), (v), (vi) and (vii).

(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, for time period up to and including December 31, 2025; or in accordance with the standards adopted in § 170.205(a)(3), (4), and (6).

(ii) *Correct patient.* Upon receipt of a transition of care/referral summary formatted according to the standards adopted § 170.205(a)(3) through (5) for the period up to and including December 31, 2025; or according to the standards adopted § 170.205(a)(3), (4), and (6), 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 standards:

(*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) *General requirements.* Upon receipt of a transition of care/referral summary formatted in accordance with the standards adopted in § 170.205(a)(3), (4), and (6), a Health IT Module must demonstrate that the transition of care/referral summary received can be properly matched to the correct patient according to the standards adopted in § 170.205(a)(3), (4), and (6), enable a user to reconcile and incorporate by default each data element in at least one of the versions of the USCDI standard specified in § 170.213 according to paragraph (b)(2)(v) of this section, and execute all reconciliation and incorporation rules that are enabled and/or configured by an organization within their deployed technology according to paragraph (b)(2)(vi) of this section.

(v) *User reconciliation.* Enable a user to reconcile data as follows. For each data element included in at least one of the versions of the USCDI standard in § 170.213:

(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 date.

(B) Enable a user to create a single reconciled list of each of the data.

(C) Enable a user to review and validate the accuracy of a final set of data.

(D) Upon a user's confirmation, automatically update and incorporate the data.

(vi) *User configuration.* Enable a user to set individual or organizational rules that allow automatic reconciliation and incorporation for each of the data classes included in at least one of the versions of the USCDI standard specified in § 170.213, including functionality that allows the user to select trusted data and trusted sources for automatic reconciliation and incorporation.

(vii) *System verification.* Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to:

(A) The standard specified in § 170.205(a)(4) using the Continuity of Care Document template and,

(B) The standard(s) specified in § 170.205(a)(5) for the time period up to and including December 31, 2025; or § 170.205(a)(6).

(3) *Electronic prescribing.* (i) [Reserved]

(ii) For technology certified subsequent to June 30, 2020:

(A) For the time period up to and including December 31, 2027, enable a user to perform the following prescription-related electronic transactions in accordance with the standards specified in § 170.205(b)(1) or (2); at least one of the versions of the standard adopted in § 170.207(d)(1); and the standard adopted in § 170.207(d)(2) if using the standard in § 170.205(b)(2). On and after January 1, 2028, enable a user to perform the following prescription-related electronic transactions in accordance with the standards specified in § 170.205(b)(2) and (d)(1) and (2).

(*1*) 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*) [Reserved]

(*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).

(*10*) Electronic prior authorization transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse, PANotification). These transactions are required if using the standard in 170.205(b)(2).

(B) Enable a user to exchange race and ethnicity information when performing the following prescription-related electronic transactions, if using the standard in § 170.205(b)(2):

(*1*) Receive fill status notifications (RxFill).

(*2*) Request and respond to change prescriptions (RxChangeRequest, RxChangeResponse).

(*3*) Request to cancel prescriptions (CancelRx).

(*4)* Request and respond to renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(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) 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) [Reserved]

(vii) Electronic prior authorization (ePA) transactions (PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse and PACancelRequest, PACancelResponse, PANotification). These transactions are required if using the standard in § 170.205(b)(2).

(*2*) [Reserved]

(D) Enable a user to enter, receive, and transmit structured and codified prescribing instructions in accordance with the standard specified in § 170.205(b)(2). This section is only required if using the standard in § 170.205(b)(2).

(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.

(G) On and after January 1, 2028, meet the requirements specified in paragraph (d)(13)(ii) of this section for user-facing authentication.

(4) *Real-time prescription benefit*—(i) *Send and receive information.* Enable a user to perform the following transactions using the XML format in accordance with at least one of the versions of the standards adopted in both §§ 170.205(c) and 170.207(d)(1), and the standard in § 170.207(d)(2) as follows:

(A) Enable a user to request patient-specific prescription benefit information, estimated cost information, and therapeutic alternatives, in accordance with the RTPBRequest transaction.

(B) Enable a user to receive patient-specific prescription benefit information, estimated cost information, and therapeutic alternatives in response to a request, in accordance with the RTPBResponse transaction.

(C) Enable a user to be notified of errors when there is a problem with a real-time prescription benefit transaction, in accordance with the RTPBError transaction.

(ii) *Display.* Display to a user in human readable format patient-specific prescription benefit information, estimated cost information, and therapeutic alternatives, in accordance with at least one of the versions of the standard adopted in § 170.205(c).

(iii) *Scope.* The scope of this criterion is limited to medications and vaccines covered by a pharmacy benefit.

(5)–(6) [Reserved]

(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 document, section, and entry (data element) level.

(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 document, section, and entry (data element) level; 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) for the time period up to and including December 31, 2025; or § 170.205(a)(6).

(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) Except as specified in paragraph (b)(10)(i)(F) of this section, 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).

(F) A Health IT Module that acts primarily as an intermediary between systems and, through integration, functions without any direct human interaction need not meet the requirement in paragraph (b)(10)(i)(B) of this section, and may satisfy this criterion through a developer-assisted process provided that:

(*1*) The EHI that the Health IT Module stores or that the Health IT Module causes to be stored is a copy, whether in the same or another format, of EHI also stored by another Health IT Module with which the Health IT Module is integrated; and

(*2*) The developer has not received more than 10 requests for a single patient EHI export from that Health IT Module during the immediately preceding calendar year.

(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.

(11) *Decision support interventions*—(i) *Decision support intervention interaction.* Interventions provided to a user must occur when a user is interacting with technology.

(ii) *Decision support configuration.* (A) Enable interventions specified in paragraphs (b)(11)(iii) of this section to be configured by a limited set of identified users based on a user's role.

(B) Enable interventions when a patient's medications, allergies and intolerance, and problems are incorporated from a transition of care or referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(C) Enable a user to provide electronic feedback data for evidence-based decision support interventions selected via the capability provided in paragraph (b)(11)(iii)(A) of this section and make available such feedback data to a limited set of identified users for export, in a computable format, including at a minimum the intervention, action taken, user feedback provided (if applicable), user, date, and location.

(iii) *Decision support intervention selection.* Enable a limited set of identified users to select (*i.e.,* activate) electronic decision support interventions (in addition to drug-drug and drug-allergy contraindication checking) that are:

(A) Evidence-based decision support interventions and use any data based on the following data expressed in the standards in § 170.213:

(*1*) Problems;

(*2*) Medications;

(*3*) Allergies and Intolerances;

(*4*) At least one demographic specified in paragraph (a)(5)(i) of this section;

(*5*) Laboratory;

(*6*) Vital Signs;

(*7*) Unique Device Identifier(s) for a Patient's Implantable Device(s); and

(*8*) Procedures.

(B) Predictive Decision Support Interventions and use any data expressed in the standards in § 170.213.

(iv) *Source attributes.* Source attributes listed in paragraphs (b)(11)(iv)(A) and (B) of this section must be supported.

(A) For evidence-based decision support interventions:

(*1*) Bibliographic citation of the intervention (clinical research or guideline);

(*2*) Developer of the intervention (translation from clinical research or guideline);

(*3*) Funding source of the technical implementation for the intervention(s) development;

(*4*) Release and, if applicable, revision dates of the intervention or reference source;

(*5*) Use of race as expressed in the standards in § 170.213;

(*6*) Use of ethnicity as expressed in the standards in § 170.213;

(*7*) Use of language as expressed in the standards in § 170.213;

(*8*) Use of sexual orientation as expressed in the standards in § 170.213;

(*9*) Use of gender identity as expressed in the standards in § 170.213;

(*10*) Use of sex as expressed in the standards in § 170.213;

(*11*) Use of date of birth as expressed in the standards in § 170.213;

(*12*) Use of social determinants of health data as expressed in the standards in § 170.213; and

(*13*) Use of health status assessments data as expressed in the standards in § 170.213.

(B) For Predictive Decision Support Interventions:

(*1*) Details and output of the intervention, including:

(*i*) Name and contact information for the intervention developer;

(*ii*) Funding source of the technical implementation for the intervention(s) development;

(*iii*) Description of value that the intervention produces as an output; and

(*iv*) Whether the intervention output is a prediction, classification, recommendation, evaluation, analysis, or other type of output.

(*2*) Purpose of the intervention, including:

(*i*) Intended use of the intervention;

(*ii*) Intended patient population(s) for the intervention's use;

(*iii*) Intended user(s); and

(*iv*) Intended decision-making role for which the intervention was designed to be used/for (*e.g.,* informs, augments, replaces clinical management).

(*3*) Cautioned out-of-scope use of the intervention, including:

(*i*) Description of tasks, situations, or populations where a user is cautioned against applying the intervention; and

(*ii*) Known risks, inappropriate settings, inappropriate uses, or known limitations.

(*4*) Intervention development details and input features, including at a minimum:

(*i*) Exclusion and inclusion criteria that influenced the training data set;

(*ii*) Use of variables in paragraphs (b)(11)(iv)(A)(*5*) through (*13*) of this section as input features;

(*iii*) Description of demographic representativeness according to variables in paragraphs (b)(11)(iv)(A)(*5*) through (*13*) of this section including, at a minimum, those used as input features in the intervention;

(*iv*) Description of relevance of training data to intended deployed setting; and

(*5*) Process used to ensure fairness in development of the intervention, including:

(*i*) Description of the approach the intervention developer has taken to ensure that the intervention's output is fair; and

(*ii*) Description of approaches to manage, reduce, or eliminate bias.

(*6*) External validation process, including:

(*i*) Description of the data source, clinical setting, or environment where an intervention's validity and fairness has been assessed, other than the source of training and testing data

(*ii*) Party that conducted the external testing;

(*iii*) Description of demographic representativeness of external data according to variables in paragraph (b)(11)(iv)(A)(*5*) through (*13*) including, at a minimum, those used as input features in the intervention; and

(*iv*) Description of external validation process.

(*7*) Quantitative measures of performance, including:

(*i*) Validity of intervention in test data derived from the same source as the initial training data;

(*ii*) Fairness of intervention in test data derived from the same source as the initial training data;

(*iii*) Validity of intervention in data external to or from a different source than the initial training data;

(*iv*) Fairness of intervention in data external to or from a different source than the initial training data;

(*v*) References to evaluation of use of the intervention on outcomes, including, bibliographic citations or hyperlinks to evaluations of how well the intervention reduced morbidity, mortality, length of stay, or other outcomes;

(*8*) Ongoing maintenance of intervention implementation and use, including:

(*i*) Description of process and frequency by which the intervention's validity is monitored over time;

(*ii*) Validity of intervention in local data;

(*iii*) Description of the process and frequency by which the intervention's fairness is monitored over time;

(*iv*) Fairness of intervention in local data; and

(*9*) Update and continued validation or fairness assessment schedule, including:

(*i*) Description of process and frequency by which the intervention is updated; and

(*ii*) Description of frequency by which the intervention's performance is corrected when risks related to validity and fairness are identified.

(v) *Source attribute access and modification*—(A) *Access.* (*1*) For evidence-based decision support interventions and Predictive Decision Support Interventions supplied by the health IT developer as part of its Health IT Module, the Health IT Module must enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information specified in paragraphs (b)(11)(iv)(A) and (B) of this section.

(*2*) For Predictive Decision Support Interventions supplied by the health IT developer as part of its Health IT Module, the Health IT Module must indicate when information is not available for review for source attributes in paragraphs (b)(11)(iv)(B)(*6*), (b)(11)(iv)(B)(*7*)(*iii*) through (*v*), (b)(11)(iv)(B)(*8*)(*ii*) and (*iv*), and (b)(11)(iv)(B)(*9*) of this section.

(B) *Modify.* (*1*) For evidence-based decision support interventions and Predictive Decision Support

Interventions, the Health IT Module must enable a limited set of identified users to record, change, and access source attributes in paragraphs (b)(11)(iv)(A) and (B) of this section.

(*2*) For Predictive Decision Support Interventions, the Health IT Module must enable a limited set of identified users to record, change, and access additional source attributes not specified in paragraph (b)(11)(iv)(B) of this section.

(vi) *Intervention risk management.* Intervention risk management practices must be applied for each Predictive Decision Support Intervention supplied by the health IT developer as part of its Health IT Module.

(A) *Risk analysis.* The Predictive Decision Support Intervention(s) must be subject to analysis of potential risks and adverse impacts associated with the following characteristics: validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy.

(B) *Risk mitigation.* The Predictive Decision Support Intervention (s) must be subject to practices to mitigate risks, identified in accordance with paragraph (b)(11)(vi)(A) of this section; and

(C) *Governance.* The Predictive Decision Support Intervention(s) must be subject to policies and implemented controls for governance, including how data are acquired, managed, and used.

(c) * * *

(4) * * *

(iii) *Data.* (A) Taxpayer Identification Number.

(B) National Provider Identifier.

(C) Provider type in accordance with, at a minimum, at least one of the versions of the standard specified in § 170.207(r).

(D) Practice site address.

(E) Patient insurance in accordance with at least one of the versions of the standard specified in § 170.207(s).

(F) Patient age.

(G) Patient sex in accordance with the at least one of the versions of the standard specified in § 170.207(n).

(H) Patient race and ethnicity in accordance with, at a minimum, at least one of the versions of the standard specified in § 170.207(f)(1) and at least one of the versions of the standard specified in § 170.207(f)(2).

(I) Patient problem list data in accordance with, at a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a).

* * * * *

(d) *Privacy and security*—(1) *Authentication, access control, and authorization.* (i) Verify against a unique identifier(s) (*e.g.,* username or number) that a user seeking access to electronic health information is the one claimed; and

(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

(2) *Auditable events and tamper-resistance*—(i) *Record actions.* Technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1);

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

(ii) *Default setting.* Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) and (C) of this section.

(iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users.

(iv) *Audit log protection.* Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology.

(v) *Detection.* Technology must be able to detect whether the audit log has been altered.

(3) *Audit report(s).* Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in § 170.210(e).

(4) *Amendments.* Enable a user to select the record affected by a patient's request for amendment and perform the capabilities specified in paragraph (d)(4)(i) or (ii) of this section.

(i) *Accepted amendment.* For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location.

(ii) *Denied amendment.* For a denied amendment, at a minimum, append the request and denial of the request in at least one of the following ways:

(A) To the affected record.

(B) Include a link that indicates this information's location.

(5) *Automatic access time-out.* (i) Automatically stop user access to health information after a predetermined period of inactivity.

(ii) Require user authentication in order to resume or regain the access that was stopped.

(6) *Emergency access.* Permit an identified set of users to access electronic health information during an emergency.

(7) *Health IT encryption.* For the time period up to and including December 31, 2025, a Health IT Module must meet the requirements in paragraphs (d)(7)(i), (iv), and (v) of this section or meet the requirements in (d)(7)(ii), (iii), (iv), and (v) of this section. On and after January 1, 2026, a Health IT Module must meet the requirements in (d)(7)(ii), (iii), (iv), and (v).

(i) *End-user device encryption of electronic health information.* The requirements specified in either paragraph (d)(7)(i)(A) or (B) of this section must be met.

(A) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(B) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

(ii) *End-user device encryption of personally identifiable information.* The requirements specified in either paragraph (d)(7)(ii)(A) or (B) of this section must be met.

(A) Technology that is designed to locally store personally identifiable information on end-user devices must encrypt the personally identifiable information.

(B) Technology is designed to prevent personally identifiable information from being locally stored on end-user devices after use of the technology on those devices stops.

(iii) *Server encryption.* Technology that is designed to store personally identifiable information must encrypt the stored personally identifiable information after use of the technology on those servers stops.

(iv) *Encryption standard.* Information that is encrypted to meet paragraph (d)(7)(i)(A), (d)(7)(ii)(A), or (d)(7)(iii) of

this section must be encrypted in accordance with at least one version of the standard specified in § 170.210(a).

(v) *Default settings.* (A) Technology that is designed to meet paragraph (d)(7)(i)(A), (d)(7)(ii)(A), or (d)(7)(iii) of this section must be set by default to perform those capabilities.

(B) Unless the default configurations for the capabilities defined in paragraphs (d)(7)(i)(A), (d)(7)(ii)(A), and (d)(7)(iii) of this section cannot be disabled by any user, the ability to change these configurations must be restricted to a limited set of identified users.

(8) *Integrity.* (i) Create a message digest in accordance with the standard specified in § 170.210(c)(2).

(ii) Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

(9) *Trusted connection.* Establish a trusted connection using one of the following methods:

(i) *Message-level.* Encrypt and integrity protect message contents in accordance with at least one version of the standard specified in § 170.210(a) and the standard specified in § 170.210(c)(2).

(ii) *Transport-level.* Use a trusted connection in accordance with at least one version of the standard specified in § 170.210(a) and the standard specified in § 170.210(c)(2).

(10) *Auditing actions on health information.* (i) By default, be set to record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1).

(ii) If technology permits auditing to be disabled, the ability to do so must be restricted to a limited set of users.

(iii) Actions recorded related to electronic health information must not be capable of being changed, overwritten, or deleted by the technology.

(iv) Technology must be able to detect whether the audit log has been altered.

(11) *Accounting of disclosures.* Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).

(12) *Protect stored authentication credentials.* For the time period up to and including December 31, 2025, a Health IT Module must meet either the requirements specified in (d)(12)(i) or (ii) of this section. On and after January 1, 2026, a Health IT Module must meet the requirements in (d)(12)(ii) of this section.

(i) Health IT developers must make one of the following attestations and may provide the specified accompanying information where applicable:

(A) Yes—the Health IT Module encrypts stored authentication credentials in accordance with at least one of the standards adopted in § 170.210(a).

(B) 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.

(ii) A Health IT Module designed to store authentication credentials must protect the confidentiality and integrity of its stored authentication credentials according to at least one of the following standards:

(A) Encryption and decryption in accordance with at least one of the standards specified in § 170.210(a).

(B) Hashing in accordance with the standard specified in § 170.210(c)(2).

(13) *Multi-factor authentication.* For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements in paragraph (d)(13)(i) or (ii) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph (d)(13)(ii).

(i) Health IT developers must make one of the following attestations and, as applicable, provide the specified accompanying information:

(A) 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.

(B) 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 identity with the use of industry-recognized standards.

(ii) Using industry recognized standards, the Health IT Module must:

(A) Support authentication, through multiple elements, of the user's identity.

(B) Enable a user to configure, enable, and disable the multi-factor authentication capabilities defined in paragraphs (d)(13)(ii) introductory text and (d)(13)(ii)(A) of this section.

(e) *Patient engagement*—(1) *View, download, and transmit to 3rd party.* (i) Patients (and their authorized representatives) must be able to use internet-based technology to view, download, and transmit their health information to a 3rd party in the manner specified below. Such access must be consistent and in accordance with the standard adopted in § 170.204(a)(1) and may alternatively be demonstrated in accordance with the standard specified in § 170.204(a)(2).

(A) *View.* Patients (and their authorized representatives) must be able to use health IT to view, at a minimum, the following data:

(*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 (5) and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section for the time period up to and including December 31, 2025, or

(*2*) 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 (6) and paragraphs (e)(1)(i)(A)(*3*)(*i*) through (*iii*) of this section.

(*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).

(*8*) *Diagnostic Images.* On and after January 1, 2028, support for both diagnostic quality images and reduced quality images.

(B) *Download.* (*1*) Patients (and their authorized representatives) must be able to use technology to download an ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) in the following formats:

(*i*) Human readable format; and

(*ii*) The format specified in accordance with the standard specified in § 170.205(a)(4) and (5) for the time period up to and including December 31, 2025, or § 170.205(a)(4) and (6), and following the CCD document template.

(*2*) When downloaded according to the standard specified in § 170.205(a)(4) through (6) following the CCD document template, the ambulatory summary or inpatient summary must include, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set):

(i) Ambulatory setting only. All of the data specified in paragraphs (e)(1)(i)(A)(*1*), (*2*), (*4*), and (*5*) of this section, and, on and after January 1, 2028, an imaging link to the data specified in paragraph (e)(1)(i)(A)(*8*) of this section.

(ii) Inpatient setting only. All of the data specified in paragraphs (e)(1)(i)(A)(*1*) and (*3*) through (5) of this section, and, on and after January 1, 2028, an imaging link to the data specified in paragraph (e)(1)(i)(A)(*8*) of this section.

(*3*) Inpatient setting only: Patients (and their authorized representatives) must be able to download transition of care/referral summaries that were created as a result of a transition of care (pursuant to the capability expressed in the certification criterion specified in paragraph (b)(1) of this section).

(*4*) On and after January 1, 2028, patients (and their authorized representatives) must be able to use technology to download both diagnostic quality and reduced quality images.

(C) *Transmit to third party.* Patients (and their authorized representatives) must be able to:

(*1*) Transmit the ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) created in paragraph (e)(1)(i)(B)(*2*) of this section in accordance with both of the following ways:

(*i*) Email transmission to any email address; and

(*ii*) An encrypted method of electronic transmission.

(*2*) Inpatient setting only: Transmit transition of care/referral summaries (as a result of a transition of care/referral as referenced by (e)(1)(i)(B)(*3*) of this section) selected by the patient (or their authorized representative) in both of the ways referenced (e)(1)(i)(C)(*1*)(*i*) and (*ii*) of this section).

(D) *Timeframe selection.* With respect to the data available to view, download, and transmit as referenced paragraphs (e)(1)(i)(A) through (C) of this section, patients (and their authorized representatives) must be able to:

(*1*) Select data associated with a specific date (to be viewed, downloaded, or transmitted); and

(*2*) Select data within an identified date range (to be viewed, downloaded, or transmitted).

(ii) *Activity history log.* (A) When any of the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section are used, the following information must be recorded and made accessible to the patient (or his/her authorized representative):

(*1*) The action(s) (*i.e.,* view, download, transmission) that occurred;

(*2*) The date and time each action occurred in accordance with the standard specified in § 170.210(g);

(*3*) The user who took the action; and

(*4*) Where applicable, the addressee to whom an ambulatory summary or inpatient summary was transmitted.

(B) [Reserved]

(iii) *Multi-factor authentication.* On and after January 1, 2028, meet the requirements specified in § 170.315(d)(13)(ii) for patient facing authentication.

(2) [Reserved]

(3) *Patient health information capture.* Enable a user to:

(i) Identify, record, and access information directly and electronically shared by a patient (or authorized representative).

(ii) Reference and link to patient health information documents.

(f) *Public health*—(1) *Immunization registries—bi-directional exchange.* For the time period up to and including December 31, 2026, a Health IT Module must meet either the requirements specified in paragraph (f)(1)(i) or in paragraphs (f)(1)(ii) and (iii) of this section. On and after January 1, 2027, a Health IT Module must meet the requirements specified in paragraphs (f)(1)(ii) and (iii) of this section.

(i) Create immunization information for electronic transmission in accordance with paragraphs (f)(1)(i)(A) through (C) of this section and enable a user to request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with the standard in § 170.205(e)(4).

(A) The standard and applicable implementation specifications specified in § 170.205(e)(4).

(B) At a minimum, the version of the standard specified in § 170.207(e)(5) for historical vaccines.

(C) At a minimum, the version of the standard specified in § 170.207(e)(6) for administered vaccines.

(ii) Enable a user to engage in bi-directional immunization information exchange including to:

(A) Create immunization information for electronic transmission and support request, access, and display in accordance with the standards in paragraphs (f)(1)(ii)(A)(*1*) through (*3*) of this section;

(*1*) At least one of the versions of the standard and applicable implementation specifications specified in § 170.205(e).

(*2*) At a minimum, the version of the standard specified in § 170.207(e)(5) for historical vaccines.

(*3*) At a minimum, the version of the standard specified in § 170.207(e)(6) for administered vaccines.

(B) Request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with at least one of the versions of the standard in § 170.205(e); and

(C) Receive incoming patient-level immunization-specific query or request from external systems and respond in accordance with paragraph (f)(1)(ii)(A) of this section.

(iii) Receive incoming patient-level immunization-specific query or request from external systems and respond.

(2) *Syndromic surveillance—Transmission to public health agencies.* Create syndrome-based public health surveillance information for electronic transmission in accordance with at least one of the versions of the standards (and applicable implementation specifications) specified in § 170.205(d).

(3) *Reportable laboratory results—Transmission to public health agencies—and Laboratory Orders—Receive and validate.* For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (f)(3)(i) or (ii) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph (f)(3)(ii) of this section.

(i) Create reportable laboratory tests and values/results for electronic

transmission in accordance with paragraphs (f)(3)(i)(A) and (B) of this section.

(A) At least one of the standards specified in § 170.205(g).

(B) At a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a), at least one of the versions of LOINC specified in § 170.207(c), and at least one of the versions of the Unified Code for Units of Measure standard specified in § 170.207(m).

(ii) Create and transmit reportable laboratory values/results and receive and validate reportable laboratory orders in accordance with paragraphs (f)(3)(ii)(A) through (C) of this section.

(A) Create and transmit reportable laboratory information according to at least one of the standards specified in § 170.205(g).

(B) Receive laboratory test orders formatted in accordance with the standard specified in § 170.205(g)(2) and validate conformance. That is, demonstrate the ability to detect valid and invalid electronic reportable laboratory orders received and formatted in accordance with the standard specified in § 170.205(g)(2). The Health IT Module must include the capability to:

(*1*) Identify valid electronic reportable laboratory orders received and process the data elements required for the standard specified in § 170.205(g)(2).

(*2*) Correctly interpret empty sections and null combinations;

(*3*) Detect errors in laboratory information received including invalid vocabulary standards and codes not specified in the standard specified in § 170.205(g)(2);

(*4*) Record errors encountered and allow a user through at least one method to:

(*i*) Be notified of the errors produced;

(*ii*) Review the errors produced; and,

(*iii*) Store or maintain error records for audit or other follow up action.

(*5*) *Parse and filter.* Enable a user to parse and filter electronic laboratory test orders validated in accordance with paragraph (f)(3)(ii) of this section at a minimum for any data element identified as ''mandatory'' or ''must support'' in the Public Health Profile within the IG according to the standard specified in § 170.205(g)(3).

(C) Create reportable laboratory test values/results for electronic transmission in accordance with the Public Health Profile within the standard specified in § 170.205(g)(3), and, at a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a), at least one of the LOINC standard versions specified in § 170.207(c), and at least one of the versions of the Unified Code for Units of Measure standard specified in § 170.207(m).

(4) *Cancer registry reporting—transmission to public health agencies.* For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (f)(4)(i) or the requirements specified in paragraph (f)(4)(ii) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph (f)(4)(ii) of this section.

(i) Create cancer case information for electronic transmission in accordance with paragraphs (f)(4)(i)(A) and (B) of this section.

(A) The standard (and applicable implementation specifications) specified in § 170.205(i)(2).

(B) At a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a) and at least one of the LOINC standard versions specified in § 170.207(c).

(ii) Create cancer case information for electronic transmission in accordance with either paragraph (i)(A) or (B) of this section; and in accordance with paragraph (i)(C) of this section.

(A) The ''Central Cancer Registry Reporting Bundle'' and accompanying profiles according to the standard specified in § 170.205(i)(3). All data elements indicated as ''mandatory'' and ''must support'' within the IG by the standards and implementation specifications must be supported. Including support for the requirements described in the ''Central Cancer Registry Reporting EHR Capability Statement.''

(B) The standard (and applicable implementation specifications) specified in § 170.205(i)(2) and, at a minimum, at least one of the versions of SNOMED CT U.S. Edition specified in § 170.207(a) and at least one of the LOINC standard versions specified in § 170.207(c).

(C) The ''US Pathology Exchange Bundle'' and accompanying profiles according to the implementation specification adopted in § 170.205(i)(4). All data elements indicated as ''mandatory'' and ''must support'' within the IG by the standards and implementation specifications must be supported. Including support for the requirements described in the ''Central Cancer Registry Reporting Pathology EHR Capability Statement.''

(5) *Electronic case reporting—transmission to public health agencies.* Enable a user to create a case report for electronic transmission meeting the requirements described in paragraphs (f)(5)(i) of this section for the time period up to and including December 31, 2025; or the requirements described in paragraph (f)(5)(ii) of this section.

(i) *Functional electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:

(A) Consume and maintain a table of trigger codes to determine which encounters may be reportable.

(B) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

(C) Create a case report for electronic transmission:

(*1*) Based on a matched trigger from paragraph (f)(5)(i)(B).

(*2*) That includes, at a minimum:

(*i*) The data classes expressed in the standards in § 170.213.

(*ii*) Encounter diagnoses formatted according to at least one of the standards specified in § 170.207(i) or (a)(1).

(*iii*) The provider's name, office contact information, and reason for visit.

(*iv*) An identifier representing the row and version of the trigger table that triggered the case report.

(ii) *Standards-based electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:

(A) Consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4).

(B) Create a case report consistent with at least one of the following standards:

(*1*) The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1); or

(*2*) For the period up to and including December 31, 2027, the HL7 CDA eICR IG in § 170.205(t)(2). Adoption of the CDA-based standard in § 170.205(t)(2) expires on January 1, 2028.

(C) Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in paragraph (f)(5)(ii)(B) of this section.

(D) Transmit a case report electronically to a system capable of receiving a case report.

(6) *Antimicrobial use and resistance reporting—transmission to public health agencies.* Create antimicrobial use and resistance reporting information for electronic transmission in accordance

with at least one of the versions of the standard specified in § 170.205(r).

(7) *Health care surveys—transmission to public health agencies.* Create health care survey information for electronic transmission in accordance with at least one of the versions of the standard specified in § 170.205(s).

(8) *Birth reporting—Transmission to public health agencies*—(i) *Live birth.* Create provider live birth report for electronic transmission in accordance with the standard specified in § 170.205(v).

(9) *Prescription Drug Monitoring Program (PDMP) databases—query, receive, validate, parse, and filter: Functional requirement.* Enable a user to query a PDMP, including bi-directional interstate exchange, to receive PDMP data in an interoperable manner, to establish access roles in accordance with applicable law, and to maintain records of access and auditable events as follows.

(i) *Query.* Enable both passive and active bi-directional query of a PDMP, including an interstate exchange query, in accordance with paragraphs (f)(9)(i)(A) through (C) of this section.

(A) Initiate a passive or automated query of an applicable PDMP, including an interstate exchange query:

(*1*) Upon the recording, change, or access of a medication order;

(*2*) Upon the creation and transmission of an electronic prescription for a controlled substance; and

(*3*) Upon entry of controlled substance medication data into a medication list or reconciliation of a medication list including controlled substance medication data.

(B) Enable an active or user-initiated query of a PDMP including an interstate exchange query.

(C) Send an acknowledgement message in response to receipt of data after a query is performed.

(ii) *Receive, validate, parse, and filter.* Enable a user to receive, validate, parse, and filter electronic PDMP information in accordance with paragraphs (f)(9)(ii)(A) through (C) of this section.

(A) *Receive.* At a minimum, receive electronic controlled substance medication prescription information transmitted in accordance with (f)(9)(ii)(A)(*1*) through (*3*) of this section. As an alternative to enabling such receipt via paragraph (f)(9)(ii)(A)(*1*) through (*3*), receipt may also be optionally enabled through paragraph (f)(9)(ii)(A)(*4*) of this section:

(*1*) Receive through a method that conforms to the standard in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2);

(*2*) Receive through a method that conforms to the standard in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol; and

(*3*) Receive via an application programming interface in accordance with the standard specified in § 170.215(a)(1).

(*4*) Optional: receive through a connection governed by the Trusted Exchange Framework and Common Agreement.

(B) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic controlled substance medication prescription information received. The Health IT Module must include the capability to:

(*1*) Identify valid electronic controlled substance medication prescription information received and process the data elements including any necessary data mapping to at least one of the versions of the USCDI standard in § 170.213 to enable use as discrete data elements, aggregation with other data, incorporation into a patient medication list, and parsing and filtering in accordance with paragraph (f)(9)(ii)(C);

(*2*) Correctly interpret empty sections and null combinations;

(*3*) Detect errors in electronic controlled substance medication prescription information received including invalid vocabulary standards and data not represented using a vocabulary standard; and

(*4*) Record errors encountered and allow a user through at least one method to:

(*i*) Be notified of the errors produced;

(*ii*) Review the errors produced; and

(*iii*) Store or maintain error records for audit or other follow up action.

(C) *Parse and filter.* Enable a user to parse and filter electronic PDMP information received and validated in accordance with paragraph (f)(9)(ii)(B) at a minimum for any data element identified in at least one of the versions of the USCDI standard in § 170.213.

(iii) *Access controls.* Enable access controls including access roles and recording access including actions for auditable events and tamper-resistance in accordance with paragraphs (f)(9)(iii)(A) and (B) of this section.

(A) Enable access roles for providers and pharmacists and enable a user to customize additional roles for any delegate or surrogate under applicable law.

(B) Record access actions and maintain an audit log of actions.

(10)–(20) [Reserved]

(21) *Immunization information—receive, validate, parse, filter, and exchange—response.* Consistent with at least one of the versions of the standard and implementation specification specified in § 170.205(e), enable electronic immunization information to be received, validated, parsed, and filtered in accordance with paragraphs (f)(21)(i) through (iii) of this section and engage in exchange of immunization information in accordance with paragraph (f)(21)(iv) of this section.

(i) *Receive.* Receive electronic immunization information transmitted.

(A) *Required.* Through a method that conforms to Simple Object Access Protocol (SOAP)-based transport;

(B) *Optional.* (*1*) Receive through a connection governed by the Trusted Exchange Framework and Common Agreement;

(*2*) Through a method that conforms to the standard specified in § 170.205(p)(1) when the technology is also using a Simple Mail Transfer Protocol (SMTP)-based edge protocol; or

(*3*) Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic immunization information received and formatted in accordance with the standards specified in § 170.207(e)(5) and (6). The Health IT Module must include the capability to:

(A) Identify valid electronic immunization information received and process the data elements required for the standards specified in § 170.207(e)(5) and (6). Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with paragraph (f)(21)(iii) of this section;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in immunization information received including invalid vocabulary standards and codes not specified in the standards specified in § 170.207(e)(5) and (6); and

(D) Record errors encountered and allow a user through at least one method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filter immunization information received and validated in accordance with paragraph (f)(21)(ii) of

this section according to the standard specified in § 170.207(e)(5) or (6).

(iv) *Exchange—response.* Functional requirement. Respond to incoming patient-level queries from external systems—this includes providing immunization information as structured data.

(22) *Syndromic surveillance—receive, validate, parse, and filter.* Consistent with at least one of the versions of the standard(s) and implementation specification(s) specified in § 170.205(d), enable a user to receive, validate, parse and filter electronic syndrome-based public health surveillance information in accordance with paragraphs (f)(22)(i) through (iii) of this section.

(i) *Receive.* Receive electronic syndrome-based public health surveillance information transmitted:

(A) *Required.* Through a method that conforms to a Secure File Transfer Protocol (SFTP) connection.

(B) *Optional.* Receipt also may be supported:

(*1*) Receive through a connection governed by the Trusted Exchange Framework and Common Agreement; or

(*2*) Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic syndrome-based public health surveillance information received. The Health IT Module must include the capability to:

(A) Identify valid syndrome-based public health surveillance information received and process the data elements. Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with paragraph (f)(22)(iii) of this section;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in syndrome-based public health surveillance information received including invalid vocabulary standards and codes not specified; and

(D) Record errors encountered and allow a user through at least one method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filter electronic syndrome-based public health surveillance information received and validated in accordance with paragraph (f)(22)(ii) of this section.

(23) *Reportable laboratory test values/results—receive, validate, parse, and filter.* Consistent with at least one of the standard(s) and implementation specification(s) specified in § 170.205(g)(1) or the Public Health Profile within the implementation specification in § 170.205(g)(3), enable a user to receive, validate, parse and filter electronic reportable laboratory test values/results in accordance with paragraphs (f)(23)(i) through (iii) of this section.

(i) *Receive.* Receive electronic reportable laboratory test values/results transmitted:

(A) *Required.* (*1*) Through a method that conforms to the standard specified in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2); and

(*2*) Through a method that conforms to the standard in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol.

(B) *Optional.* (*1*) Receive through a connection governed by the Trusted Exchange Framework and Common Agreement℠; or

(*2*) Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic reportable laboratory test values/results received. The Health IT Module must include the capability to:

(A) Identify valid electronic reportable laboratory test values/results received and process the data elements. Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with paragraph (f)(23)(iii) of this section;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in electronic reportable laboratory test values/results received including invalid vocabulary standards and codes not specified; and

(D) Record errors encountered and allow a user through at least one method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filter electronic reportable laboratory test values/results received and validated in accordance with paragraph (f)(23)(ii) of this section.

(24) *Cancer pathology reporting—receive, validate, parse, and filter.* Consistent with the standard(s) and implementation specification(s) specified in § 170.205(i)(4), enable a user to receive, validate, parse and filter cancer pathology reports in accordance with paragraphs (f)(24)(i) through (iii) of this section.

(i) *Receive.* Receive electronic cancer pathology reports transmitted:

(A) *Required.* Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(B) *Optional.* Receive through a connection governed by the Trusted Exchange Framework and Common Agreement.

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic cancer pathology reports received. The Health IT Module must include the capability to:

(A) Identify valid electronic cancer pathology reports received and process the data elements. Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with paragraph (f)(24)(iii) of this section;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in electronic cancer pathology reports received including invalid vocabulary standards and codes not specified; and

(D) Record errors encountered and allow a user through at least one method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filter electronic reportable cancer pathology reports received and validated in accordance with paragraph (f)(24)(ii) of this section.

(25) *Electronic case reporting—receive, validate, parse, filter electronic initial case reports and reportability response; and create and transmit reportability response.* Consistent with at least one of the standard(s) and implementation specification(s) specified in § 170.205(t), enable a user to receive, validate, parse, and filter electronic case reporting information in accordance with paragraphs (f)(25)(i) through (iii) of this section, and to create and transmit a reportability response in accordance with paragraph (f)(25)(iv) of this section.

(i) *Receive.* Receive electronic case reporting information transmitted:

(A) *Required.* Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(B) *Optional.* (*1*) Receive through a connection governed by the Trusted Exchange Framework and Common Agreement;

(*2*) Through a method that conforms to the standard specified in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol.

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic case reporting information received. The Health IT Module must include the capability to:

(A) Identify valid electronic case reporting information received and process the data elements for, at a minimum, the data classes expressed in at least one of the versions of the USCDI standard specified in § 170.213. Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with paragraph (f)(25)(iii) of this section;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in electronic case reporting information received including invalid vocabulary standards and codes not specified; and

(D) Record errors encountered and allow a user through at least one method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filer electronic case reporting information received and validated in accordance with paragraph (f)(25)(ii) of this section, at a minimum, for any data element identified in at least one of the versions of the USCDI standard specified in § 170.213.

(iv) *Reportability response.* Enable a user to create a response in accordance with the HL7 eCR FHIR IG in § 170.205(t)(3) and transmit the response.

(26)–(27) [Reserved]

(28) *Birth reporting—receive, validate, parse, and filter.* Consistent with the standard(s) and implementation specification(s) specified in § 170.205(v), enable a user to receive, validate, parse, and filter birth reporting information in accordance with paragraphs (f)(28)(i) through (iii) of this section.

(i) *Receive.* Receive electronic birth reports transmitted:

(A) *Required.* Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(B) *Optional.* (*1*) Receive through a connection governed by the Trusted Exchange Framework and Common Agreement;

(*2*) Through a method that conforms to the standard specified in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2); or

(*3*) Through a method that conforms to the standard in § 170.205(p) when the technology is also using an SMTP-based edge protocol.

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic birth reports received. The Health IT Module must include the capability to:

(A) Identify valid electronic birth report received and process the data elements. Processing must include any necessary data mapping to enable use as discrete data elements, aggregation with other data, and parsing and filtering in accordance with paragraph (f)(28)(iii) of this section;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in electronic birth reports received including invalid vocabulary standards and codes not specified; and,

(D) Record errors encountered and allow a user through at least one method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filter electronic birth reports received and validated in accordance with paragraph (f)(28)(ii) of this section.

(29) *Prescription Drug Monitoring Program (PDMP) data—receive, validate, parse, filter prescription data, support query and exchange.* Enable a user to receive and validate electronic prescription information for controlled substance medications in accordance with paragraphs (f)(29)(i) through (ii), and support query of PDMP and exchange of PDMP data in accordance with paragraphs (f)(29)(iii) and (iv) of this section.

(i) *Receive.* Receive electronic prescription information for controlled substances transmitted:

(A) *Required.* (*1*) Through a method that conforms to the standard in § 170.202(d), from a service that has implemented the standard specified in § 170.202(a)(2);

(*2*) Through a method that conforms to the standard in § 170.205(p)(1) when the technology is also using an SMTP-based edge protocol; and

(*3*) Via an application programming interface in accordance with the standard specified in § 170.215(a)(1) or at least one of the versions of the standard specified in § 170.215(d).

(B) *Optional.* Receive through a connection governed by the Trusted Exchange Framework and Common Agreement.

(ii) *Validate conformance—system performance.* Demonstrate the ability to detect valid and invalid electronic controlled substance medication prescription information received. The Health IT Module must include the capability to:

(A) Identify valid electronic controlled substance medication prescription information received and process the data elements including any necessary data mapping or translation between standards;

(B) Correctly interpret empty sections and null combinations;

(C) Detect errors in electronic controlled substance medication prescription information received including invalid vocabulary standards and data not represented using a vocabulary standard; and,

(D) Record errors encountered and allow a user through at least on method to:

(*1*) Be notified of the errors produced;

(*2*) Review the errors produced; and,

(*3*) Store or maintain error records for audit or other follow up action.

(iii) *Parse and filter.* Enable a user to parse and filter electronic controlled substance medication prescription information received and validated in accordance with paragraph (f)(29)(ii) of this section.

(iv) *Query and exchange.* Enable patient-level queries from external systems of electronic controlled substance medication prescription information of the PDMP including an interstate exchange query in accordance with:

(A) *Exchange—response.* Respond to incoming patient-level queries from external system.

(B) *Exchange—patient access.* Enable patient access to view electronic controlled substance medication prescription information.

(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) *Safety-enhanced design.* (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) (until the certification criterion's expiration date), and (14) and (b)(2), (3), and (11) of this section.

(ii) *Number of test participants.* A minimum of 10 test participants must be used for the testing of each capability identified in paragraph (g)(3)(i) of this section.

(iii) One of the following must be submitted on the user-centered design processed used:

(A) Name, description, and citation (URL and/or publication citation) for an industry or Federal Government standard.

(B) Name the process(es), provide an outline of the process(es), a short description of the process(es), and an explanation of the reason(s) why use of any of the existing user-centered design standards was impractical.

(iv) The following information/sections from NISTIR 7742 must be submitted for each capability to which user-centered design processes were applied:

(A) Name and product version; date and location of the test; test environment; description of the intended users; and total number of participants;

(B) Description of participants, including: Sex; age; education; occupation/role; professional experience; computer experience; and product experience;

(C) Description of the user tasks that were tested and association of each task to corresponding certification criteria;

(D) The specific metrics captured during the testing of each user task performed in (g)(3)(iv)(C) of this section, which must include: Task success (%); task failures (%); task standard deviations (%); task performance time; and user satisfaction rating (based on a scale with 1 as very difficult and 5 as very easy) or an alternative acceptable user satisfaction measure;

(E) Test results for each task using the metrics identified above in paragraph (g)(3)(iv)(D) of this section; and

(F) Results and data analysis narrative, including: Major test finding; effectiveness; efficiency; satisfaction; and areas for improvement.

(v) Submit test scenarios used in summative usability testing.

(4) *Quality management system.* (i) For each capability that a technology includes and for which that capability's certification is sought, the use of a Quality Management System (QMS) in the development, testing, implementation, and maintenance of that capability must be identified that satisfies one of the following ways:

(A) The QMS used is established by the Federal government or a standards developing organization.

(B) The QMS used is mapped to one or more QMS established by the Federal government or standards developing organization(s).

(ii) When a single QMS was used for applicable capabilities, it would only need to be identified once.

(iii) When different QMS were applied to specific capabilities, each QMS applied would need to be identified.

(5) *Accessibility-centered design.* For each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or law in the development, testing, implementation and maintenance of that capability must be identified.

(i) When a single accessibility-centered design standard or law was used for applicable capabilities, it would only need to be identified once.

(ii) When different accessibility-centered design standards and laws were applied to specific capabilities, each accessibility-centered design standard or law applied would need to be identified. This would include the application of an accessibility-centered design standard or law to some capabilities and none to others.

(iii) When no accessibility-centered design standard or law was applied to all applicable capabilities such a response is acceptable to satisfy this certification criterion.

(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 standards in § 170.213 in accordance with § 170.205(a)(4) and (5) and paragraphs (g)(6)(i)(C)(*1*) through (*4*) of this section for the time period up to and including December 31, 2025; or

(B) The data classes expressed in the standards in § 170.213, and in accordance with § 170.205(a)(4) and (6) and paragraphs (g)(6)(i)(C)(*1*) through (*3*) of this section.

(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 paragraph (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 paragraph (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.

(7) *Application access—patient selection.* The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

(i) *Functional requirement.* The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

(ii) [Reserved]

(8) [Reserved]

(9) *Application access—all data request.* The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) *Functional requirements.* (A)(*1*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in at least one of the versions of the USCDI standard 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 (*v*) of this section for the time period up to and including December 31, 2025; or

(*2*) Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in at least one of the versions of the USCDI standard 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 (6) following the CCD document template, and as specified in paragraphs (g)(9)(i)(A)(3)(*i*) through (*v*) of this section.

(*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).

(*v*) *Imaging link.* On and after January 1, 2028, an imaging link.

(B) Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

(ii) [Reserved]

(10) *Standardized API for patient and population services.* Support the following capabilities to enable API-based access to EHI for patients, users, and systems:

(i) *Registration.* For the period up to and including December 31, 2027, enable apps to register with the Health IT Module's ''authorization server'' by meeting either the requirements specified in paragraph (g)(10)(i)(A) or both paragraphs (g)(10)(i)(A) and (B) of this section. On and after January 1, 2028, enable apps to register with the Health IT Module's ''authorization server'' by meeting the requirements specified in paragraphs (g)(10)(i)(A) and (B) of this section.

(A) *Functional registration.* Support functional registration for confidential and public apps according to the requirements in § 170.315(j)(1).

(B) *Dynamic registration.* Support dynamic registration for confidential apps according to the requirements in § 170.315(j)(2).

(ii) *Patient and user access*—(A) *Authentication and authorization for patient and user access*—(*1*) *Authentication and authorization for patient access*—(*i*) *SMART authentication and authorization for patient access.* Support authentication and authorization during the process of granting access to patient data to patients according to the requirements in paragraph (j)(9) of this section.

(*ii*) *Asymmetric certificate-based authentication for patient access.* For the period up to and including December 31, 2027, may support asymmetric certificate-based authentication according to the requirements in paragraph(j)(5) of this section for patient-facing apps dynamically registered using the capabilities in paragraph (g)(10)(i)(B) of this section. On and after January 1, 2028, must support asymmetric certificate-based authentication according to the requirements in paragraph (j)(5) of this section for patient-facing apps dynamically registered using the capabilities in paragraph (g)(10)(i)(B).

(*iii*) *Multi-factor authentication.* For the period up to and including December 31, 2027, may meet the requirements specified in paragraph (d)(13)(ii) of this section for patient-facing authentication. On and after January 1, 2028, must meet the requirements specified in paragraph (d)(13)(ii) for patient-facing authentication.

(*2*) *Authentication and authorization for user access*—(*i*) *SMART authentication and authorization for user access.* For the period up to and including December 31, 2027, support authentication and authorization during the process of granting access to patient data to users according to the requirements in paragraph (j)(10)(i) of this section and may also support user authorization revocation according to paragraph (j)(10)(ii) of this section. On and after January 1, 2028, must also support user authorization revocation according to paragraph (j)(10)(ii).

(*ii*) *Asymmetric certificate-based authentication for B2B user access.* For the period up to and including December 31, 2027, may also support asymmetric certificate-based authentication according to the requirements in paragraph (j)(11) of this section for user-facing apps dynamically registered using the capabilities in paragraph (g)(10)(i)(B) of this section. On and after January 1, 2028, must support asymmetric certificate-based authentication according to the requirements in paragraph (j)(11) for user-facing apps dynamically registered using the capabilities in paragraph (g)(10)(i)(B).

(B) *Information access.* Support the following methods to allow access to patient data for patient-facing apps and user-facing apps:

(*1*) *Read and search API.* Support read and search capabilities in one of the standards adopted in § 170.215(a) and support the ''US Core Server CapabilityStatement'' of the

corresponding implementation specification adopted in § 170.215(b)(1) for each of the data elements included in at least one of the versions of the USCDI standard adopted in § 170.213. Support for imaging links requests is optional. On and after January 1, 2028, requests for imaging links must be supported.

(*2*) *Verifiable health records.* For the period up to and including December 31, 2027, may also support the issuance of verifiable health records for vaccination status and infectious disease-related laboratory testing according to the requirements specified in paragraph (j)(22) of this section. On and after January 1, 2028, must support the issuance of verifiable health records for vaccination status and infectious disease-related laboratory testing according to the requirements specified in paragraph (j)(22).

(*3*) *Subscriptions.* For the period up to and including December 31, 2027, may also support subscriptions as a server for patient-facing apps and user-facing apps according to the requirements specified in paragraph (j)(23) of this section. On and after January 1, 2028, must support subscriptions as a server for patient-facing apps and user-facing apps according to the requirements specified in paragraph (j)(23).

(iii) *System access*—(A) *Authentication and authorization for system access*—(*1*) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization according to the requirements in paragraph (j)(7) of this section for system apps functionally registered using the capabilities in paragraph (g)(10)(i)(A) of this section.

(*2*) *Asymmetric certificate-based system authentication and authorization.* For the period up to and including December 31, 2027, may also support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) of this section for system apps dynamically registered using the capabilities in paragraph (g)(10)(i)(B) of this section. On and after January 1, 2028, must support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) for system apps dynamically registered using the capabilities in paragraph (g)(10)(i)(B).

(B) *Information access.* Support the following methods to allow access to patient data for system apps:

(*1*) *Read and search API.* Support read and search capabilities in one of the standards adopted in § 170.215(a) and support the ''US Core Server CapabilityStatement'' of the corresponding implementation specification adopted in § 170.215(b)(1) for each of the data included in at least one of the versions of the USCDI standard adopted in § 170.213. Support for imaging links requests is optional. On and after January 1, 2028, requests for imaging links must be supported.

(*2*) *Bulk FHIR API.* For the time period up to and including December 31, 2027, a Health IT Module must support read capabilities in at least one of the standards adopted in § 170.215(a), at least one of the implementation specifications adopted in § 170.215(b)(1), and at least one of the versions of the implementation specification adopted in § 170.215(d) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213. Support for imaging links requests is optional. On and after January 1, 2028, requests for imaging links must be supported. Additionally, for the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (g)(10)(iii)(B)(*2*)(*i*) or both paragraphs (g)(10)(iii)(B)(*2*)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraphs (g)(10)(iii)(B)(*2*)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

(*i*) The ''GroupLevelExport'' operation; and

(*ii*) The ''type'' query parameter for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213 and imaging links.

(*3*) *Subscriptions.* For the time period up to and including December 31, 2027, may support subscriptions as a server for system apps according to the requirements specified in paragraph (j)(23) of this section. On and after January 1, 2028, must support subscriptions as a server for system apps according to the requirements specified in paragraph (j)(23).

(iv) *Workflow triggers for decision support interventions.* For the time period up to and including December 31, 2027, may support workflow triggers for decision support interventions according to the requirements specified in paragraphs (j)(20) and (g)(10)(iv)(A) of this section. On and after January 1, 2028, support workflow triggers for decision support interventions by supporting the capabilities specified in paragraph (j)(20), including the following:

(A) *Workflow triggers.* Support the execution of decision support workflow triggers in accordance with the implementation specification in § 170.215(f)(1), including support for ''patient-view'' and ''order-sign'' hooks.

(B) [Reserved]

(11)–(19) [Reserved]

(20) *Standardized API for public health data exchange.* Support the following capabilities to enable API-based access, exchange, and use of EHI for public health purposes.

(i) *Registration.* Support the following registration capabilities to support the full scope of API capabilities in paragraph (g)(20) of this section:

(A) *Functional registration.* Support functional registration for confidential apps according to the requirements in paragraph (j)(1) of this section.

(B) *Dynamic registration.* Support dynamic registration for confidential apps according to the requirements in paragraph (j)(2) of this section.

(ii) *Authentication and authorization for system access*—(A) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization according to the requirements in paragraph (j)(7) of this section for system apps functionally registered using the capabilities in paragraph (g)(20)(i)(A) of this section.

(B) *Asymmetric certificate-based system authentication and authorization.* Support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) of this section for system apps dynamically registered using the capabilities in paragraph (g)(20)(i)(B) of this section.

(iii) *Public health information access*—(A) *Public Health Profiles.* Support the HL7 FHIR Profiles specified in the implementation specification in § 170.215(b)(2) for the following HL7 FHIR Resources:

(*1*) Condition;

(*2*) Encounter;

(*3*) Location;

(*4*) Observation;

(*5*) Organization;

(*6*) Patient;

(*7*) Practitioner role.

(B) *Information access.* Support the following methods to allow access to patient data:

(1) Read and search API—(*i*) *Read.* Support the ability for a system client to read HL7 FHIR Resources using the ''id'' data element for the HL7 FHIR Resources included in paragraph (g)(20)(iii)(A) of this section, and return

the information profiled according to the implementation specification in § 170.215(b)(2).

(*ii*) *Search.* Support the ability for a system client to search HL7 FHIR Resources according to the applicable search requirements in the ''US Core Server Capability Statement'' for the HL7 FHIR Resources included in paragraph (g)(20)(iii)(A) of this section and return the information profiled according to the implementation specification in § 170.215(b)(2).

(*2*) *Bulk FHIR API.* Support read and search capabilities in one of the standards and implementation specifications adopted in § 170.215(a) and at least one of the versions of the standard specified in § 170.215(d) for the HL7 FHIR Resources included in paragraph (g)(20)(iii)(A) of this section, and return the information profiled according to the implementation specification in § 170.215(b)(2). Additionally, for the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (g)(20)(iii)(B)(*2*)(*i*) of this section or both paragraphs (g)(20)(iii)(B)(*2*)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraphs (g)(20)(iii)(B)(*2*)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

(*i*) The ''GroupLevelExport'' operation; and

(*ii*) The ''_type'' query parameter for each of the data included in paragraph (g)(20)(iii)(A) of this section.

(C) *Subscriptions.* Support subscriptions according to the requirements in paragraph (j)(23) of this section, including:

(*1*) Support the ability for a client to subscribe to notifications filtered according to the conditions below and send notifications for the following event-based interactions according to the standard in § 170.215(a) and implementation specification in § 170.215(h)(1):

(*i*) When a patient encounter starts, filtered by ''Encounter.reasonCode'' and ''Encounter.subject'';

(*ii*) When a patient encounter ends, filtered by ''Encounter.reasonCode'' and ''Encounter.subject''.

(21)–(29) [Reserved]

(30) *Patient access API.* Support the following capabilities to enable patients to access health and administrative information.

(i) *Registration.* Support the following registration capabilities to support the full scope of API capabilities in paragraph (g)(30) of this section:

(A) *Functional registration.* Support functional registration for confidential and public apps according to the requirements included in paragraph (j)(1) of this section.

(B) *Dynamic registration.* Support dynamic registration for confidential apps according to the requirements in paragraph (j)(2) of this section.

(ii) *Authentication and authorization for patient access*—(A) *SMART authentication and authorization for patient access.* Support authentication and authorization during the process of granting access to patient data to patients according to the requirements in paragraph (j)(9) of this section.

(B) *Asymmetric certificate-based authentication for patient access.* Support asymmetric certificate-based authentication according to the requirements in paragraph (j)(5) of this section for patient-facing apps dynamically registered using the capabilities in paragraph (g)(30)(i)(B) of this section.

(C) *Multi-factor authentication.* On and after January 1, 2028, meet the requirements specified in paragraph (d)(13)(ii) of this section for patient facing authentication.

(iii) *Drug formulary API.* Publish information regarding the payer's drug formulary via a standardized API(s) according to at least one of the versions of the implementation specification adopted in § 170.215(m), including the requirements described in the ''US Drug Formulary Server Capability Statement.''

(A) *Authenticated API.* Provide support for the ''Authenticated API'' according to at least one of the versions of the implementation specification adopted in § 170.215(m) and requirements in paragraphs (g)(30)(i) and (ii) of this section.

(B) *Unauthenticated API.* Provide support for the ''Unauthenticated API'' according to at least one of the versions of the implementation specification adopted in § 170.215(m).

(iv) *Patient health information, coverage, and claims API*—(A) *Patient access to clinical and coverage information.* Allow patients to access and share clinical and coverage information via a standardized API(s) according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(*1*) Support the ability for patients to authenticate and share information with an application, service, or health plan according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2), including support for:

(*i*) The requirements associated with the ''Oauth2.0 or SMART-on-FHIR Member-authorized Exchange'' exchange method, including the requirements in the section ''OAuth2.0 and FHIR API.''

(*ii*) The requirements included in the ''PDEX Server Capability Statement'' and the HL7 FHIR Profiles, Resources, and operations included in Section 4.5.4 ''Capability Statement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(*iii*) The capabilities described in ''US Core Server Capability Statement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213.

(B) *Patient access to claims information.* Allow patients to access claims information via a standardized API(s) according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

(*1*) Support the ''Authentication and Authorization Requirements'' section of at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

(*2*) Support the requirements described in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specifications adopted in § 170.215(k)(1).

(31) *Provider access API—client.* Support the following capabilities to enable a provider to request and receive patient clinical and coverage information from a payer and receive and process the response.

(i) Support the ability to request patient history from a payer according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(ii) *API interactions.* Support the following API interactions as a client.

(A) *Read and search API*—(*1*) *Clinical and coverage information.* Support the ability to interact with a ''PDEX Server'' as a client, including support for all the corresponding client capabilities for requirements in the ''PDEX Server CapabilityStatement'' and the HL7 FHIR Profiles, Resources, and operations included in Section 4.5.4 ''CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(*2*) *Claims information.* Support all the corresponding client capabilities for requirements included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

(*3*) *USCDI and US Core.* The corresponding client capabilities described in ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213.

(B) *Bulk FHIR API.* Support the ability to request and receive information as a client according to at least one of the versions of the standard adopted in § 170.215(a) and at least one of the versions of the implementation specification adopted in § 170.215(d) for each of the data included in paragraph (g)(31)(ii)(A) of this section. Additionally, for the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (g)(31)(ii)(B)(*1*) of this section or both paragraphs (g)(31)(ii)(B)(*1*) and (*2*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraphs (g)(31)(ii)(B)(*1*) and (*2*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

(*1*) The ''GroupLevelExport'' operation; and

(*2*) The ''_type'' query parameter for each of the data included in paragraph (g)(31)(ii)(A) of this section.

(iii) *Information receipt.* Support the ability to receive, parse, and write patient health history, coverage, and claims information to the Health IT Module for:

(A) *Clinical and coverage information.* All HL7 FHIR Profiles and Resources included in the ''PDEX Server CapabilityStatement'' and the HL7 FHIR Profiles and Resources included in the Section 4.5.4 ''CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(B) *Claims information.* Claims information by supporting the information included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

(C) *USCDI and US Core.* The capabilities described in the ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213.

(32) *Provider access API—server.* Support the following capabilities to enable providers to request and receive patient health history and coverage information from payers.

(i) *Registration.* Support the following registration capabilities to support the full scope of API capabilities in paragraph (g)(32) of this section:

(A) Support functional registration for confidential apps according to the requirements included in paragraph (j)(1) of this section.

(B) Support dynamic registration for confidential apps according to the requirements in paragraph (j)(2) of this section.

(ii) *Authentication and authorization*—(A) *Authentication and authorization for user access.* Support the ability to authenticate and authorize an app during the process of granting access to patient data to users according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) and at least one implementation specification adopted in § 170.215(c).

(*1*) *Asymmetric certificate-based authentication for B2B user access.* Support asymmetric certificate-based authentication according to the requirements in paragraph (j)(11) of this section for user-facing apps dynamically registered using the capabilities in paragraph (g)(32)(i)(B) of this section.

(*2*) [Reserved]

(B) *Authentication and authorization for system access.* Support the ability to authenticate and authorize an app during the process of granting access to patient data to system apps according to at least one of the versions of the standard adopted in § 170.215(a) and at least one of the versions of the implementation specification adopted in § 170.215(d).

(*1*) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization according to the requirements in paragraph (j)(7) of this section for system apps functionally registered using the capabilities in paragraph (g)(32)(i)(A) of this section.

(*2*) *Asymmetric certificate-based system authentication and authorization.* Support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) of this section for system apps dynamically registered using the capabilities in paragraph (g)(32)(i)(B) of this section.

(iii) *Information access.* Support the following capabilities to allow a provider to request patient health and coverage information from a payer and to receive a response.

(A) *Request.* Support the ability for a client to request patient health history, coverage, and claims information according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(B) *Lookup.* Support the ability to identify patient clinical, coverage, and claims information based on the information provided by the client in paragraph (g)(32)(iii)(A) of this section.

(C) *Supported information and capabilities*—(*1*) *Clinical and coverage information.* Support the requirements described in the ''PDEX Server CapabilityStatement'' and the HL7 FHIR Profiles and operations included in Section 4.5.4 ''CapabilityStatement'' via a standardized API according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(*2*) *Claims information.* Support the requirements in the in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

(*3*) *USCDI and US Core.* The capabilities described in ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213.

(D) *Response.* Support returning patient clinical, coverage, and non-financial claims and encounter information according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2) for each of the data included in paragraphs (g)(32)(C)(*1*) through (*3*) of this section.

(E) *Bulk FHIR API.* A Health IT Module must support responding to requests for patient data according to at least one of the versions of the standard adopted in § 170.215(a) and at least one of the versions of the implementation specification adopted in § 170.215(d) for each of the data included in paragraphs (g)(32)(C)(*1*) through (*3*) of this section. Additionally, for the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (g)(32)(iii)(E)(*1*) of this section or both

paragraphs (g)(32)(iii)(E)(*1*) and (*2*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraphs (g)(32)(iii)(E)(*1*) and (*2*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

(*1*) The ''GroupLevelExport'' operation; and

(*2*) The ''_type'' query parameter for each of the data included in paragraphs (g)(32)(C) through (E) of this section.

(33) *Payer-to-payer API.* Support the following capabilities to enable payers to exchange patient health information with other payers via a standardized API(s).

(i) *Registration.* Support the following registration capabilities to support the full scope of API capabilities in paragraph (g)(33) of this section:

(A) *Functional registration.* Support registration for confidential apps according to the requirements included in paragraph (j)(1) of this section.

(B) *Dynamic registration.* Support dynamic registration for confidential apps according to the requirements included in paragraph (j)(2) of this section.

(ii) *Authentication and authorization*—(A) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization according to the requirements in paragraph (j)(7) of this section for system apps functionally registered using the capabilities in paragraph (g)(33)(i)(A) of this section.

(B) *Asymmetric certificate-based system authentication and authorization.* Support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) of this section for system apps dynamically registered using the capabilities in paragraph (g)(33)(i)(B) of this section.

(iii) *Information access.* (A) Support the requirements included in the ''Payer-to-Payer Exchange'' section of at least one of the versions of the implementation specifications adopted in § 170.215(k)(2) as a client and server including support for the following to allow access to information in paragraphs (g)(33)(iii)(B) through (D) of this section:

(*1*) Support the following ''Data Retrieval Methods'' from at least one of the implementation specifications adopted in § 170.215(k)(2): ''Query all clinical resource individually,'' ''$patient-everything operation,'' and ''Bulk FHIR Asynchronous protocols.''

(*2*) *Bulk FHIR API.* For the time period up to and including December 31, 2027, a Health IT Module must respond to requests for patient data according to at least one of the versions of the standard adopted in § 170.215(a), and at least one of the versions of the implementation specification adopted in § 170.215(d) for each of the data elements included in paragraphs (g)(33)(iii)(B) through (D) of this section. Additionally, for the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (g)(33)(iii)(A)(2)(*i*) or both paragraphs (g)(33)(iii)(A)(*2*)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d). On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraphs (g)(33)(iii)(A)(2)(*i*) and (*ii*) of this section according to at least one of the versions of the implementation specification adopted in § 170.215(d).

(*i*) The ''GroupLevelExport'' operation; and

(*ii*) The ''_type'' query parameter for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213.

(B) *Clinical and coverage information.* Support the requirements described in the ''PDEX Server CapabilityStatement'' as a client and server via a standardized API according to at least one of the versions of the implementation specification adopted in § 170.215(k)(2).

(C) *Claims information.* Support claims information by supporting the data included in the ''C4BB CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(k)(1).

(D) *USCDI and US Core.* The capabilities described in ''US Core Server CapabilityStatement'' according to at least one of the versions of the implementation specification adopted in § 170.215(b)(1) for each of the data classes and data elements included in at least one of the versions of the USCDI standard adopted in § 170.213.

(34) *Prior authorization API—provider.* Support the following capabilities to enable providers to request and receive coverage requirements from payers at the time treatment decisions are being made.

(i) *Coverage discovery.* Support the following capabilities to initiate and exchange information with payer systems as a client to support the identification of coverage requirements.

(A) Support the ''Privacy, Security, and Safety'' section of at least one of the versions of the implementation specification adopted in § 170.215(j)(1).

(B) Support the capabilities in paragraph (j)(20) of this section to enable workflow triggers to call decision support services, including the following:

(*1*) Support ''appointment-book'', ''encounter-start'', ''encounter-discharge'', ''order-dispatch'', ''order-select,'' and ''order-sign'' CDS Hooks according to at least one of the versions of the implementation specification adopted in § 170.215(j)(1) and requirements in paragraph (j)(20) of this section.

(*2*) [Reserved]

(C) Support the requirements applicable to ''CRD Clients'' in at least one of the versions of the implementation specification adopted in § 170.215(j)(1) including:

(*1*) The requirements in the ''CRD Client CapabilityStatement.''

(*2*) The ''SHOULD'' requirements applicable to ''CRD Clients'' in Section 5.8 ''Additional Data Retrieval.''

(ii) *Documentation and rules exchange.* Support the ability to request and populate prior authorization documentation templates and rules from payer systems according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2).

(A) *Light DTR capabilities.* (*1*) Support the capabilities included in the ''Light DTR EHR'' CapabilityStatement according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2).

(*2*) *Registration.* Support the following capabilities to support the full scope of API capabilities in paragraph (g)(34)(ii)(A) of this section:

(*i*) *Functional registration.* Support functional registration of the ''DTR SMART Client'' according to the requirements included in paragraph (j)(1) of this section.

(*ii*) *Dynamic registration.* Support dynamic registration of the ''DTR SMART Client'' according to the requirements included in paragraph (j)(2) of this section.

(*3*) *App Launch, authentication, and authorization.* Support launching the ''DTR SMART Client'' according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2) to allow providers to launch an app to complete documentation for prior authorization according to at least one of the versions of the implementation specifications adopted in § 170.215(j)(2).

(*i*) *SMART authentication and authorization for user access.* Support

authentication and authorization during the process of granting access to patient data to users according to the requirements in paragraph (j)(10) of this section.

(*ii*) *Asymmetric certificate-based authentication for B2B user access.* Support asymmetric certificate-based authentication according to the requirements in paragraph (j)(11) of this section for the ''Light DTR Client'' dynamically registered using the capabilities in paragraph (g)(34)(ii)(A)(*2*)(*ii*) of this section.

(B) *Full DTR capabilities.* Support the capabilities included in the ''Full DTR EHR'' CapabilityStatement according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2).

(iii) *Prior authorization submission.* Support the following capabilities to submit a prior authorization request to a payer system.

(*A*) *Prior authorization transactions.* Support the ability to submit a prior authorization request to a payer system according to at least one of the implementation specifications adopted in 170.215(j)(3), including the following requirements:

(*1*) Support the ''EHR PAS Capabilities'' CapabilityStatement according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3).

(*2*) Support the ability to include documentation created in paragraph (g)(34)(ii) of this section in a prior authorization request to a payer system according to at least one of the versions of the implementation specifications adopted in § 170.215(j)(3).

(*3*) Support the ability to consume and process a ''ClaimResponse'' according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3).

(*4*) Support subscriptions as a client according to the requirements in paragraph (j)(24) of this section and at least one of the versions of the implementation specification adopted in § 170.215(j)(3) in order to support ''pended authorization responses''.

(B) [Reserved]

(35) *Prior authorization API—payer.* Support the following capabilities to enable providers to request and receive coverage requirements from payers at the time treatment decisions are being made.

(i) *Coverage discovery.* Support the following capabilities to exchange information with provider systems to support the identification of coverage requirements.

(A) Support the ability to receive and respond to decision support requests as a service by supporting the capabilities in paragraph (j)(21) of this section.

(B) Support the requirements applicable to ''CRD Server'' included in at least one of the versions of the implementation specification adopted in paragraph (j)(1) of this section including the requirements in the ''CRD Server CapabilityStatement.''

(ii) *Documentation and rules exchange.* Support the following capabilities to exchange prior authorization documentation requirements with provider systems.

(A) *Registration.* Support the following registration capabilities to support the full scope of API capabilities in this paragraph (g)(35)(ii):

(*1*) *Functional registration.* Support functional registration for the ''DTR SMART Client'' and ''Full DTR EHR'' according to the requirements included in paragraph (j)(1) of this section.

(*2*) *Dynamic registration.* Support dynamic registration for the ''DTR SMART Client'' and ''Full DTR EHR'' according to the requirements included in paragraph (j)(2) of this section.

(B) *Authentication and authorization for system access—*(*1*) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization according to the requirements in paragraph (j)(7) of this section for the ''DTR SMART Client'' and ''Full DTR EHR'' functionally registered using the capabilities in paragraph (g)(35)(ii)(A)(*1*) of this section.

(*2*) *Asymmetric certificate-based system authentication and authorization.* Support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) of this section for the ''DTR SMART Client'' and ''Full DTR EHR'' dynamically registered using the capabilities in paragraph (g)(35)(ii)(A)(*2*) of this section.

(C) *Prior authorization documentation exchange.* Support the ability to receive and respond to a prior authorization documentation request with documentation templates and rules according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2), including:

(*1*) Support the capabilities included in the ''DTR Payer Service'' CapabilityStatement according to at least one of the versions of the implementation specification adopted in § 170.215(j)(2).

(*2*) [Reserved]

(iii) *Prior authorization receipt and response.* Support the following capabilities to receive and respond to a prior authorization request.

(A) *Registration.* Support the following registration capabilities to support the full scope of API capabilities in this paragraph (g)(35)(iii):

(*1*) *Functional registration.* Support functional registration for confidential apps according to the requirements included in paragraph (j)(1) of this section.

(*2*) *Dynamic registration.* Support dynamic registration according to the requirements included in paragraph (j)(2) of this section.

(B) *Authentication and authorization for system access—*(*1*) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization according to the requirements in paragraph (j)(7) of this section for system apps functionally registered using the capabilities in paragraph (g)(35)(iii)(A)(*1*) of this section.

(*2*) *Asymmetric certificate-based system authentication and authorization.* Support asymmetric certificate-based system authentication and authorization according to the requirements in paragraph (j)(8) of this section for system apps dynamically registered using the capabilities in paragraph (g)(35)(iii)(A)(*2*) of this section.

(C) *Prior authorization transactions.* Support the ability to receive, process, and respond to a prior authorization request according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3), including the following requirements:

(*1*) Support the ''Intermediary PAS Capabilities'' according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3).

(*2*) Support an endpoint for receiving prior authorization requests according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3).

(*3*) Support the ability to respond to a prior authorization request with a ''ClaimResponse'' according to at least one of the versions of the implementation specification adopted in § 170.215(j)(3).

(*4*) Support subscriptions as a server according to the requirements of at least one of the versions of the implementation specification in § 170.215(j)(3) including support for ''pended authorization responses.''

(36) *Provider directory API—health plan coverage.* Support the ability to publish a payer's insurance plans, their associated networks, and the organizations and providers that participate in these networks according to at least one of the versions of the implementation specification adopted

in § 170.215(n), including the requirements described in the ''Plan-Net CapabilityStatement.''

(h) *Transport methods and other protocols*—(1) *Direct project*—(i) *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in § 170.202(a)(2), including formatted only as a ''wrapped'' message.

(ii) *Delivery notification in direct.* Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

(2) *Direct project, edge protocol, and XDR/XDM.* (i) Able to send and receive health information in accordance with:

(A) The standard specified in § 170.202(a)(2), including formatted only as a ''wrapped'' message;

(B) The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and

(C) Both edge protocol methods specified by the standard in § 170.202(d).

(ii) *Delivery notification in direct.* Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

(j) *Modular API capabilities.* The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(1) *Functional registration.* Support the ability to register applications with a Health IT Module's authorization server.

(2) *Dynamic registration.* Support the ability to dynamically register confidential apps according to the implementation specifications adopted in § 170.215(o), including mandatory support for sections ''Home,'' ''Discovery,'' and ''Registration'' as well as the ''community'' query parameter as defined in section ''Multiple Trust Communities'' of the implementation specifications adopted in § 170.215(o).

(3)–(4) [Reserved]

(5) *Asymmetric certificate-based authentication for patient access.* Support asymmetric certificate-based authentication during the process of granting access to patient data to patients according to the implementation specifications adopted in § 170.215(o), including support for asymmetric certificate-based authentication as detailed in section ''Consumer-Facing'' of the implementation specifications adopted in § 170.215(o).

(6) *SMART App Launch user authorization.* Support user authorization during the process of granting access to patient data according to at least one of the implementation specifications adopted in § 170.215(c), including support for:

(i) *Refresh tokens.* Support issuing a refresh token valid for a period of no less than three months to confidential apps and native apps capable of securing a refresh token.

(ii) *Token introspection.* Support the ability to receive and validate tokens issued by the Health IT Module in accordance with at least one implementation specification adopted in § 170.215(c).

(iii) *Persistent access until revocation.* Support the ability for a user to enable for confidential apps persistent access to patient information without requiring user re-authentication or re-authorization until authorization revocation at the user's direction.

(iv) *User authorization revocation.* A Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a user's direction within 1 hour of the request.

(7) *SMART Backend Services system authentication and authorization.* Support system authentication and authorization during the process of granting access to patient data in accordance with the ''Backend Services'' section of at least one implementation specification adopted in § 170.215(c), including support for:

(i) *Token introspection.* Support the ability to receive and validate tokens issued by the Health IT Module in accordance with at least one implementation specification adopted in § 170.215(c).

(ii) [Reserved]

(8) *Asymmetric certificate-based system authentication and authorization.* Support system authentication and authorization for the ''client_credentials'' grant type during the process of granting access to patient data according to the implementation specifications adopted in § 170.215(o), including support for the ''Business-to-Business'' section of the implementation specifications adopted in § 170.215(o) and the following:

(i) *Token introspection.* Support the ability to receive and validate tokens issued by the Health IT Module in accordance with at least one implementation specification in § 170.215(c).

(ii) [Reserved]

(9) *SMART patient access for standalone apps.* Support patient authorization and authorization revocation at a patient's direction according to the requirements in § 170.315(j)(6), including support for one of the following sets of SMART capabilities listed in paragraphs (j)(9)(i) through (iii) of this section. For the time period up to and including December 31, 2025, a Health IT Module must meet either the requirements specified in paragraph (j)(9)(i), (ii), or (iii) of this section. For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (j)(9)(ii) or (iii) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph (j)(9)(iii) of this section.

(i) Support the ''Patient Access for Standalone Apps'' Capability Set, as well as the capabilities of ''launch-standalone'' and ''context-standalone-patient,'' and the capabilities in subsections ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-user'' capability according to the implementation specification adopted in § 170.215(c)(1).

(ii) Support the ''Patient Access for Standalone Apps'' Capability Set as well as the capabilities of ''launch-standalone'' and ''context-standalone-patient,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' and ''permission-user'' capabilities according to the implementation specification adopted in § 170.215(c)(2).

(iii) Support the ''Patient Access for Standalone Apps'' Capability Set as well as the capabilities of ''launch-standalone'' and ''context-standalone-patient,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' and ''permission-user'' capabilities according to the implementation specification adopted in § 170.215(c)(3).

(10) *SMART clinician access for EHR launch.* For the time period up to and including December 31, 2025, a Health IT Module must meet either the requirements specified in paragraph (j)(10)(i)(A), (B), or (C) of this section. For the time period up to and including December 31, 2027, a Health IT Module must meet either the requirements specified in paragraph (j)(10)(i)(B) or (C) of this section. On and after January 1, 2028, a Health IT Module must meet the requirements specified in paragraph (j)(10)(i)(C) of this section.

(i) *User authorization.* Support user authorization according to the requirements in paragraphs (j)(6)(i) through (iii) of this section, including

support for one of the following sets of SMART capabilities:

(A) Support the ''Clinician Access for EHR Launch'' Capability Set as well as the capabilities of ''launch-ehr,'' ''context-banner,'' ''context-style,'' and ''context-ehr-patient'' as well as the capabilities in subsections ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' according to the implementation specification adopted in § 170.215(c)(1).

(B) Support the ''Clinician Access for EHR Launch'' Capability Set as well as the capabilities of ''launch-ehr,'' ''context-banner,'' ''context-style,'' ''context-ehr-patient,'' and ''context-ehr-encounter,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' capability according to the implementation specification adopted in § 170.215(c)(2).

(C) Support the ''Clinician Access for EHR Launch'' Capability Set as well as the capabilities of ''launch-ehr,'' ''context-banner,'' ''context-style,'' ''context-ehr-patient,'' and ''context-ehr-encounter,'' and the capabilities in subsections ''Authorization Methods,'' ''Client Types,'' ''Single Sign-on,'' and ''Permissions'' except the ''permission-online'' capability according to the implementation specification adopted in § 170.215(c)(3).

(ii) *User authorization revocation.* Support user authorization revocation according to the requirements in paragraph (j)(6)(iv) of this section.

(11) *Asymmetric certificate-based authentication for B2B user access.* Support asymmetric certificate-based authentication for the ''authorization_code'' grant type during the process of granting access to patient data to users according to the implementation specifications adopted in § 170.215(o), including support for asymmetric certificate-based authentication as detailed in section ''Business-to-Business'' of the implementation specifications adopted in § 170.215(o).

(12)–(19) [Reserved]

(20) *Workflow triggers for decision support interventions—clients.* Support the requirements of the implementation specification in § 170.215(f) as a ''CDS Client'' including support for the following:

(i) *Registration.* Support registration of CDS Services according to at least one of the implementation specifications in § 170.215(f).

(ii) *Authentication and authorization.* Support authentication and authorization according to the implementation specification in § 170.215(f)(1).

(iii) *Workflow triggers.* Support the execution of decision support workflow triggers in accordance with the implementation specification in § 170.215(f)(1).

(iv) *Information exchange.* Send a decision support request to a CDS Service according to the implementation specification in § 170.215(f)(1), including support for the following:

(A) *Pre-fetch.* Support the ability to deliver a CDS Hook request with prefetched information according to the ''Prefetch Template'' section of the implementation specification in § 170.215(f)(1).

(B) *Resource access via API.* Support access to HL7 FHIR Resources via a RESTful API to support decision support intervention workflows according to the ''FHIR Resource Access'' section of the implementation specification in § 170.215(f)(1).

(C) *Receive and display response.* Support the receipt of a decision support response according to the implementation specification in § 170.215(f)(1), including support for the following:

(*1*) *Display to the end user.* Support the display of the contents of a decision support response to an end-user.

(*2*) *SMART app launch.* Support the ability to launch internal apps and SMART apps from decision support responses according to the implementation specification in § 170.215(f)(1), including support for the ''Link'' field ''appContext.''

(21) *Workflow triggers for decision support interventions—services.* Support the requirements of the implementation specification in § 170.215(f)(1) as a ''CDS Service'' including support for the following:

(i) *Registration.* Support registration of CDS Clients according to the implementation specification in § 170.215(f)(1).

(ii) *Authentication and authorization.* Support authentication and authorization according to the implementation specification in § 170.215(f)(1).

(iii) *Information exchange to support decision support.* Respond to requests for recommendations and guidance via a RESTful API according to the implementation specification in § 170.215(f)(1), including support for the following:

(A) *Receive and process decision support request.* Receive and process decision support request according to the implementation specification in § 170.215(f)(1), including:

(*1*) The ability to receive pre-fetched information according to the ''Prefetch Template'' section of the implementation specification in § 170.215(f)(1); and

(*2*) The ability to fetch HL7 FHIR Resources via an API according to the ''FHIR Resource Access'' section of the implementation specification in § 170.215(f)(1).

(B) *Decision support response.* Support returning a decision support response according to the implementation specification in § 170.215(f), including support for the ''Link'' field ''appContext.''

(22) *Verifiable health records.* Support the issuance of verifiable health records for vaccination status and infectious disease-related laboratory testing according to implementation specifications adopted in § 170.215(g)(1)(i) through (2)(i), including support for the following:

(i) *Information profiles.* Support the ''data minimization'' and ''allowable data'' profiles of the following according to the implementation specification adopted in § 170.215(g)(2)(i): ''Immunization Bundle,'' ''COVID–19 Labs Bundle,'' and ''Generic Labs Bundle,'' ''Patient—United States,'' ''Vaccination,'' ''Lab results—COVID–19–,'' and ''Lab results—Generic.''

(ii) *API.* Support the ''$health-cards-issue'' operation via a standardized API according to the implementation specification adopted in § 170.215(g)(1).

(23) *Subscriptions—server.* Support subscriptions as a server according to the implementation specifications in § 170.215(h)(1), including:

(i) Support the requirements in section ''1.6 Topic-Based Subscriptions—FHIR R4'' of the implementation specification in § 170.215(h)(1).

(ii) Support the ''R4/B Topic-Based Subscription'' profile according to the implementation specification in § 170.215(h)(1).

(iii) Support the requirements included in the ''R4 Topic-Based Subscription Server Capability Statement'' of the implementation specification in § 170.215(h)(1), including support for ''create,'' ''update,'' and ''delete'' interactions for HL7 FHIR Subscription Resources according to the implementation specification in § 170.215(h)(1).

(iv) Send subscription notifications to subscribed clients according to section ''1.6 Topic-Based Subscriptions—FHIR R4'' of the implementation specification in § 170.215(h)(1), including:

(A) Support for ''id-only'' Payload Types as specified in the ''Payload Types'' section of the implementation specification in § 170.215(h)(1).

(B) Support for the ''REST-Hook'' channel as specified in the ''Channels''

section of the implementation specification in § 170.215(h)(1).

(v) Support the following subscription topics and parameters:

(A) *USCDI change notifications.* Support the ability for a client to subscribe to notifications filtered by a patient identifier and send notifications when any of the Resources specified in § 170.315(j)(23)(v)(B) are created or updated as applicable according to the standard in § 170.215(a) and implementation specification in § 170.215(h)(1).

(B) *Resource notifications.* Support the ability for a client to subscribe to notifications filtered according to the conditions below and send notifications for the following Resource interactions according to the standard in § 170.215(a) and implementation specification in § 170.215(h)(1):

(*1*) ''AllergyIntolerance'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''patient'' data elements.

(*2*) ''CarePlan'' Resource is created or updated, including support for filtering subscription notifications using ''category'' and ''subject'' data elements.

(*3*) ''CareTeam'' Resource is created, or updated, including support for filtering subscription notifications using ''category'' and ''subject'' data elements.

(*4*) ''Condition'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.

(*5*) ''Coverage'' Resource is created or updated, including support for filtering subscription notifications using ''beneficiary'' and ''type'' data elements.

(*6*) ''DiagnosticReport'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.

(*7*) ''DocumentReference'' Resource is created or updated, including support for filtering subscription notifications using ''subject'' and ''type'' data elements.

(*8*) ''Encounter'' Resource is created or updated, including support for filtering subscription notifications using ''reasonCode,'' ''subject,'' and ''type'' data elements.

(*9*) ''Goal'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''description,'' and ''subject'' data elements.

(*10*) ''Immunization'' Resource is created or updated, including support for filtering subscription notifications using ''patient,'' and ''vaccineCode'' data elements.

(*11*) ''MedicationDispense'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''medication[x],'' and ''subject'' data elements.

(*12*) ''MedicationRequest'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''medication[x],'' and ''subject'' data elements.

(*13*) ''Observation'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.

(*14*) ''Patient'' Resource is updated, including support for filtering subscription notifications using the ''identifier'' data element.

(*15*) ''Procedure'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.

(*16*) ''QuestionnaireResponse'' Resource is created or updated, including support for filtering subscription notifications using the ''subject'' data element.

(*17*) ''RelatedPerson'' Resource is created or updated, including support for filtering subscription notifications using the ''patient'' data element.

(*18*) ''ServiceRequest'' Resource is created or updated, including support for filtering subscription notifications using ''category,'' ''code,'' and ''subject'' data elements.

(*19*) ''Specimen'' Resource is created or updated, including support for filtering subscription notifications using ''patient'' and ''type'' data elements.

(24) *Subscriptions—client.* Support subscriptions as a client according to the implementation specifications in § 170.215(h)(1), including:

(i) Support the requirements in section ''1.6 Topic-Based Subscriptions—FHIR R4'' of the implementation specifications in § 170.215(h)(1).

(ii) Support the ''R4/B Topic-Based Subscription'' profile according to the implementation specifications in § 170.215(h)(1).

(iii) Support the accompanying client capabilities for the minimum requirements included in the ''R4 Topic-Based Subscription Server Capability Statement'' of the implementation specification in § 170.215(h)(1), including support for ''create,'' ''update,'' and ''delete'' interactions for HL7 FHIR Subscription Resources according to the implementation specification in § 170.215(h)(1).

(iv) Receive subscription notifications according to section ''1.6 Topic-Based Subscriptions—FHIR R4'' of the implementation specifications in § 170.215(h)(1), including:

(A) Support for ''id-only'' Payload Types as specified in the ''Payload Types'' section of the implementation specifications in § 170.215(h)(1).

(B) Support for consuming notifications via the ''REST-Hook'' channel as specified in the ''Channels'' section of the implementation specifications in § 170.215(h)(1).

■ 11. Amend § 170.402 by adding paragraph (b)(2)(iii) to read as follows:

§ 170.402 Assurances.

(b) * * *

(2) * * *

(iii) On and after January 1, 2028, a health IT developer of a Health IT Module certified to the certification criterion in § 170.315(b)(10) and meets the requirements of § 170.315(b)(10)(i)(F) must:

(A) Report to its ONC–ACB no later than March 1 of each calendar year how many requests it received during the immediately preceding calendar year; and

(B) Provide all of its customers of that Health IT Module with an updated version of the Health IT Module fully compliant with § 170.315(b)(10)(i)(A) through (F) no later than the end of the second calendar year following the calendar year in which the developer has received more than 10 requests for a single patient export from that Health IT Module.

■ 12. Amend § 170.404 by:

■ a. Revising the introductory text;

■ b. Revising and republishing paragraph (a)(2);

■ c. Revising paragraphs (b)(1) through (3); and

■ d. Revising the definitions of ''Certified API Developer'' and ''Certified API technology''.

The revisions and republication read as follows:

§ 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), (20), and (30) through (36), and (j), unless otherwise specified in this section.

(a) * * *

(2) *Transparency conditions*—A Certified API Developer must publish complete business and technical documentation, including the documentation described in paragraphs (a)(2)(i) and (ii) of this section, via a publicly accessible hyperlink that

allows any person to directly access the information without any preconditions or additional steps.

(i) *Technical documentation.* The API(s) must include complete accompanying technical documentation that contains, as applicable:

(A) 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.

(B) 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).

(C) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(ii) *Terms and conditions.* The API(s) must include complete accompanying business documentation that contains, at a minimum:

(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.

* * * * *

(b) * * *

(1) *Authenticity verification and registration for production use.* The following apply to a Certified API Developer with a Health IT Module certified to one or more of § 170.315(g)(10), (20), (30), and (32) through (35):

(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 any of the criteria in § 170.315(g)(10), (20), (30), and (32) through (35). This process shall not apply to API Users that are part of a trust community supported at an API Information Source deployment submitting registration requests conformant to the specifications in § 170.215(o).

(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. If the API User is part of a trust community supported at an API Information Source deployment and submitted a valid registration request conformant to the specifications in § 170.215(o), then the application must instead be enabled for production use within one business day.

(2) *Publication of API discovery details for patient access.* For the time period up to and including December 31, 2027, Certified API Developers with Health IT Modules certified to § 170.315(g)(10) must meet either the API discovery detail requirements in paragraphs (b)(2)(i) and (ii) of this section or the requirements in (b)(2)(i), (iii), and (iv) of this section. On and after January 1, 2028, all Certified API Developers with Health IT Modules certified to § 170.315(g)(10) must meet the requirements in (b)(2)(i), (iii), and (iv) of this section. Certified API Developers with Health IT Modules certified to § 170.315(g)(30) must meet the requirements in paragraphs (b)(2)(i), (iii), and (iv) of this section.

(i) *API discovery terms.* API discovery details in paragraphs (b)(2)(ii), (iii), and (iv) of this section must be published and reviewed according to the following terms:

(A) Publicly published, at no charge, for all its customers regardless of whether the Health IT Module is centrally managed by the Certified API Developer or locally deployed by an API Information Source.

(B) Reviewed quarterly and as necessary updated.

(ii) *API discovery in FHIR format.* API discovery details must be published in the following formats in accordance with the standards in § 170.215(a):

(A) Service base URLs must be publicly published in the Endpoint resource format.

(B) Organization details for each service base URL must be publicly published in the Organization resource format. Each Organization resource must contain:

(*1*) A reference, in the Organization.endpoint element, to the Endpoint resources containing service base URLs managed by this organization.

(*2*) The organization's name, location, and facility identifier.

(C) Endpoint and Organization resources must be collected into a Bundle resource format.

(iii) *API discovery in user-access brand format.* API discovery details and related API Information Source details, including the API Information Source's name, location, and facility identifier, must be publicly published in an aggregate vendor-consolidated Bundle according to the ''User-access Brands and Endpoints'' specification in at least one implementation specification adopted in § 170.215(c).

(iv) *Trust community discovery for dynamic registration.* Trust community details such as trust community name, contact information, web address, and identifying Uniform Resource Identifier (URI) must be publicly published in a computable format at no charge for each service base URL published in accordance with (b)(2)(iii) of this section.

(3) *Publication of API discovery details for payer information.* A Certified API Developer certified to § 170.315(g)(32), (33), (35), or (36) must conform to the following:

(i) The Certified API Developer must publicly publish API discovery details for all of its customers with Health IT Modules certified to § 170.315(g)(30), (32), (33), (35), or (36) regardless of whether the Health IT Modules are centrally managed by the Certified API Developer or locally deployed by an implementer of the certified API technology;

(ii) The API Information Source details, including the API Information Source's name and location, must be

published in an aggregate vendor-consolidated Bundle according to the ''User-access Brands and Endpoints'' specification in at least one implementation specification adopted in § 170.215(c); and

(iii) All API discovery details for payer information published according to this section must be reviewed quarterly and, as necessary, updated by the Certified API Developer.

* * * * *

(c) * * *

Certified API Developer means a health IT developer that creates ''certified API technology.''

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), (20), and (30) through (36), and (j).

* * * * *

■ 13. Amend § 170.405 by revising paragraph (a) to read as follows.

§ 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 of the ONC Certification Criteria for Health IT in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), (g)(20) and (30) through (36), (h), and (j) 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.

* * * * *

■ 14. Amend § 170.406 by revising paragraph (a)(2) to read as follows:

§ 170.406 Attestations.

(a) * * *

(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; and, § 170.402(b)(4) if the health IT developer certified a Health IT Module(s) to § 170.315(b)(11).

* * * * *

■ 15. Amend § 170.407 by revising and republishing paragraphs (a)(1), (2), (a)(3)(i) and (ii), and (b) to read as follows:

§ 170.407 Insights Condition and Maintenance of Certification.

(a) *Condition of certification*—(1) *Measure responses.* A health IT developer must submit (to the independent entity designated by the Secretary) for each reporting period pursuant to paragraph (b) of this section:

(i) Responses for the measures specified in this section, which must include:

(A) Data aggregated at the product level (across versions);

(B) Documentation available via a publicly accessible hyperlink, related to the data sources and methodology used to generate measures;

(C) Percentage of total customers (*e.g.,* hospitals, individual clinician users) represented in provided data; and

(D) Health care provider identifiers (*e.g.,* National Provider Identifier (NPI), CMS Certification Number (CCN), or health system ID) for providers included in the data; or

(ii) A response (attestation) that it does not:

(A) Meet the minimum reporting qualifications requirement in paragraph (a)(2) of this section; or

(B) Have health IT certified to the certification criteria specified in each measure in paragraphs (a)(3)(i) through (vii) of this section; or

(C) Have any users using the certified health IT specified in each measure in paragraphs (a)(3)(i) through (vii) of this section during the reporting period.

(2) *Minimum reporting qualifications requirement.* At least 50 hospitals or 500 individual clinician users across the developer's certified health IT.

(3) *Measures*—(i) *Individuals' access to electronic health information through certified health IT.* If a health IT developer has a Health IT Module certified to § 170.315(e)(1) or (g)(10) or both, then the health IT developer must submit responses for the number of unique individuals who access electronic health information (EHI) themselves or through their authorized representatives overall and by different methods of access through certified health IT.

(ii) *C–CDA reconciliation and incorporation through certified health IT.* If a health IT developer has a Health IT Module certified to § 170.315(b)(2), then the health IT developer must submit responses for:

(A) Encounters;

(B) Unique patients with an encounter;

(C) C–CDA documents obtained (unique and overall);

(D) C–CDA documents reconciled and incorporated both through manual and automated processes; and

(E) Specific data classes and elements from C–CDA documents reconciled and incorporated both through manual and automated processes.

* * * * *

(b) *Maintenance of certification.* (1) A health IT developer must provide responses to the Insights Condition of Certification specified in paragraph (a) of this section annually:

(i) A health IT developer must provide responses for measures specified in:

(A) Paragraphs (a)(3)(i) and (iii), (a)(3)(iv)(A) and (B), and (a)(3)(vi) of this section beginning July 2027;

(B) Paragraphs (a)(3)(ii)(A) through (C), (a)(3)(iv)(C), (a)(3)(v), (a)(3)(vi)(A) and (B), and (a)(3)(vii) of this section beginning July 2028;

(C) Paragraphs (a)(3)(ii)(D) and (a)(3)(vii)(A) of this section beginning July 2029; and

(D) Paragraph (a)(3)(ii)(E) of this section beginning July 2030.

(ii) A health IT developer must provide responses applicable to all their certified health IT that meet the requirements specified in paragraph (a) of this section as of January 1st of the year prior in which the responses are submitted.

(2) For certified Health IT Modules included in paragraph (a) of this section that are updated using Inherited Certified Status after January 1 of the year prior in which the responses are submitted, a health IT developer must include the newer version of the certified Health IT Module(s) in its annual responses to the Insights Condition of Certification.

■ 16. Amend § 170.502 by revising the definition of ''Gap certification'' to read as follows:

§ 170.502 Definitions.

* * * * *

Gap certification means the certification of a previously certified Health IT Module(s) to:

(1) All applicable new and/or revised certification criteria adopted by the Secretary at subpart C of this part based on test results issued by a NVLAP-accredited testing laboratory under the ONC Health IT Certification Program or an ONC–ATL; and

(2) All other applicable certification criteria adopted by the Secretary at subpart C of this part based on the test results used to previously certify the Health IT Module(s) under the ONC Health IT Certification Program.

* * * * *

■ 17. Amend § 170.505 by revising paragraph (a)(2) to read as follows:

§ 170.505 Correspondence

(a) * * *

(2) The applicant for ONC–ATL status, the applicant for ONC–ACB status, an ONC–ACB, an ONC–ATL, health IT developer, or a party to any proceeding under this subpart will be considered to have received

correspondence or other written communication from ONC or the National Coordinator on the first of the following:

(i) The date on which ONC or the National Coordinator receives a response to the correspondence via written or verbal communication methods;

(ii) The date of the delivery confirmation to the address on record for correspondence sent by express or certified mail; or

(iii) The date of the seventh business day (as defined in § 170.102) after the date on which the email, express, or certified mail was sent.

* * * * *

■ 18. Revise § 170.511 to read as follows:

§ 170.511 Authorization scope for ONC–ATL status.

Applicants may seek authorization from the National Coordinator to perform the testing of Health IT Modules to a portion of a certification criterion, one certification criterion, or many or all certification criteria adopted by the Secretary under subpart C of this part.

■ 19. Amend § 170.523 by:
■ a. Revising paragraph (i)(2)(iii),
■ b. Adding paragraph (i)(4);
■ c. Revising paragraphs (j)(3) and (m)(3) through (5);
■ d. Adding paragraph (m)(6);
■ e. Redesignating paragraphs (p) through (u) as paragraphs (r) through (w);
■ f. Adding new paragraphs (p) and (q); and
■ g. Add paragraphs (x) and (y).

The revisions and additions read as follows:

§ 170.523 Principles of proper conduct for ONC–ACBs.

* * * * *

(i) * * *

(1) * * *

(2) * * *

(iii) Certification criteria, Maintenance of Certification, and other ONC Health IT Certification Program requirements surveilled;

* * * * *

(4) Notify the National Coordinator prior to initiating a suspension in accordance with § 170.556(d)(5) or withdraw certification in accordance with § 170.556(d)(6) for a Health IT Module for a non-conformity pertaining to a Maintenance of Certification requirement for which the ONC–ACBs have responsibilities in this section.

* * * * *

(j) * * *

(3) Previous certifications that it performed if its conduct necessitates the recertification of Health IT Module(s);

* * * * *

(m) * * *

(3) All use cases for § 170.315(d)(13), for the time period up to and including December 31, 2027;

(4) All updates made to certified Health IT Modules in compliance with § 170.405(b)(3);

(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; and

(6) On and after January 1, 2027, all updates to API discovery details for § 170.404(b)(2) and (3).

* * * * *

(p) *Assurances.* (1) Confirm that health IT developers retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program in accordance with § 170.402(b)(1).

(2) Confirm that applicable health IT developers update the Health IT Module and provide the updated Health IT Module within the specified timeframes in accordance with § 170.402(b)(2) and (3).

(3) Confirm that applicable health IT developers comply with the predictive decision support intervention transparency requirements in accordance with § 170.402(b)(4).

(q) *Application programming interfaces.* (1) Confirm that applicable health IT developers comply with the authenticity verification and registration for production use requirements for application programming interface Maintenance of Certification requirements in accordance with § 170.404(b)(1).

(2) Confirm that applicable health IT developers publish API discovery details for all Health IT Modules certified to § 170.315(g)(10) and (30) in accordance with § 170.404(b)(2).

(r) *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.

(s) *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.

(t) *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).

(u) *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).

(v) *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.

(w) *Insights.* Confirm that developers of certified health IT submit responses for Insights Conditions and Maintenance of Certification requirements in accordance with § 170.407.

(x) *Reporting for non-compliance with approved corrective action plans.* Report to ONC, pursuant to paragraph § 170.556(d)(7)(ii) of this subpart, the developer's failure to timely complete a corrective action plan specific to a Maintenance of Certification requirement for which an ONC–ACB has specific responsibilities under this section. The ONC–ACB must include all documentation pertaining to the identified non-conformity, including the following information:

(1) The Health IT Module and associated product(s);

(2) The nature of the non-conformity(ies);

(3) The corrective action plan documentation;

(4) Communications and records of proceedings; and

(5) Any additional information requested by ONC.

(y) *Authorization withdrawal notice.* Provide ONC notice of intent to withdraw its authorization from the Certification Program:

(1) Submit written notice to ONC 180 days prior to the withdrawal date.

(2) Submit all records to ONC related to the certification of Health IT Modules required by paragraph (g) of this section.

■ 20. Amend 170.524 by revising paragraph (f)(1) to read as follows:

§ 170.524 Principles of proper conduct for ONC–ATLs.

* * * * *

(f) * * *

(1) Retain all records related to the testing of Health IT Modules to the ONC Certification Criteria for Health IT beginning with the codification of those certification criteria in the Code of Federal Regulations through a minimum of three years from the effective date of the removal of those certification criteria from the Code of Federal Regulations; and

* * * * *

■ 21. Amend § 170.550 by:

■ a. Adding paragraph (g)(6);

■ b. Revising paragraphs (h)(1),

■ c. Revising and republishing paragraph (h)(3);

■ d. Adding paragraph (h)(4); and

■ e. Removing and reserving paragraph (m).

The additions, revisions, and republication read as follows:

§ 170.550 Health IT Module certification.

* * * * *

(g) * * *

(6) Section 170.315(b)(4) if the Health IT Module is presented for certification to the certification criteria in § 170.315(b)(3).

(h) * * *

(1) When certifying a Health IT Module to the ONC Certification Criteria for Health IT, 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 (xii) of this section have also been met (and are included within the scope of the certification).

* * * * *

(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) and (12) and, for the time period up to and including December 31, 2027, (d)(13).

(ii) Section 170.315(a)(4), (10), and (13) and, on and after January 1, 2028, (b)(11), are also certified to the certification criteria specified in § 170.315(d)(1) through (3), (5) through (7), and (12) and, for the time period up to and including December 31, 2027, (d)(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),(5) through (8), and (12) and, for the time period up to and including December 31, 2027, (d)(13);

(iv) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1) (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), and (d)(3), (5), and (12) and, for the time period up to and including December 31, 2027, (d)(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), and (12) and, for the time period up to and including December 31, 2027, (d)(13);

(vi) Section 170.315(e)(2) and (3) are also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A) and (B), (d)(2)(ii) through (v), and (d)(3), (5), (9), and (12) and, for the time period up to and including December 31, 2027, (d)(13);

(vii) Section 170.315(f) is also certified to the certification criteria specified in § 170.315(d)(1) through (3), (7), and (12) and, for the time period up to and including December 31, 2027, (d)(13);

(viii) Section 170.315(g)(7) through (10), (20), and (30) through (36) are also certified to the certification criteria specified in § 170.315(d)(1), (9), and (12) and, for the time period up to and including December 31, 2027, (d)(13); and § 170.315(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), and (d)(3) and (12) and, for the time period up to and including December 31, 2027, (d)(13);

(x) Section 170.315(j) 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), and (12).

(4) *Methods to demonstrate compliance with each privacy and security criterion.* One of the following methods must be used to meet each applicable privacy and security criterion listed in paragraph (h)(3) of this section:

(i) Directly, by demonstrating a technical capability to satisfy the applicable certification criterion or certification criteria; or

(ii) Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

* * * * *

■ 22. Amend 170.555 by revising paragraph (b)(2) to read as follows:

§ 170.555 Certification to newer versions of certain standards.

* * * * *

(b) * * *

(2) A certified Health IT Module may be upgraded to comply with newer versions of standards identified as minimum standards in subpart B of this part without adversely affecting its certification status unless the Secretary prohibits the use of a newer version for certification.

■ 23. Amend § 170.556 by revising and republishing paragraphs (b) and (d) and revising paragraph (e)(3) to read as follows:

§ 170.556 In-the-field surveillance and maintenance of certification for Health IT.

* * * * *

(b) *Reactive surveillance.* An ONC–ACB must initiate surveillance (including, as necessary, in-the-field surveillance required by paragraph (a) of this section) whenever it becomes aware of facts or circumstances that would cause a reasonable person in the ONC–ACB's position to question one or more of the following in paragraphs (b)(1) through (3) of this section. Additionally, when an ONC–ACB performs reactive surveillance under this paragraph, it must verify that the requirements of § 170.523(k) have been followed as applicable to the issued certification.

(1) A certified Health IT Module's continued conformity to the requirements of its certification;

(2) A developer's satisfaction of the Maintenance of Certification requirements in § 170.402(b)(1);

(3) An applicable developer's satisfaction of the Maintenance of Certification requirements for which an ONC–ACB has a responsibility under § 170.523 to confirm compliance;

* * * * *

(d) *Corrective action plan and procedures.* (1) When an ONC–ACB determines, through surveillance under this section or otherwise, that a Health IT Module does not conform to the requirements of its certification or that the health IT developer is out of compliance with a Maintenance of Certification requirement specified in subpart D of this part for which the ONC–ACB has specific responsibilities under § 170.523, it must notify the developer of its findings and require the developer to submit a proposed

corrective action plan for the applicable certification criterion, certification criteria, certification requirement, or Maintenance of Certification requirement.

(2) The ONC–ACB shall provide direction to the developer as to the required elements of the corrective action plan.

(3) The ONC–ACB shall verify the required elements of the corrective action plan as specified in this paragraph.

(i) At a minimum, any corrective action plan submitted by a developer to an ONC–ACB must at least include all the following elements for each identified non-conformity:

(A) A description of the identified non-conformities;

(B) The timeframe under which corrective action will be completed; and

(C) An attestation by the developer that it has completed all elements of the approved corrective action plan.

(ii) For all identified non-conformities with respect to any Program requirement codified in subpart A, B, C, or E of this part, the corrective action plan must include the following elements, in addition to the elements identified in paragraph (d)(3)(i) of this section:

(A) An assessment of how widespread or isolated the identified non-conformities may be across all of the developer's customers and users of the certified Health IT Module;

(B) How the developer will address the identified non-conformities, both at any locations where surveillance has identified the non-conformity to have occurred and for all other potentially affected customers and users; and

(C) How the developer will ensure that all affected and potentially affected customers and users are alerted to the identified non-conformities, including a detailed description of how the developer will assess the scope and impact of the problem and include identifying all potentially affected customers; how the developer will promptly ensure that all potentially affected customers are notified of the problem and plan for resolution; how and when the developer will resolve issues for individual affected customers; and how the developer will ensure that all issues are in fact resolved.

(iii) For all identified non-conformities with respect to any Program requirement codified in subpart D of this part, the corrective action plan must include the following elements, in addition to elements identified in paragraph (d)(3)(i) of this section:

(A) How the developer will address the identified non-conformities specific to Maintenance of Certification requirements codified in subpart D of this part; and

(B) How the developer will ensure that all identified non-conformities specific to Maintenance of Certification requirements codified in subpart D of this part are resolved.

(iv) The ONC–ACB may require the corrective action plan to include elements beyond those specified in this paragraph as the minimum necessary.

(4) When the ONC–ACB receives a proposed corrective action plan (or a revised proposed corrective action plan), the ONC–ACB shall either approve the corrective action plan or if the plan does not adequately address the required elements described by paragraph (d)(3) of this section, instruct the developer to submit a revised proposed corrective action plan.

(5) For an identified non-conformity with respect to any Program requirement codified in subpart A, B, C, or E of this part or any Program requirement codified in subpart D of this part for which the ONC–ACB has responsibilities under § 170.523, consistent with its accreditation to ISO/IEC 17065 and procedures for suspending a certification, an ONC–ACB shall initiate suspension procedures for a Health IT Module:

(i) Thirty (30) days after notifying the developer of a non-conformity pursuant to paragraph (d)(1) of this section, if the developer has not submitted a proposed corrective action plan;

(ii) Ninety (90) days after notifying the developer of a non-conformity pursuant to paragraph (d)(1) of this section, if the ONC–ACB cannot approve a corrective action plan because the developer has not submitted a revised proposed corrective action plan in accordance with paragraph (d)(4) of this section; and

(iii) Immediately, if the developer has not completed the corrective actions specified by an approved corrective action plan within the time specified therein.

(6) If a certified Health IT Module's certification has been suspended, an ONC–ACB is permitted to initiate certification withdrawal procedures for the Health IT Module (consistent with its accreditation to ISO/IEC 17065 and procedures for withdrawing a certification) when the health IT developer has not completed the actions necessary to reinstate the suspended certification.

(7) Notification procedures for failure to timely submit a proposed or revised proposed corrective action plan, or complete an approved corrective action plan requirements in subpart D of this part.

(i) For an identified non-conformity with respect to any Program requirement codified in subpart D of this part for which the ONC–ACB has responsibilities under § 170.523, consistent with its accreditation to ISO/IEC 17065 and procedures for notifying ONC, an ONC–ACB shall notify the National Coordinator immediately if one or more of the following occurs:

(A) The developer has not submitted a proposed corrective action plan within the time specified in paragraph (d)(5) of this section.

(B) The ONC–ACB cannot approve a corrective action plan because the developer has not submitted a revised proposed corrective action plan in accordance with paragraph (d)(4) of this section.

(C) The developer has not completed the corrective actions specified by an approved corrective action plan within the time specified therein.

(ii) When a health IT developer fails to obtain approval for a proposed corrective action plan or to complete an approved corrective action plan with respect to any Program requirement codified in subpart D of this part for which the ONC–ACB has responsibilities under § 170.523, the ONC–ACB shall report the information specified in § 170.523(x) to ONC pursuant to paragraph (d)(7)(i) of this section.

(A) The ONC–ACB must notify the developer immediately when the ONC–ACB begins the notification procedures in paragraph (d)(7)(i) of this section.

(e) * * *

(3) *Reporting of corrective action plans.* When a corrective action plan is initiated for a Health IT Module, an ONC–ACB must report the Health IT Module and associated product and corrective action information to the National Coordinator in accordance with § 170.523(f)(1)(xxii) as applicable.

* * * * *

■ 24. Amend § 170.580 by:

■ a. Revising paragraphs (a)(3)(iii) and (v), (a)(4)(ii), (b)(2)(ii)(A)(*3*), (b)(2)(ii)(B) introductory text, (b)(2)(iii), (c)(1), (c)(2) introductory text, (c)(7), and (d)(1), (2), and (6); and

■ b. Revising and republishing paragraphs (e), (f), and (g).

The revisions and republications read as follows:

§ 170.580 ONC review of certified health IT.

(a) * * *

(3) * * *

(iii) The National Coordinator's determination on matters under ONC

Direct Review is controlling and supersedes any determination by an ONC–ACB on the same matters.

* * * * *

(v) The National Coordinator may end all or any part of ONC's 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 doing so would serve the effective administration or oversight of the ONC Health IT Certification Program.

(4) * * *

(ii) The National Coordinator may rely on Office of Inspector General findings to form the basis of a direct review action.

(b) * * *

(2) * * *

(ii) * * *

(A) * * *

(*3*) Providing ONC within 30 days, or within the adjusted timeframe set in accordance with paragraph (b)(2)(ii)(B) of this section, a written explanation and all supporting documentation addressing the non-conformity, clearly labeling as ''previously submitted'' any documentation previously submitted to ONC in response to paragraph (b)(1)(ii)(A)(*3*) of this section, as applicable, and any additional information indicated by ONC.

(B) The National Coordinator may decide to shorten the 30-day timeframe specified in paragraph (b)(2)(ii)(A)(*3*) of this section where the non-conformity is specific to failure to timely complete a Condition or Maintenance of Certification requirement in any of the requirements in § 170.401 through § 170.407 or may adjust the 30-day timeframe specified in paragraph (b)(2)(ii)(A)(*3*) be shorter or longer based on factors including, but not limited to:

* * * * *

(iii) *National Coordinator determination.* After receiving the health IT developer's response provided in accordance with paragraph (b)(2)(ii) of this section, the National Coordinator shall direct ONC to either issue a written determination ending its review or continue with its review under the provisions of this section.

(c) * * *

(1) If the National Coordinator 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.

(2) ONC shall provide direction to the health IT developer as to the required elements of the corrective action plan, which shall include such required elements as the National Coordinator determines necessary to comprehensively and expeditiously resolve the identified non-conformity(ies). Each corrective action plan shall include, for each specific non-conformity, all the elements in paragraphs (c)(2)(i) through (viii) except those that are explicitly waived by the National Coordinator:

* * * * *

(7) ONC may reinstitute a corrective action plan if the National Coordinator later determines that a health IT developer has not fulfilled all of the developer's obligations under the corrective action plan as attested in accordance with paragraph (c)(6) of this section.

(d) * * *

(1) ONC may suspend the certification of a Health IT Module at any time if the National Coordinator determines that ONC has a reasonable belief that the certified health IT may present a serious risk to public health or safety.

(2) When the National Coordinator decides to suspend a certification, ONC will notify the health IT developer of its determination through a notice of suspension.

* * * * *

(6) Any suspension issued under this paragraph (d) may be canceled at any time if:

(i) The National Coordinator determines that ONC no longer has a reasonable belief that the certified health IT presents a serious risk to public health or safety; or

(ii) The Secretary, who may choose to review National Coordinator determinations under this paragraph at their discretion, directs the National Coordinator to cancel the suspension.

(e) Proposed termination. (1) Excluding situations of noncompliance with a Condition or Maintenance of Certification requirement under subpart D of this part, the National Coordinator may propose to terminate a certification issued to a Health IT Module if:

(i) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

(A) Fact-finding;

(B) A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(*3*) of this section;

(C) A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(*3*) of this section; or

(D) A notice of suspension.

(ii) 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;

(iii) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(iv) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(v) 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;

(vi) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(vii) The National Coordinator concludes that a certified health IT's non-conformity(ies) cannot be cured.

(2) When the National Coordinator decides to propose to terminate a certification, ONC will notify the health IT developer of the proposed termination through a notice of proposed termination.

(i) The notice of proposed termination will include, but may not be limited to:

(A) An explanation for the proposed termination;

(B) Information supporting the proposed termination; and

(C) Instructions for responding to the proposed termination.

(3) The health IT developer may respond to a notice of proposed termination, but must do so within 10 days of receiving the notice of proposed termination and must include appropriate documentation explaining in writing why its certification should not be terminated.

(4) Upon receipt of the health IT developer's written response to a notice of proposed termination, the National Coordinator has up to 30 days to make a determination based on ONC's review of the information submitted by the health IT developer. The National Coordinator may extend this timeframe if the complexity of the case requires additional time for ONC review. ONC will, as applicable:

(i) Notify the health IT developer in writing that it has ceased all or part of its review of the health IT developer's certified health IT.

(ii) Notify the health IT developer in writing of its intent to continue all or part of its review of the certified health IT under the provisions of this section.

(iii) Proceed to terminate the certification of the health IT under

review consistent with paragraph (f) of this section.

(f) *Termination.* (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) The National Coordinator concludes that the non-conformity(ies) cannot be cured.

(iv) The National Coordinator determines, based on the notification made by an ONC–ACB under 45 CFR 170.556(d)(7) and the record sent to ONC pursuant to 45 CFR 170.523(x), that the developer did not fulfill its obligations under a corrective action plan.

(2) When the National Coordinator decides to terminate a certification, ONC will notify the health IT developer of its determination through a notice of termination.

(i) The notice of termination will include, but may not be limited to:

(A) An explanation for the termination;

(B) Information supporting the determination;

(C) The consequences of termination for the health IT developer and the Health IT Module under the ONC Health IT Certification Program; and

(D) Instructions for appealing the termination.

(ii) A termination of a certification will become effective after the following applicable occurrence:

(A) The expiration of the 10-day period for filing a statement of intent to appeal in paragraph (g)(3)(i) of this section if the health IT developer does not file a statement of intent to appeal.

(B) The expiration of the 30-day period for filing an appeal in paragraph (g)(3)(ii) of this section if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(C) A final determination to terminate the certification per paragraph (g)(7) of this section if a health IT developer files an appeal.

(3) The health IT developer must notify all potentially affected customers of the identified non-conformity(ies) and termination of certification in a timely manner.

(4) The National Coordinator may rescind a termination determination before the termination becomes effective if the National Coordinator determines that termination is no longer appropriate.

(5) The Secretary may, at the Secretary's discretion, review a termination determination made by the National Coordinator pursuant to paragraph (f)(1) of this section before the termination becomes effective as specified in paragraph (f)(2)(ii) of this section. If the Secretary directs the National Coordinator to rescind the termination, ONC may:

(i) Resume all or part of its review of certified health IT or a health IT developer's actions or practices under this section unless the Secretary specifically directs otherwise; or

(ii) End all or part of its review of certified health IT or a health IT developer's actions or practices under this section unless the Secretary specifically directs otherwise.

(g) *Appeal*—(1) *Basis for appeal.* A health IT developer may appeal a determination to suspend or terminate a certification issued to a Health IT Module under this section, a determination to issue a certification ban under § 170.581(a)(2), or both, if the health IT developer asserts:

(i) The determination is based on an incorrect application of ONC Health IT Certification Program requirements for a:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

(ii) The National Coordinator's determination was not sufficiently supported by the information included in the notice(s) issued under paragraph (d)(2) or (f)(2) of this section, or both.

(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) *Time for filing a request for appeal.* (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).

(ii) An appeal, including all supporting documentation, must be filed within 30 days of the filing of the intent to appeal.

(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) *Assignment of a hearing officer.* The National Coordinator will arrange for assignment of the case to a hearing officer to adjudicate the appeal on his or her behalf.

(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.

(ii) The hearing officer must be trained in a nationally recognized ethics code that articulates nationally recognized standards of conduct for hearing officers/officials.

(iii) The hearing officer must be an officer properly appointed by the Secretary of Health and Human Services.

(6) *Adjudication.* (i) The hearing officer may make a determination based on:

(A) The written record, which includes the:

(*1*) National Coordinator determination and supporting documentation;

(*2*) Information provided by the health IT developer with the appeal filed in accordance with paragraphs (g)(1) through (3) of this section; and

(*3*) Information ONC provides in accordance with paragraph (g)(6)(v) of this section; or(B) All the information provided in accordance with paragraph (g)(6)(i)(A) and any additional information from a hearing conducted in-person, via telephone, or otherwise.

(ii) The hearing officer will have the discretion to conduct a hearing if he/she:

(A) Requires clarification by either party regarding the written record under paragraph (g)(6)(i)(A) of this section;

(B) Requires either party to answer questions regarding the written record under paragraph (g)(6)(i)(A) of this section; or

(C) Otherwise determines a hearing is necessary.

(iii) The hearing officer will neither receive witness testimony nor accept any new information beyond what was provided in accordance with paragraph (g)(6)(i) of this section.

(iv) The default process will be a determination in accordance with paragraph (g)(6)(i)(A) of this section.

(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, the National Coordinator's determination to suspend or terminate the certification or issue a certification ban.

(7) *Determination by the hearing officer.* (i) The hearing officer will issue a written determination to the health IT developer within a timeframe agreed to by the health IT developer and ONC and approved by the hearing officer, unless the National Coordinator cancels the suspension or rescinds the termination determination.

(ii) The determination on appeal, as issued by the hearing officer, becomes final thirty (30) calendar days after the hearing officer sent notice of the determination to the health IT developer unless the Secretary, at the Secretary's sole discretion, chooses within that time to review the determination and decides to revise or rescind the determination.

■ 25. Amend § 170.581 by:

■ a. Revising paragraphs (a)(1)(i) and (a)(2);

■ b. Adding paragraph (a)(3); and

■ c. Revising paragraphs (b) introductory text and (d)(4).

The revisions and addition read as follows:

§ 170.581 Certification Ban

(a) * * *

(1) * * *

(i) Terminated by ONC under § 170.580(f);

* * * * *

(2) The National Coordinator determines a certification ban is appropriate per ONC Direct Review under § 170.580(a)(2)(iii) or based on ONC's review of the record sent to ONC pursuant to § 170.523(x) and confirmation of a determination made by an ONC–ACB under § 170.556(d)(7).

(3) A certification ban determination made by the National Coordinator under paragraph (a)(2) of this section is subject to review by the Secretary, at the Secretary's sole discretion, at any time prior to its effective date.

(b) *Notice of certification ban.* When the National Coordinator 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:

* * * * *

(d) * * *

(4) Upon review of ONC's assessment of the developer's demonstration under paragraph (d)(2) of this section and recommendation, the National Coordinator determines the health IT developer's demonstration under paragraph (d)(2) satisfactory and grants reinstatement into the ONC Health IT Certification Program.

PART 171—INFORMATION BLOCKING

■ 26. The authority citation for part 171 continues to read as follows:

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

■ 27. Amend § 171.101 by adding paragraph (c) to read as follows:

§ 171.101 Applicability

* * * * *

(c) If any provision of this part is held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or circumstance, it shall be construed to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

■ 28. Amend § 171.102 by adding definitions for ''Business day or business days'', ''Health information technology'', and ''Reproductive health care'' in alphabetical order and by revising the definition of ''Health care provider'' to read as follows:

§ 171.102 Definitions.

* * * * *

Business day or *business days* is defined as it is in § 170.102.

* * * * *

Health care provider has the same meaning as ''health care provider'' in 42 U.S.C. 300jj(3), within which for purposes of this definition:

(1) *Laboratory* has the same meaning as ''laboratory'' in 42 U.S.C. 300jj(10); and

(2) *Pharmacist* has the same meaning as ''pharmacist'' in 42 U.S.C. 300jj(12).

* * * * *

Health information technology or *health IT* has the same meaning as ''health information technology'' in 42 U.S.C. 300jj(5).

Reproductive health care is defined as it is in 45 CFR 160.103.

* * * * *

■ 29. Add § 171.104 to read as follows:

§ 171.104 Interferences.

(a) The following constitute practices that are likely to interfere with the access, exchange, or use of electronic health information (EHI) for purposes of § 171.103:

(1) *Delay on new access.* Delaying patient access to new EHI, such as diagnostic testing results, so clinicians or other actor representatives can review the EHI.

(2) *Portal access.* Delaying patient access to EHI in a portal when the actor has the EHI and the actor's system has the technical capability to support automated access, exchange, or use of the EHI via the portal.

(3) *API access.* Delaying the access, exchange, or use of EHI to or by a third-party app designated and authorized by the patient, when there is a deployed application programming interface (API) able to support the access, exchange, or use of the EHI.

(4) *Non-standard implementation.* Implementing health information

technology in ways that are likely to restrict access, exchange, or use of EHI with respect to exporting electronic health information, including, but not limited to, exports for transitioning between health IT systems.

(5) *Contract provisions.* Negotiating or enforcing a contract provision that restricts or limits otherwise lawful access, exchange, or use of EHI.

(6) *Non-compete provisions in agreements.* Negotiating or enforcing a clause in any agreement that:

(i) Prevents or restricts an employee (other than the actor's employees), a contractor, or a contractor's employee.

(ii) Who accesses, exchanges, or uses the EHI in the actor's health IT.

(iii) From accessing, exchanging, or using EHI in other health IT in order to design, develop, or upgrade such other health IT.

(7) *Manner or content requested.* Improperly encouraging or inducing requestors to limit the scope, manner, or timing of EHI requested for access, exchange, or use.

(8) *Medical images.* Requiring that the access, exchange, or use of any medical images (including, but not limited to, photograph, x-rays, and imaging scans) occur by exchanging physical copies or copies on physical media (such as thumb drive or DVD) when the actor and the requestor possess the technical capability to access, exchange, or use the images through fully electronic means.

(9) *Omissions.* The following omissions:

(i) Not exchanging EHI under circumstances in which such exchange is lawful;

(ii) Not making EHI available for lawful use;

(iii) Not complying with another valid law enforceable against the actor that requires access, exchange or use of EHI;

(iv) A Certified API Developer (as defined in 45 CFR 170.404) failing to publish API discovery details as required by the maintenance of certification requirement in 45 CFR 170.404(b)(2);

(v) An API Information Source (as defined in 45 CFR 170.404) failing to disclose to the Certified API Developer the information necessary for the Certified API Developer to publish the API discovery details required by 45 CFR 170.404(b)(2).

(b) The acts and omissions that will constitute practices that are likely to interfere with the access, exchange, or use of electronic health information (EHI) for purposes of § 171.103 include acts and omissions beyond those listed in paragraph (a) of this section.

■ 30. Amend § 171.202 by revising paragraphs (a)(2), (d), and (e) introductory text to read as follows:

§ 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?

* * * * *

(a) * * *

(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)(2)(i) 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)(2)(i) or (ii) of this section.

(v) An executor, administrator, or other person having authority to act on behalf of a deceased person described in paragraph (a)(2)(i) or (ii) of this section or the individual's estate under State or other law.

* * * * *

(d) *Sub-exception—interfering with individual access based on unreviewable grounds.*

Regardless of whether the actor is otherwise required to comply with 45 CFR 164.524, the actor's practice must be implemented in circumstances consistent with 45 CFR 164.524(a)(2) and must meet the implementation specifications that apply under 45 CFR 164.524 to denial of access on unreviewable grounds.

(e) *Sub-exception—individual's request not to share EHI.* An actor may elect not to provide access, exchange, or use of an individual's electronic health information if the following requirements are met—

* * * * *

■ 31. Amend § 171.204 by revising paragraphs (a)(2) and (3) and (b) to read as follows:

§ 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?

(a) * * *

(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) Is not permitted by applicable law to be made available; or

(ii) May be withheld in accordance with § 171.201, § 171.202, or § 171.206.

* * * * *

(3) *Third party seeking modification use.* The request is to enable use of EHI in order to modify EHI provided that the request for such use is not from any of the following:

(i) A covered entity as defined in 45 CFR 160.103 requesting such use from an actor that is its business associate as defined in 45 CFR 160.103.

(ii) A health care provider, as defined in § 171.102 and who is not a covered entity as defined in 45 CFR 160.103, requesting such use from an actor who engages in activities that would make the actor the health care provider's business associate if the health care provider were a covered entity.

* * * * *

(b) *Responding to requests.* The actor must respond to the requestor as specified below based on the condition in paragraph (a) of this section that applies to the actor's not fulfilling the particular requested access, exchange, or use of electronic health information:

(1) If an actor does not fulfill a request for access, exchange, or use of electronic health information for reasons consistent with paragraph (a)(1), (2), or (3) of this section, the actor must, within ten business days of the actor receiving the request, inform the requestor in writing of the reason(s) that request is infeasible.

(2) If an actor does not fulfill a request for access, exchange, or use of electronic health information for reasons consistent with paragraph (a)(4) or (5) of this section, the actor must:

(i) Determine, without unnecessary delay and based on a reasonable assessment of the facts, that the requested access, exchange, or use cannot be provided in accordance with § 171.301 or is infeasible under the circumstances; and

(ii) Inform the requestor in writing of the reason(s) that request is infeasible within ten business days of the determination under paragraph (b)(2)(i) of this section.

■ 32. Add § 171.206 to read as follows:

§ 171.206 Protecting Care Access—When will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to reduce potential exposure to legal action not be considered information blocking?

An actor's practice that is implemented to reduce potential exposure to legal action will not be considered information blocking when the practice satisfies the condition in paragraph (a) of this section and also satisfies the requirements of at least one of the conditions in paragraph (b) or (c) of this section.

(a) *Threshold condition.* To satisfy this condition, a practice must meet each of the following requirements:

(1) *Belief.* The practice is undertaken based on the actor's good faith belief that:

(i) Persons seeking, obtaining, providing, or facilitating reproductive health care are at risk of being potentially exposed to legal action that could arise as a consequence of particular access, exchange, or use of specific electronic health information; and

(ii) Specific practices likely to interfere with such access, exchange, or use of such electronic health information could reduce that risk.

(2) *Tailoring.* The practice is no broader than necessary to reduce the risk of potential exposure to legal action that the actor in good faith believes could arise from the particular access, exchange, or use of the specific electronic health information.

(3) *Implementation.* The practice is implemented either consistent with an organizational policy that meets paragraph (a)(3)(i) of this section or pursuant to a case-by-case determination that meets paragraph (a)(3)(ii) of this section.

(i) An organizational policy must:

(A) Be in writing;

(B) Be based on relevant clinical, technical, and other appropriate expertise;

(C) Identify the connection or relationship between the interference with particular access, exchange, or use of specific electronic health information and the risk of potential exposure to legal action that the actor believes the interference could reduce;

(D) Be implemented in a consistent and non-discriminatory manner; and

(E) Conform to the requirements in paragraphs (a)(1) and (2) of this section and to the requirements of at least one of the conditions in paragraph (b) or (c) of this section that are applicable to the prohibition of the access, exchange, or use of the electronic health information.

(ii) A case-by-case determination:

(A) Is made by the actor in the absence of an organizational policy applicable to the particular situation;

(B) Is based on facts and circumstances known to, or believed in good faith by, the actor at the time of the determination;

(C) Conforms to the conditions in paragraphs (a)(1) and (2) of this section; and

(D) Is documented either before or contemporaneous with engaging in any practice based on the determination. Documentation of the determination must identify the connection or relationship between the interference with particular access, exchange, or use of specific electronic health information and the risk of potential exposure to legal action.

(b) *Patient protection condition.* When implemented for the purpose of reducing the patient's risk of potential exposure to legal action, the practice must:

(1) Affect only the access, exchange, or use of specific electronic health information the actor in good faith believes could expose the patient to legal action because the electronic health information shows, or would carry a substantial risk of supporting a reasonable inference, that the patient:

(i) Obtained reproductive health care;

(ii) Inquired about or expressed an interest in seeking reproductive health care; or

(iii) Has any health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated.

(2) Be subject to nullification by an explicit request or directive from the patient that the access, exchange, or use of the specific electronic health information occur despite the risk(s) to the patient that the actor has identified.

(3) For purposes of paragraphs (b)(1) and (2) of this section, ''patient'' means the natural person who is the subject of the electronic health information or another natural person referenced in, or identifiable from, the EHI as a person who has sought or obtained reproductive health care.

(c) *Care access condition.* When implemented for the purpose of reducing the risk of potential exposure to legal action for one or more licensed health care professionals, other health care providers, or other persons involved in providing or facilitating reproductive health care that is lawful under the circumstances in which such health care is provided, the practice must affect only access, exchange, or use of specific electronic health information that the actor believes could expose a care provider(s) and facilitator(s) to legal action because the information shows, or would carry a substantial risk of supporting a reasonable inference, that they provide or facilitate, or have provided or have facilitated, reproductive health care.

(d) *Presumption.* For purposes of determining whether an actor's practice meets paragraph (b)(1)(i) or (c) of this section, care provided by someone other than the actor is presumed to have been lawful unless the actor has actual knowledge that the care was not lawful under the circumstances in which such care is provided.

(e) *Definition of legal action.* As used in this section, legal action means any one or more of the following—

(1) A criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care;

(2) A civil or criminal action brought in a court to impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care; or

(3) An administrative action or proceeding against any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

■ 33. Add § 171.304 to read as follows:

§ 171.304 Requestor preferences exception—When will an actor's practice of tailoring the access, exchange, or use of electronic health information to a requestor's preference(s) not be considered information blocking?

An actor's practice of tailoring the access, exchange, or use of electronic health information to a requestor's preference will not be considered information blocking when the practice meets the conditions in paragraphs (a) through (d) of this section.

(a) *Request.* A requestor, without any improper encouragement or inducement by the actor, requests in writing that the actor:

(1) Limit the scope of electronic health information made available for access, exchange, or use by the requestor;

(2) Delay provision of access, exchange, or use by the requestor of particular electronic health information until a condition specified by the requestor (such as passage of a particular event or completion of an action) has been met; or

(3) Delay provision of access, exchange, or use by the requestor of particular electronic health information for a specified period of time.

(b) *Implementation.* The actor's practice must be:

(1) Tailored to the specific request; and

(2) Implemented in a consistent and non-discriminatory manner.

(c) *Transparency.* The actor must explain to the requestor in plain language, whether verbally or in writing, what tailoring the actor will implement and must notify, verbally or in writing, any requestor(s) of changes in the actor's ability to maintain tailoring. To satisfy this condition, the actor must, at a minimum:

(1) Explain to the requestor what tailoring the actor will implement and how that will impact what EHI will be available to the requestor and when or under what conditions EHI will be available to the requestor;

(2) Upon the actor experiencing any change in operational status, technical capabilities, or other circumstances affecting the actor's ability or willingness to maintain particular tailoring of electronic health information, the actor must make reasonable efforts to promptly notify each requestor for which the actor had implemented the affected tailoring; and

(3) Contemporaneously document in writing any explanation consistent with paragraph (c)(1) of this section or notice consistent with paragraph (c)(2) of this section that is not provided in writing to the requestor.

(d) *Reduction or removal.* An actor must act on any subsequent request from the requestor who previously requested scope, condition, or timing tailoring of the requestor's EHI access, exchange, or use to reduce or remove restrictions as promptly as feasible.

■ 34. Revise § 171.401 to read as follows:

§ 171.401 Definitions.

Common Agreement has the meaning given to it in 45 CFR 172.102.

Framework Agreement has the meaning given to it in 45 CFR 172.102.

Participant has the meaning given to it in 45 CFR 172.102.

Qualified Health Information Network or *QHIN* has the meaning given to it in 45 CFR 172.102.

Subparticipant has the meaning given to it in 45 CFR 172.102.

■ 35. Add part 172 to read as follows:

PART 172—TRUSTED EXCHANGE FRAMEWORK AND COMMON AGREEMENT

Subpart A—General Provisions

Sec.
172.100 Basis, purpose, and scope.
172.101 Applicability.
172.102 Definitions.
172.103 Responsibilities ONC may delegate to the RCE.

Subpart B—Qualifications for Designation

172.200 Applicability.
172.201 QHIN Designation requirements.
172.202 QHINS that offer Individual Access Services.

Subpart C—QHIN Onboarding and Designation Processes

172.300 Applicability.
172.301 Submission of QHIN application.
172.302 Review of QHIN application.
172.303 QHIN approval and onboarding.
172.304 QHIN Designation.
172.305 Withdrawal of QHIN application.
172.306 Denial of QHIN application.
172.307 Re-application and renewed applications.

Subpart D—Suspension

172.400 Applicability.
172.401 QHIN suspensions.
172.402 Selective suspension of exchange between QHINs.

Subpart E—Termination

172.500 Applicability
172.501 QHIN self-termination.
172.502 QHIN termination.
172.503 Termination by mutual agreement.

Subpart F—Review of RCE Decisions

172.600 Applicability.
172.601 ONC review.
172.602 Basis for appeal by QHIN or applicant QHIN.
172.603 Method and timing for filing an appeal.
172.604 Effect of appeal on suspension and termination.
172.605 Assignment of a hearing officer.
172.606 Adjudication.
172.607 Determination by the hearing officer.

Subpart G—QHIN Attestation for the Adoption of the Trusted Exchange Framework and Common Agreement

172.700 Applicability.
172.701 Attestation submission and acceptance.
172.702 QHIN directory.

Authority: 42 U.S.C. 300jj–11; 5 U.S.C. 552.

Subpart A—General Provisions

§ 172.100 Basis, purpose, and scope.

(a) *Basis and authority.* The provisions of this part implement section 3001(c)(9) of the Public Health Service Act.

(b) *Purpose.* The purpose of this part is to:

(1) Ensure full network-to-network exchange of health information; and

(2) Establish a voluntary process for a Qualified Health Information Network™ (QHIN™) to attest to adoption of the Trusted Exchange Framework and Common Agreement™ (TEFCA™).

(c) *Scope.* This part addresses:

(1) Minimum qualifications needed for a health information network to be Designated as a QHIN capable of trusted exchange under TEFCA.

(2) Procedures governing QHIN Onboarding and Designation, suspension, termination, and further administrative review.

(3) Attestation submission requirements for a QHIN to attest to its adoption of TEFCA.

(4) ONC attestation acceptance and removal processes for publication of attesting QHINs in the QHIN Directory.

§ 172.101 Applicability.

(a) This part applies to Applicant QHINS, QHINs, terminated QHINs, and the Recognized Coordinating Entity.

(b) If any provision of this part is held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or circumstance, it shall be construed to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

§ 172.102 Definitions.

For purposes of this part, the following definitions apply:

Applicable Law means all Federal, State, local, or Tribal laws and regulations then in effect and applicable to the subject matter herein. For the avoidance of doubt, Federal agencies are subject only to Federal law.

Applicant QHIN means any organization with a pending QHIN application before the Office of the National Coordinator for Health Information Technology (ONC).

Business Associate Agreement (BAA) means a contract, agreement, or other arrangement that satisfies the implementation specifications described within 45 CFR parts 160 and 164 and subparts A, C, and E, as applicable.

Business day or *business days* has the meaning assigned to it in 45 CFR 170.102.

Common Agreement means the most recent version of the agreement referenced in section 3001(c)(9) of the Public Service Health Act as published in the **Federal Register**.

Confidential Information means any information that is designated as Confidential Information by the person or entity that discloses it, or that a reasonable person would understand to be of a confidential nature and is disclosed to another person or entity pursuant to TEFCA Exchange. For the avoidance of doubt, ''Confidential

Information'' does not include electronic protected health information (ePHI). Notwithstanding any label to the contrary, ''Confidential Information'' does not include any information that:

(1) Is or becomes known publicly through no fault of the Recipient; or

(2) Is learned by the recipient from a third party that the recipient reasonably believes is entitled to disclose it without restriction; or

(3) Is already known to the recipient before receipt from the discloser, as shown by the Recipient's written records; or

(4) Is independently developed by recipient without the use of or reference to the discloser's Confidential Information, as shown by the recipient's written records, and was not subject to confidentiality restrictions prior to receipt of such information from the discloser; or

(5) Must be disclosed under operation of law, provided that, to the extent permitted by Applicable Law, the recipient gives the discloser reasonable notice to allow the discloser to object to such redisclosure, and such redisclosure is made to the minimum extent necessary to comply with Applicable Law.

Connectivity Services means the technical services provided by a QHIN, Participant, or Subparticipant to its Participants and Subparticipants that facilitate TEFCA Exchange and are consistent with the technical requirements of the TEFCA framework.

Covered Entity has the meaning assigned to such term at 45 CFR 160.103.

Designated Network means the Health Information Network that a QHIN uses to offer and provide Designated Network Services.

Designated Network Services means the Connectivity Services and/or Governance Services.

Designation (including its correlative meanings ''*Designate,*'' ''*Designated,*'' and ''*Designating*''*)* means the written determination that an Applicant QHIN has satisfied all requirements and is now a QHIN.

Disclosure (including its correlative meanings ''*Disclose,*'' ''*Disclosed,*'' and ''*Disclosing*''*)* means the release, transfer, provision of access to, or divulging in any manner of TEFCA Information (TI) outside the entity holding the information.

Electronic Protected Health Information (ePHI) has the meaning assigned to such term at 45 CFR 160.103.

Exchange Purpose(s) or *XP(s)* means the reason for a transmission, Query, Use, Disclosure, or Response transacted through TEFCA Exchange as a step in the transaction. Types of Exchange Purposes include, but are not limited to, treatment, payment, health care operations, Individual Access Services, public health, and government benefits determination.

Exchange Purpose Code or *XP Code* means a code that identifies the Exchange Purpose being used for TEFCA Exchange.

Foreign Control means a non-U.S. Person(s) or non-U.S. Entity(ies) having the direct or indirect power, whether or not exercised, to direct or decide matters materially affecting the Applicant's ability to function as a QHIN in a manner that presents a national security risk.

Framework Agreement(s) means with respect to QHINs, the Common Agreement; and with respect to a Participant or Subparticipant, the Participant/Subparticipant Terms of Participation (ToP).

Governance Services means the governance functions described in applicable SOP(s), which are performed by a QHIN's Designated Network Governance Body for its Participants and Subparticipants to facilitate TEFCA Exchange in compliance with the then-applicable requirements of the Framework Agreements.

Health information network or *HIN* has the meaning assigned to it in 45 CFR 171.102.

Individual has the meaning assigned to such term at 45 CFR 171.202(a)(2).

HIPAA means the Health Insurance Portability and Accountability Act of 1996.

HIPAA Rules means the regulations set forth at 45 CFR parts 160, 162, and 164.

HIPAA Privacy Rule means the regulations set forth at 45 CFR parts 160 and 164 and subparts A and E.

HIPAA Security Rule means the regulations set forth at 45 CFR parts 160 and 164 and subparts A and C.

Individual Access Services (IAS) means the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant or Subparticipant, as applicable, agrees to satisfy that Individual's ability to access, inspect, or obtain a copy of that Individual's Required Information using TEFCA Exchange.

Individually Identifiable Information refers to information that identifies an Individual or with respect to which there is a reasonable basis to believe that the information could be used to identify an Individual.

Node means a technical system that is controlled directly or indirectly by a QHIN, Participant, or Subparticipant and that is listed in the RCE Directory Service.

Non-U.S. Entity means any Entity that is not a U.S. Entity.

Non-U.S. Person means any individual who is not a U.S. Qualified Person.

Onboarding means the process a prospective QHIN must undergo to become a QHIN and become operational in the production environment.

Organized Health Care Arrangement has the meaning assigned to such term at 45 CFR 160.103.

Participant means a U.S. Entity that has entered into the Participant/Subparticipant Terms of Participation in a legally binding contract with a QHIN to use the QHIN's Designated Network Services to participate in TEFCA Exchange in compliance with the Participant/Subparticipant Terms of Participation.

Participant/Subparticipant Terms of Participation (ToP) means the requirements to which QHINs must contractually obligate their Participants to agree; to which QHINs must contractually obligate their Participants to contractually obligate their Subparticipants and Subparticipants of the Subparticipants to agree, in order to participate in TEFCA Exchange including the QHIN Technical Framework (QTF), all applicable Standard Operating Procedures (SOPs), and all other attachments, exhibits, and artifacts incorporated therein by reference.

Qualified Health Information Network™ or *QHIN*™ means a Health Information Network that has been so Designated.

Query(s) (including its correlative uses/tenses ''*Queried*'' and ''*Querying*''*)* means the act of asking for information through TEFCA Exchange.

Recognized Coordinating Entity® or *RCE*™ means ONC's contractor that administers the implementation of TEFCA.

Required Information means the Electronic Health Information, as defined in 45 CFR 171.102, that is:

(1) Maintained in a Responding Node by any QHIN, Participant, or Subparticipant prior to or during the term of the applicable Framework Agreement; and

(2) Relevant for a required XP Code.

Response(s) (including its correlative uses/tenses ''*Responds,*'' ''*Responded*'' and ''*Responding*''*)* means the act of providing the information that is the subject of a Query or otherwise

transmitting a message in response to a Query through TEFCA Exchange.

Subparticipant means a U.S. Entity that has entered into the Participant/Subparticipant Terms of Participation in a legally binding contract with a Participant or another Subparticipant to use the Participant's or Subparticipant's Connectivity Services to participate in TEFCA Exchange in compliance with the Participant/Subparticipant Terms of Participation.

TEFCA Dispute Resolution Process means an informal, non-binding process under TEFCA through which QHINs can meet, confer, and seek to amicably resolve disputes.

TEFCA Exchange means the transaction of information between Nodes using an XP Code.

TEFCA Information or TI means any information that is transacted through TEFCA Exchange except to the extent that such information is received by a QHIN, Participant, or Subparticipant that is a Covered Entity, Business Associate, or non-HIPAA entity that is exempt from compliance with the Privacy section of the applicable Framework Agreement and is incorporated into such recipient's system of record, at which point the information is no longer TEFCA Information with respect to such recipient and is governed by the HIPAA Rules and other Applicable Law.

TEFCA Security Incident means:

(1) An unauthorized acquisition, access, Disclosure, or Use of unencrypted TEFCA Information using TEFCA Exchange, except any of the following:

(i) Any unintentional acquisition, access, Use, or Disclosure of TEFCA Information by a Workforce Member or person acting under the authority of a QHIN, Participant, or Subparticipant, if such acquisition, access, Use, or Disclosure:

(A) Was made in good faith;

(B) Was made by a person acting within their scope of authority;

(C) Was made to another Workforce Member or person acting under the authority of any QHIN, Participant, or Subparticipant; and

(D) Does not result in further acquisition, access, Use, or Disclosure in a manner not permitted under Applicable Law and the Framework Agreements.

(ii) A Disclosure of TI where a QHIN, Participant, or Subparticipant has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

(iii) A Disclosure of TI that has been de-identified in accordance with the standard at 45 CFR 164.514.

(2) Other security events that adversely affect a QHIN's, Participant's, or Subparticipant's participation in TEFCA Exchange.

Threat Condition means:

(1) A breach of a material provision of a Framework Agreement that has not been cured within fifteen (15) calendar days of receiving notice of the material breach (or such other period of time to which the contracting parties have agreed), which written notice shall include such specific information about the breach that is available at the time of the notice; or

(2) A TEFCA Security Incident; or

(3) An event that ONC (or an RCE), a QHIN, its Participant, or their Subparticipant has reason to believe will disrupt normal TEFCA Exchange, either:

(i) Due to actual compromise of, or the need to mitigate demonstrated vulnerabilities in, systems or data of the QHIN, Participant, or Subparticipant, as applicable; or

(ii) Through replication in the systems, networks, applications, or data of another QHIN, Participant, or Subparticipant; or

(4) Any event that could pose a risk to the interests of national security as directed by an agency of the United States government.

Trusted Exchange Framework means the most recent version of the framework referenced in section 3001(c)(9) of the Public Service Health Act published in the **Federal Register**.

U.S. Entity/Entities means any corporation, limited liability company, partnership, or other legal entity that meets all of the following requirements:

(1) The entity is organized under the laws of a State or commonwealth of the United States or the Federal law of the United States and is subject to the jurisdiction of the United States and the State or commonwealth under which it was formed;

(2) The entity's principal place of business, as determined under Federal common law, is in the United States; and

(3) None of the entity's directors, officers, or executives, and none of the owners with a five percent (5%) or greater interest in the entity, are listed on the *Specially Designated Nationals and Blocked Persons List* published by the United States Department of the Treasury's Office of Foreign Asset Control or on the United States Department of Health and Human Services, Office of Inspector General's List of Excluded Individuals/Entities.

U.S. Qualified Person means those individuals who are U.S. nationals and citizens at birth as defined in 8 U.S.C 1401, U.S. nationals but not citizens of the United States at birth as defined in 8 U.S.C. 1408, lawful permanent residents of the United States as defined in Immigration and Nationality Act, and non-immigrant aliens who are hired by a U.S. Entity as an employee in a specialty occupation pursuant to an H–1B Visa.

Use(s) (including correlative uses/tenses, such as ''Uses,'' ''Used,'' and ''Using''), with respect to TI, means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

§ 172.103 Responsibilities ONC may delegate to the RCE.

(a) ONC may delegate to the RCE the TEFCA implementation responsibilities specified in the following sections:

(1) Any section(s) of subpart C of this part;

(2) Any section(s) of subpart D of this part;

(3) Section 172.501; and

(4) Section 172.503.

(b) Any authority exercised by the RCE under this section is subject to review under subpart F of this part.

Subpart B—Qualifications for Designation

§ 172.200 Applicability.

This subpart establishes Designation qualifications.

(a) *Applicant QHIN.* An Applicant QHIN must meet all requirements in § 172.201 to be Designated. An Applicant QHIN that proposes to offer Individual Access Services must also meet all requirements in § 172.202 to be Designated.

(b) *QHIN.* A QHIN must continue to meet all requirements in § 172.201 to maintain its Designation. A QHIN that offers Individual Access Services must also continue to meet all requirements in § 172.202 to maintain its Designation.

(c) *Performance of TEFCA Exchange.* The Designation qualifications in §§ 172.201 and 172.202 describe certain requirements for Designation.

§ 172.201 QHIN Designation requirements.

(a) *Ownership requirements.* An entity must:

(1) be a U.S. Entity;

(2) Not be under Foreign Control.

(b) *Exchange requirements.* An entity must, beginning at the time of application, either directly or through the experience of its parent entity:

(1) Be capable of exchanging information among more than two unaffiliated organizations;

(2) Be capable of exchanging all Required Information;

(3) Be exchanging information for at least one Exchange Purpose authorized under TEFCA;

(4) Be capable of receiving and responding to transactions from other QHINs for all Exchange Purposes authorized under TEFCA;

(5) Be capable of initiating transactions for the Exchange Purposes authorized under TEFCA that such entity will permit its Participants and Subparticipants to use through TEFCA Exchange.

(c) *Designated Network Services requirements.* An entity must:

(1) Maintain the organizational infrastructure and legal authority to operate and govern its Designated Network;

(2) Maintain adequate written policies and procedures to support meaningful TEFCA Exchange and fulfill all responsibilities of a QHIN in this Part;

(3) Maintain a Designated Network that can support a transaction volume that keeps pace with the demands of network users;

(4) Maintain the capacity to support secure technical connectivity and data exchange with other QHINs;

(5) Maintain an enforceable dispute resolution policy governing Participants in the Designated Network that permits Participants to reasonably, timely, and fairly adjudicate disputes that arise between each other, the QHIN, or other QHINs;

(6) Maintain an enforceable change management policy consistent with the responsibilities of a QHIN;

(7) Maintain a representative and participatory group or groups with the authority to approve processes for governing the Designated Network;

(8) Maintain privacy and security policies that permit the entity to support TEFCA Exchange;

(9) Maintain data breach response and management policies that support meaningful TEFCA Exchange; and

(10) Maintain adequate financial and personnel resources to support all its responsibilities as a QHIN, including sufficient financial reserves or insurance-based cybersecurity coverage, or a combination of both.

§ 172.202 QHINs that offer Individual Access Services.

The following requirements apply to QHINs that offer Individual Access Services:

(a) A QHIN must obtain express consent from any individual before providing Individual Access Services.

(b) A QHIN must make publicly available a privacy and security notice that meets minimum TEFCA standards.

(c) A QHIN, that is the IAS provider for an individual, must delete the individual's Individually Identifiable Information maintained by the QHIN upon request by the individual except as prohibited by Applicable Law or where such information is contained in audit logs.

(d) A QHIN must permit any individual to export in a computable format all of the individual's Individually Identifiable Information maintained by the QHIN as an Individual Access Services provider.

(e) All Individually Identifiable Information the QHIN maintains must satisfy the following criteria:

(1) All Individually Identifiable Information must be encrypted.

(2) Without unreasonable delay and in no case later than sixty (60) calendar days following discovery of the unauthorized acquisition, access, Disclosure, or Use of Individually Identifiable Information, the QHIN must notify in plain language each individual whose Individually Identifiable Information has been or is reasonably believed to have been affected by unauthorized acquisition, access, Disclosure, or Use involving the QHIN.

(3) A QHIN must have an agreement with a qualified, independent third-party credential service provider and must verify, through the credential service provider, the identities of individuals seeking Individual Access Services prior to the individuals' first use of such services and upon expiration of their credentials.

Subpart C—QHIN Onboarding and Designation Processes

§ 172.300 Applicability.

This subpart establishes, as to QHINs, the application, review, Onboarding, withdrawal, and redetermination processes for Designation.

§ 172.301 Submission of QHIN application.

An entity seeking to be Designated as a QHIN must submit all of the following information in a manner specified by ONC:

(a) Completed QHIN application, with supporting documentation, in a form specified by ONC; and

(b) A signed copy of the Common Agreement.

§ 172.302 Review of QHIN application.

(a) ONC (or an RCE) will review a QHIN application to determine if the Applicant QHIN has completed all parts of the application and provided the necessary supporting documentation. If the QHIN application is not complete, the applicant will be notified in writing of the missing information within thirty (30) calendar days of receipt of the application. This timeframe may be extended by providing written notice to the Applicant QHIN.

(b) Once the QHIN application is complete, ONC (or an RCE) will review the application to determine whether the Applicant QHIN satisfies the requirements for Designation set forth in § 172.201 and, if the Applicant QHIN proposes to provide IAS, the requirements set forth in § 172.202. ONC (or an RCE) will complete its review within sixty (60) calendar days of the Applicant QHIN being provided with written notice that its application is complete. This timeframe may be extended by providing written notice to the Applicant QHIN.

(c) Additional information may be requested from the Applicant QHIN while ONC (or an RCE) is reviewing the application. The timeframe for responding to the request and the manner to submit additional information will be provided to the applicant and may be extended on written notice to the Applicant QHIN.

(d) Failure to respond to a request within the proposed timeframe or in the manner specified is a basis for a QHIN Application to be deemed withdrawn, as set forth in § 172.305(c). In such situations, the Applicant QHIN will be provided with written notice that the application has been deemed withdrawn.

(e) If, following submission of the application, any information submitted by the Applicant QHIN becomes untrue or materially changes, the Applicant QHIN must notify ONC (or an RCE) in the manner specified by ONC (or an RCE) of such changes in writing within five (5) business days of the submitted material becoming untrue or materially changing.

§ 172.303 QHIN approval and Onboarding.

(a) An Applicant QHIN has the burden of demonstrating its compliance with all qualifications for Designation in § 172.201 and, if the Applicant QHIN proposes to provide IAS, the qualifications in § 172.202.

(b) If ONC (or an RCE) determines that an Applicant QHIN meets the requirements for Designation set forth in § 172.201, and if the Applicant QHIN proposes to provide IAS, the qualifications set forth in § 172.202, then ONC (or an RCE) will notify the applicant in writing that its application has been approved, and the Applicant QHIN may proceed with Onboarding.

(c) An approved Applicant QHIN must submit a signed version of the Common Agreement within a timeframe set by ONC (or an RCE).

(d) An approved Applicant QHIN must complete the Onboarding process, including any tests required to ensure the Applicant QHIN's network can connect to those of other QHINs and other Applicant QHINs, within twelve (12) months of approval of its QHIN application, unless that timeframe is extended in ONC (or an RCE's) sole discretion by up to twelve (12) months.

§ 172.304 QHIN designation.

(a) If all requirements of the Onboarding process specified in § 172.303 have been satisfied:

(1) The Common Agreement will be countersigned; and

(2) The Applicant QHIN will be provided with a written determination indicating that the applicant has been provisionally Designated as a QHIN, along with a copy of the countersigned Common Agreement.

(b) Within thirty (30) calendar days of receiving its provisional Designation, each QHIN must demonstrate in a manner specified by ONC (or an RCE) that it has completed a successful transaction with all other in-production QHINs according to standards and procedures for TEFCA Exchange.

(c) If a QHIN is unable to complete the requirement in subsection (b) of this section within the thirty (30)-day period provided, the QHIN must provide ONC (or an RCE) with a written explanation of why the QHIN has been unable to complete a successful transaction with all other in-production QHINs within the allotted time and include a detailed plan and timeline for completion of a successful transaction with all other in-production QHINs. The QHIN's plan will be reviewed and either approved or rejected based on the reasonableness of the explanation and the specific facts and circumstances, within five (5) business days of receipt. If the QHIN fails to provide its plan or the plan is rejected, ONC (or an RCE) will rescind its provisional approval of the application, rescind the provisional QHIN Designation, and deny the application. Within thirty (30) calendar days of end of the term of the plan, each QHIN must demonstrate in a manner specified by ONC (or an RCE) that it has completed a successful transaction with all other in-production QHINs according to standards and procedures for TEFCA Exchange.

(d) A QHIN Designation will become final sixty (60) days after a Designated QHIN has submitted its documentation that it has completed a successful transaction with all other in-production QHINs.

§ 172.305 Withdrawal of QHIN application.

(a) An Applicant QHIN may voluntarily withdraw its QHIN application by providing written notice in a manner specified by ONC (or an RCE).

(b) An Applicant QHIN may withdraw its QHIN application at any point prior to Designation.

(c) Upon written notice to the Applicant QHIN, a QHIN application may be deemed withdrawn as a result of the Applicant QHIN's failure to respond to requests for information from ONC (or an RCE).

§ 172.306 Denial of QHIN application.

If an Applicant QHIN's application is denied, the Applicant QHIN will be provided with written notice that includes the basis for the denial.

§ 172.307 Re-application.

(a) Subject to paragraphs (b), (c), and (d) of this section, applications may be resubmitted by Applicant QHINs by complying with the provisions of § 172.301 in the event that an application is denied or withdrawn.

(b) The Applicant QHIN may reapply at any time after it has voluntarily withdrawn its application as specified in § 172.305(a).

(c) If ONC (or an RCE) deems a QHIN application to be withdrawn as a result of the Applicant QHIN's failure to respond to requests for information, then the Applicant QHIN may reapply by submitting a new QHIN application no sooner than six (6) months after the date on which its previous application was submitted. The Applicant QHIN must respond to the prior request for information and must include an explanation as to why no response was previously provided within the required timeframe.

(d) If ONC (or an RCE) denies a QHIN application, the Applicant QHIN may reapply by submitting a new application consistent with the requirements in § 172.301 no sooner than six (6) months after the date shown on the written notice of denial. The application must specifically address the deficiencies that constituted the basis for denying the Applicant QHIN's previous application.

Subpart D—Suspension

§ 172.400 Applicability.

This subpart describes suspension responsibilities, notice requirements for suspension, and the effect of suspension.

§ 172.401 QHIN suspensions.

(a) A QHIN's authority to engage in TEFCA Exchange may be suspended if ONC (or an RCE) determines that the QHIN is responsible for a Threat Condition.

(b) If ONC (or an RCE) determines that one of a QHIN's Participants or Subparticipants has done something or failed to do something that resulted in a Threat Condition, ONC (or an RCE) may direct the QHIN to suspend that Participant's or Subparticipant's authority to engage in TEFCA Exchange.

(c) ONC (or an RCE) will make a reasonable effort to notify a QHIN in writing in advance of an intent to suspend the QHIN or to provide direction to the QHIN to suspend one of the QHIN's Participants or Subparticipants, and to give the QHIN an opportunity to respond. Such notice will identify the Threat Condition giving rise to such suspension.

(d) ONC (or an RCE) shall lift a suspension of either the QHIN or one of the QHIN's Participants or Subparticipants once the Threat Condition is resolved.

§ 172.402 Selective suspension of exchange between QHINs.

(a) A QHIN may, in good faith and to the extent permitted by Applicable Law, suspend TEFCA Exchange with another QHIN because of reasonable concerns related to the privacy and security of information that is exchanged.

(b) If a QHIN decides to suspend TEFCA Exchange with another QHIN, it is required to promptly notify, in writing, ONC (or an RCE) and the QHIN with which it is suspending exchange of its decision and the reason(s) for making the decision.

(c) If a QHIN suspends TEFCA Exchange with another QHIN under paragraph (a) of this section, it must, within thirty (30) calendar days, initiate the TEFCA Dispute Resolution Process in order to resolve the issues that led to the decision to suspend, or the QHIN may end its suspension and resume TEFCA Exchange with the other QHIN within thirty (30) calendar days of suspending TEFCA Exchange with the QHIN.

(d) Provided that a QHIN suspends TEFCA exchange with another QHIN in accordance with this section and in accordance with Applicable Law, such suspension will not be deemed a violation of the Common Agreement.

Subpart E—Termination

§ 172.500 Applicability.

This subpart establishes QHIN termination responsibilities, notice

requirements for termination, and the effect of termination.

§ 172.501 QHIN self-termination.

A QHIN may terminate its own Designation at any time without cause by providing ninety (90) calendar days prior written notice.

§ 172.502 QHIN termination.

A QHIN's Designation will be terminated with immediate effect by ONC (or an RCE) giving written notice of termination to the QHIN if the QHIN:

(a) Fails to comply with any of the regulations of this part and fails to remedy such material breach within thirty (30) calendar days after receiving written notice of such failure; provided, however, that if a QHIN is diligently working to remedy its material breach at the end of this thirty- (30-) day period, then ONC (or an RCE) must provide the QHIN with up to another thirty (30) calendar days to remedy its material breach; or

(b) A QHIN breaches a material provision of the Common Agreement where such breach is not capable of remedy.

§ 172.503 Termination by mutual agreement.

A QHIN's Designation may be terminated at any time and for any reason by mutual, written agreement between the QHIN and ONC (or an RCE).

Subpart F—Review of RCE or ONC Decisions

§ 172.600 Applicability.

This subpart establishes processes for review of RCE or ONC actions, including QHIN appeal rights and the process for filing an appeal.

§ 172.601 ONC review.

(a) ONC may, in its sole discretion, review all or any part of any RCE determination, policy, or action.

(b) ONC may, in its sole discretion and on notice to affected QHINs or Applicant QHINs, stay any RCE determination, policy, or other action pending ONC review.

(c) ONC may, in its sole discretion and on written notice, request that a QHIN, Applicant QHIN, or the RCE provide ONC additional information regarding any RCE determination, policy, or other action.

(d) On completion of its review, ONC may affirm, modify, or reverse the determination, policy, or other action under review. ONC will provide notice to affected QHINs or Applicant QHINs that includes the basis for ONC's decision.

(e) ONC will provide written notice under this section to affected QHINs or Applicant QHINs in the same manner as the original RCE determination, policy, or other action under review.

§ 172.602 Basis for appeal by QHIN or applicant QHIN.

An Applicant QHIN or QHIN may appeal the following decisions to ONC or a hearing officer, as appropriate:

(a) *Applicant QHIN.* An Applicant QHIN may appeal a denial of its QHIN application.

(b) *QHIN.* A QHIN may appeal:

(1) A decision to suspend the QHIN or to instruct the QHIN to suspend its Participant or Subparticipant.

(2) A decision to terminate the QHIN's Common Agreement.

§ 172.603 Method and timing for filing an appeal.

(a) To initiate an appeal, an authorized representative of the Applicant QHIN or QHIN must submit electronically, in writing to ONC, a notice of appeal that includes the date of the notice of appeal, the date of the decision being appealed, the Applicant QHIN or QHIN that is appealing, and the decision being appealed within fifteen (15) calendar days of the Applicant QHIN's or QHIN's receipt of the notice of denial of a QHIN application, suspension or instruction to suspend its Participant or Subparticipant, or termination. With regard to an appeal of a termination, the 15-calendar day timeframe may be extended by ONC up to another fifteen (15) calendar days if the QHIN has been granted an extension for completing its remedy under § 172.502(a).

(b) An authorized representative of an Applicant QHIN or QHIN must submit electronically to ONC, within thirty (30) calendar days of filing the intent to appeal, the following:

(1) A statement of the basis for appeal, including a description of the facts supporting the appeal with citations to documentation submitted by the QHIN or Applicant QHIN; and

(2) Any documentation the QHIN would like considered during the appeal.

(c) The Applicant QHIN or QHIN filing the appeal may not submit on appeal any evidence that it did not submit prior to the appeal except evidence permitted by the hearing officer under § 172.606.

§ 172.604 Effect of appeal on suspension and termination.

An appeal does not stay the suspension or termination, unless otherwise ordered by ONC or the hearing officer assigned under § 172.605(b).

§ 172.605 Assignment of a hearing officer.

(a) On receipt of an appeal under § 172.603, ONC may exercise its authority under § 172.601 to review an RCE determination being appealed. An appealing QHIN or Applicant QHIN that is not satisfied with ONC's subsequent determination may appeal that determination to a hearing officer by filing a new notice of appeal and other appeal documents that comply with § 172.603.

(b) If ONC declines review under paragraph (a) of this section, or if ONC made the determination under review, ONC will arrange for assignment of the case to a hearing officer to adjudicate the appeal.

(c) The hearing officer must be an officer appointed by the Secretary of Health and Human Services.

(d) The hearing officer may not be responsible to, or subject to the supervision or direction of, personnel engaged in the performance of investigative or prosecutorial functions for ONC, nor may any officer, employee, or agent of ONC engaged in investigative or prosecutorial functions in connection with any adjudication, in that adjudication or one that is factually related, participate or advise in the decision of the hearing officer, except as a counsel to ONC or as a witness.

§ 172.606 Adjudication.

(a) The hearing officer will decide issues of law and fact *de novo* and will apply a preponderance of the evidence standard when deciding appeals.

(b) In making a determination, the hearing officer may consider:

(1) The written record, which includes:

(i) The RCE's or ONC's determination and supporting information;

(ii) Appeal materials submitted by the Applicant QHIN or QHIN under § 172.603.

(2) Any information from a hearing conducted in-person, via telephone, or otherwise. The hearing officer has sole discretion to conduct a hearing:

(i) To require either party to clarify the written record under paragraph (b)(1) of this section;

or

(ii) If the hearing officer otherwise determines a hearing is necessary.

(c) The hearing officer will neither receive witness testimony nor accept any new information beyond what was provided in accordance with paragraph (b) of this section, except for good cause shown by the party seeking to submit new information.

§ 172.607 Determination by the hearing officer.

(a) The hearing officer will issue a written determination.

(b) The hearing officer's determination on appeal is the final decision of HHS unless within 10 business days, the Secretary, in the Secretary's sole discretion, chooses to review the determination. ONC will notify the appealing party if the Secretary chooses to review the determination and will provide notice of the Secretary's final determination.

Subpart G—QHIN Attestation for the Adoption of the Trusted Exchange Framework and Common Agreement

§ 172.700 Applicability.

This subpart applies to QHINs.

§ 172.701 Attestation submission and acceptance.

(a) *Applicability.* This subpart establishes:

(1) The attestation submission requirements for QHINs.

(2) The review and acceptance processes that ONC will follow for TEFCA attestations.

(b) *Submission of QHIN attestation.* (1) In order to be listed in the QHIN directory described in § 172.702, a QHIN must submit all of the following information to ONC:

(i) Attestation affirming its:

(A) Agreement with and adherence to the Trusted Exchange Framework; and

(B) Adoption of the Common Agreement; and

(ii) General identifying information, including:

(A) Name, address, city, State, zip code, and a hyperlink to its website.

(B) Designation of an authorized representative, including the representative's name, title, phone number, and email address.

(iii) Documentation confirming its Designation as a QHIN.

(2) A QHIN must provide ONC with written notice of any changes to its identifying information provided in accordance with this paragraph (b) within thirty (30) business days of the change(s) to its identifying information.

(c) *Submission method.* A QHIN must electronically submit its attestation and documentation either via an email address identified by ONC or via a submission on the ONC website, if available.

(d) *Review and acceptance.* (1) Within thirty (30) business days, ONC will either accept or reject an attestation submission.

(2) ONC will accept an attestation if it determines that the QHIN has satisfied the requirements of paragraphs (b) and (c) of this section. ONC will provide written notice to the applicable QHIN's authorized representative that the attestation has been accepted.

(3) ONC will reject an attestation if it determines that the requirements of paragraph (b) or (c) of this section, or both, have not been satisfied.

(4) ONC will provide written notice to the QHIN's authorized representative of the determination along with the basis for the determination.

(5) An ONC determination under this section is final agency action and not subject to further administrative review, except the Secretary may choose to review the determination as provided in § 172.607(b). However, a QHIN may, at any time, resubmit an attestation in accordance with paragraphs (b) and (c) of this section.

§ 172.702 QHIN directory.

(a) *Applicability.* This subpart establishes processes for publishing a directory of QHINs on the ONC website.

(b) *Publication.* (1) Within fifteen (15) calendar days of notifying a QHIN that its QHIN submission has been accepted, ONC will publish, at a minimum, the QHIN's name in the QHIN directory on the ONC website.

(2) ONC will identify within the QHIN directory those QHINs that are suspended under the Common Agreement.

(c) *Removal from the QHIN directory.* (1) A QHIN whose Common Agreement has been terminated no longer qualifies to be included in the QHIN directory as it is no longer considered a QHIN and will be removed from the QHIN directory.

(2) Upon termination of a QHIN's Common Agreement, ONC (or an RCE) will send a written a statement of intent to remove the QHIN from the QHIN Directory to the authorized representative of the QHIN.

(3) Any written statement given under paragraph (c)(2) of this section shall consist of the following, as appropriate:

(i) The name of the terminated QHIN and the name and contact information of the authorized representative of the QHIN.

(ii) A short statement setting forth findings of fact with respect to any violation of the Common Agreement or other basis for the QHIN's termination under the Common Agreement and justifying the termination on the basis of those findings of facts.

(iii) Other materials as the ONC (or the RCE) may deem relevant.

(d) *Duration.* A QHIN that is removed from the QHIN directory will remain removed until a new attestation is accepted by ONC in accordance with the processes specified in this subpart.

(e) *Final agency action.* An ONC determination under this section is final agency action and not subject to further administrative review, except the Secretary may choose to review the determination as provided in § 172.607(b).

Xavier Becerra,

Secretary, Department of Health and Human Services.

[FR Doc. 2024–14975 Filed 7–24–24; 8:45 am]

BILLING CODE 4150–45–P