

DEPARTMENT OF HEALTH AND HUMAN SERVICES**Office of the Secretary****45 CFR Part 171**

RIN 0955-AA06

Health Data, Technology, and Interoperability: Protecting Care Access

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

ACTION: Final rule.

SUMMARY: This final rule has finalized certain proposals from the Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability Proposed Rule (HTI-2 Proposed Rule) and in doing so supports the access, exchange, and use of electronic health information. Specifically, this final rule amends the information blocking regulations to revise two existing information blocking exceptions and establish an additional reasonable and necessary activity that does not constitute information blocking referred to as the Protecting Care Access Exception.

DATES: This final rule is effective on December 17, 2024.

FOR FURTHER INFORMATION CONTACT: Kate Tipping, Office of Policy, Assistant Secretary for Technology Policy (ASTP)/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
 - B. Summary of Information Blocking Enhancements
 - C. Costs and Benefits
- II. Background
 - A. Statutory Basis
 - B. Regulatory History
- III. Information Blocking Enhancements
 - A. Out of Scope Comments
 - B. Exceptions
 - 1. Privacy Exception Updates
 - a. Privacy Exception—Definition of Individual
 - b. Privacy Sub-exception—Individual's Request Not To Share EHI
 - 2. Infeasibility Exception Updates
 - 3. New Protecting Care Access Exception
 - a. Background and Purpose
 - b. Threshold Condition and Structure of Exception
 - c. Patient Protection Condition
 - d. Care Access Condition

- e. Presumption Provision and Definition of "Legal Action"
- IV. Severability
- V. Waiver of Delay in Effective Date
- VI. Regulatory Impact Analysis
 - A. Statement of Need
 - B. Alternatives Considered
 - C. Overall Impact—
 - 1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis
 - D. Regulatory Flexibility Act
 - E. Executive Order 13132—Federalism
 - F. Unfunded Mandates Reform Act of 1995

I. Executive Summary*A. Purpose of Regulatory Action*

The Secretary of Health and Human Services has delegated responsibility to the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (hereafter ASTP/ONC)¹ to identify reasonable and necessary activities that do not constitute information blocking.² This final rule fulfills this responsibility; advances equity and innovation; and supports the access to, and exchange and use of, electronic health information (EHI).

The final rule is also consistent with Executive Order (E.O.) 14036. E.O. 14036, Promoting Competition in the American Economy,³ 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).⁴ In this rule, we have finalized 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.

¹ The Office of the National Coordinator for Health Information Technology (ONC) was the previous name of this office. See **Federal Register**: Statement of Organization, Functions, and Delegations of Authority; Office of The National Coordinator for Health Information Technology (89 FR 60903, July 29, 2024).

² 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. ASTP/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/>.

³ Executive Order 14036: Promoting Competition in the American Economy, Jul 9, 2021 (86 FR 36987).

⁴ Executive Order 13725: Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy, Apr 15, 2016 (81 FR 23417)

Addressing information blocking is critical for promoting innovation and competition in health IT and for the delivery of health care services to individuals, as discussed in both the March 4, 2019, proposed rule, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" (84 FR 7508 and 7523) (ONC Cures Act Proposed Rule) and the May 1, 2020 final rule, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" (85 FR 25790 and 25791) (ONC Cures Act Final Rule), and reiterated in the January 9, 2024 final rule, "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing" (89 FR 1195) (HTI-1 Final Rule). Specifically, we described (84 FR 7508 and 85 FR 25791) how the information blocking provision (section 3022 of the Public Health Service Act (PHSA) (42 U.S.C. 300jj-52)) provides 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.⁵ As we explained in the ONC Cures Act Final Rule, the PHSA information blocking provision itself expressly addresses practices that impede innovation and advancements in EHI access, exchange, and use, including care delivery enabled by health IT (85 FR 25820, 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

⁵ See, e.g., Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, Making Health Care Markets Work: Competition Policy for Health Care, *JAMA*, 317(13) 1313-1314 (Apr. 2017); Diego A. Martinez et al., A Strategic Gaming Model for Health Information Exchange Markets, *Health Care Mgmt. Science* 21, 119-130 (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 <https://www.brookings.edu/articles/a-sustainable-business-model-for-health-information-exchange-platforms-the-solution-to-interoperability-in-health-care-it/>; Thomas C. Tsai Ashish K. Jha, Hospital Consolidation, Competition, and Quality: Is Bigger Necessarily Better? 312 *JAMA* 312(1), 29030 (Jul 2014).

and users, provide new or improved capabilities, and enable more robust access, exchange, and use of EHI (85 FR 25820).⁶ Information blocking may also harm competition not just in health IT markets, but also in markets for health care 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 technological 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 of health care services (85 FR 25820). The revisions to the information blocking regulations, including the addition of the new exception finalized in this final rule, will continue to promote innovation and support the lawful access, exchange, and use of EHI, while strengthening support for individuals' privacy and EHI sharing preferences.

B. Summary of Information Blocking Enhancements

We received approximately 270 comment submissions on the broad range of proposals included in the "Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability" proposed rule (89 FR 63498) (*HTI-2 Proposed Rule*). We thank all commenters for their thoughtful input. For the purposes of this final rule, we have reviewed and responded to comments on a narrowed set of proposals. Specifically, we summarize and respond to comments related to the proposals finalized in this rule (described below). Comments received in response to other proposals from the *HTI-2 Proposed Rule* are beyond the scope of this final rule, have been addressed in the "Health Data, Technology, and Interoperability: Trusted Exchange Framework and Common Agreement (TEFCA™)" final rule (RIN 0955-AA07) (*HTI-2 Final Rule*) or are still being reviewed and considered. Comments related to proposals not discussed in this final rule or the *HTI-2 Final Rule* may be the subject of subsequent final rules related to such proposals in the future.

⁶ See also Martin Gaynor, Farzad Mostashari, and Paul B. Ginsberg, Making Health Care Markets Work: Competition Policy for Health Care, *JAMA*, 317(13) 1313–1314 (Apr. 2017).

On July 25, 2024, HHS announced a reorganization that, among other things, renamed the Office of the National Coordinator for Health Information Technology (ONC). ONC is now dually titled as the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ASTP/ONC) per the *Federal Register* notice that appeared in the *Federal Register* on July 29, 2024.⁷ It was not until days after the *HTI-2 Proposed Rule's* content had been released to the public (on July 10, 2024)⁸ that the name change was announced. Therefore, when the *HTI-2 Proposed Rule* appeared in the *Federal Register* on August 5, 2024, it retained reference to the office as "ONC." We continue to refer to "ONC" when referencing the *HTI-2 Proposed Rule* in this final rule. However, in the comment summaries and responses of this final rule, we have revised and replaced "ONC" references with "ASTP/ONC."

In this final rule, we have finalized the addition of a definition of "reproductive health care" to the defined terms for purposes of the information blocking regulations, which appear in 45 CFR 171.102. We have finalized select proposed revisions (proposed in the *HTI-2 Proposed Rule* at 89 FR 63620 through 63627 and 89 FR 63803) for two existing information blocking exceptions (Privacy Exception and Infeasibility Exception) in subpart B of 45 CFR part 171. Finally, we have finalized a new information blocking exception (Protecting Care Access) in subpart B of part 171.

C. 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 (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." The Office of Management and Budget's

⁷ Statement of Organization, Functions, and Delegations of Authority; Office of The National Coordinator for Health Information Technology (89 FR 60903).

⁸ <https://www.hhs.gov/about/news/2024/07/10/hhs-proposes-hti-2-rule-improve-patient-engagement-information-sharing-public-health-interoperability.html>.

(OMB) Office of Information and Regulatory Affairs (OIRA) has determined that this final rule is a significant regulatory action under section 3(f) of Executive Order 12866 as amended by E.O. 14094.

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 added to the Public Health Service Act (PHSA) "Title XXX—Health Information Technology and Quality" (Title XXX) to improve health care 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 Title XXX of the PHSA by modifying or adding certain provisions to the PHSA relating to health IT.

Information Blocking Under the 21st Century Cures Act

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

B. Regulatory History

On March 4, 2019, the *ONC Cures Act Proposed Rule* was published in the *Federal Register* (84 FR 7424). 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.

On May 1, 2020, the *ONC Cures Act Final Rule* was published in the *Federal Register* (85 FR 25642). The final rule implemented certain provisions of the Cures Act, including Conditions and Maintenance of Certification requirements for health IT developers

and the voluntary certification of health IT for use by pediatric health providers, and identified 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. Additionally, the ONC Cures Act Final Rule modified the 2015 Edition health IT certification criteria and ONC Health IT Certification Program (Program) in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs, as well as to improve patient and health care provider access to EHI and promote 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 health care 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, a proposed rule titled, "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing" (88 FR 23746) (HTI-1 Proposed Rule) was published in the **Federal Register**. 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 criteria 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 HTI-1 Final Rule was published in the **Federal Register**, 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 HTI-1 Final Rule provided enhancements to support information sharing under the information blocking regulations, including clarifying certain definitions and establishing a new "TEFCA Manner" Exception—which provides that an actor's practice of not fulfilling a request to access, exchange, or use EHI in any alternative manner besides via TEFCA will not be considered information blocking when the practice follows certain conditions (see 45 CFR 171.403 and 89 FR 1387 through 1394). 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 August 5, 2024, the HTI-2 Proposed Rule was published in the **Federal Register** (89 FR 63498). The HTI-2 Proposed Rule is the second of the Health Data, Technology, and Interoperability rules that seek to advance interoperability, improve transparency, and support the access, exchange, and use of electronic health information. The HTI-2 Proposed Rule included 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. Additionally, the HTI-2 Proposed Rule proposed to establish a new baseline version of the USCDI standard and proposed to update the ONC Health IT Certification Program to enhance interoperability and optimize certification processes to reduce burden and costs. The HTI-2 Proposed Rule also proposed to implement certain provisions related to TEFCA, which would support reliability, privacy, security, and trust within TEFCA. In the HTI-2 Final Rule (RIN 0955-AA07), we codified definitions of certain TEFCA terms in § 171.401 of the information blocking regulations and finalized the 45 CFR part 172 TEFCA provisions.

III. Information Blocking Enhancements

In the HTI-2 Proposed Rule, we proposed revisions to defined terms for purposes of the information blocking regulations, which appear in 45 CFR 171.102. Specifically, we proposed to clarify the definition of "health care provider" (89 FR 63616, 63617, and 63802) and adopt definitions for three terms not previously included in § 171.102: "business day" (89 FR 63601, 63602, 63626, and 63802), "health information technology or health IT" (89 FR 63617 and 63802), and "reproductive health care" (89 FR 63633 and 63802). Of these, we address in this final rule only the proposal to add to § 171.102 a definition of "reproductive health care" and comments received in response to that proposal. Comments received specific to other proposed revisions to § 171.102 are beyond the scope of this final rule but may be the subject(s) of a different final rule or rules related to such proposal(s).

We proposed to revise two existing exceptions in subpart B of 45 CFR part 171 (§ 171.202 and § 171.204) and solicited comment on potential revisions to one exception in subpart D (§ 171.403). We proposed revisions to paragraphs (a), (d), and (e) of § 171.202 (89 FR 63620 through 63622, and 63803) and to paragraphs (a)(2), (a)(3) and (b) of § 171.204 (89 FR 63622 through 63628, and 63803). In this final rule, we address comments received on or relevant to proposed revisions to paragraphs (a) and (e) of § 171.202 and paragraph (a)(2) of § 171.204. Comments received specific to proposed revisions to § 171.202(d), § 171.204(a)(3), and § 171.204(b) are beyond the scope of this final rule but may be the subject(s) of a future final rule related to such proposal(s).

We proposed two new exceptions, the Protecting Care Access Exception and the Requestor Preferences Exception, in subparts B and C of part 171 respectively. The Protecting Care Access Exception was proposed as new § 171.206 (89 FR 63627 through 63639, and 63804). We have finalized the proposed Protecting Care Access Exception (§ 171.206), and we address comments relevant to it in this final rule. Comments received specific to the Requestor Preferences Exception (§ 171.304) proposal (89 FR 63639 through 63642, 63804 and 63805) are beyond the scope of this final rule but may be a subject of a future final rule related to that proposal.

We proposed to codify in § 171.401 definitions of certain terms relevant to the Trusted Exchange Framework and

Common Agreement™ (TEFCA™) (89 FR 63642, 63804, and 63805) and in § 171.104 descriptions of certain practices that constitute interference with the access, exchange, and use of electronic health information (EHI) (89 FR 63617 through 63620, 63802, and 63803). We do not address either of those proposals in this final rule, and comments regarding them are also beyond the scope of this final rule. However, in the HTI–2 Final Rule (RIN 0955–AA07), we finalized the proposed definitions of certain terms relevant to TEFCA™ in § 171.401.

A. Out of Scope Comments

In addition to comments received on proposals that we included in the HTI–2 Proposed Rule, we received numerous comments that were beyond the scope of any proposal in the HTI–2 Proposed Rule. For example, we received comments recommending that ASTP/ONC revise an information blocking exception to which we had not proposed any revisions. We also received comments recommending that we adopt new requirements for actors' conduct or technology regarding which we did not make any related proposals in the HTI–2 Proposed Rule. While we do not specifically address in this final rule all comments received on matters beyond the scope of the HTI–2 Proposed Rule, nor do we intend to address them all in any other final rule, we do address some of them (below) prior to more in-depth discussions of comments received that are specifically related to proposals addressed in this final rule.

Comment. One commenter expressed support for greater transparency and timely access to health information for patients. However, they stated that the regulations as they exist today do not appropriately mitigate patient harm within the “Preventing Harm Exception.” They stated a belief that the Preventing Harm Exception does not account for the harm caused by immediate patient access to distressing or confusing laboratory test or imaging results. They stated a belief that “the strict definition outlined by ONC does not include emotional harm.” The commenter stated that certain scenarios require particularly sensitive care conversations, where patients are able to process the results with an experienced health care professional. Therefore, they urged that we clarify that the Preventing Harm Exception includes emotional distress.

Response. We thank the commenter for their feedback. As discussed in context of finalized revisions to the *segmentation* condition of the Infeasibility Exception (§ 171.204(a)(2)),

this rule retains application of the Infeasibility Exception in circumstances where an actor cannot unambiguously segment EHI they have chosen to withhold consistent with the Preventing Harm Exception (§ 171.201) from other EHI that they could share under applicable law. Any modification to the Preventing Harm Exception or other revision to 45 CFR part 171 to create a regulatory exception designed to cover situations where a health care provider may want to limit a patient's own access to their health information based on concern about the information being upsetting or confusing the patient is beyond the scope of this final rule. We did not propose in the HTI–2 Proposed Rule any changes to the Preventing Harm Exception. The revisions we did propose to the Infeasibility Exception or Privacy Exception, or establishment of the new Protecting Care Access Exception, finalized in this rule do not change or conflict with any condition of the Preventing Harm Exception in § 171.201. We emphasize that the Preventing Harm Exception and the Protecting Care Access Exception operate independently of one another and of all other exceptions. An actor's practice does not need to satisfy any portion of any other exception in order to satisfy the Preventing Harm Exception. Likewise, an actor's practice need not satisfy any portion of any other exception to satisfy the Protecting Care Access Exception. We refer readers to the discussion in the HTI–1 Final Rule of how “stacking” of exceptions may be relevant because an actor wishes to engage in one or more practice(s) that are covered in part, but not fully covered, solely by the Privacy Exception (§ 171.202) or solely by the Preventing Harm Exception (§ 171.201) (89 FR 1352 through 1354). As we noted and emphasized in the HTI–1 Final Rule (89 FR 1354), the example detailed in that discussion was an example scenario where an individual has requested restrictions that the actor has chosen to honor, but there may be a wide variety of scenarios where “stacking” other combinations of various exceptions with one another, or with restrictions on use or disclosure of EHI under applicable law, may occur. The Protecting Care Access Exception finalized in this rule may be combined (or “stacked”) with the Infeasibility Exception when both are applicable. Later in this final rule, we discuss the revised *segmentation* condition of the Infeasibility Exception and when it may be applicable in complement to another exception under which an actor may have chosen to withhold a portion of the EHI the actor

would be permitted by applicable law to make available to a requestor for permissible purposes.

Specific to this commenter's concerns about allowing patients to access EHI before it has been explained to them or with limited context, we recognize that patients have different degrees of health literacy as well as different individual preferences for when and how to receive information that may be upsetting. We are aware that some patients may experience emotional distress from accessing new information about their health without additional context or explanation of what the information means for their health or care. We also recognize that many clinical situations are too nuanced to provide the context a patient needs through means other than a conversation with a health care professional. However, as we noted in the ONC Cures Act Final Rule (85 FR 25824 and 25825), it would be challenging to define an appropriate and unique standard for purposes of the Preventing Harm Exception for non-physical harms that all actors, as defined in § 171.102, could apply consistently and, most importantly, without unduly restricting patients' rights to access their health information. We may consider exploring options to address such concerns in future rulemaking, but we note that we would not interpret anything in 45 CFR part 171 as compelling a patient to review information before the patient is ready.

To ensure that this discussion does not introduce confusion about the applicability of the Preventing Harm Exception (§ 171.201),⁹ we remind readers that the Preventing Harm Exception relies on the same types of harm that apply for a covered entity to deny access to protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.¹⁰ For example, in situations where a patient's representative is accessing the patient's EHI (such as a parent accessing EHI of their minor child), the Preventing Harm Exception relies on the same

⁹ For the Preventing Harm Exception to cover an actor's practice likely to interfere with access, exchange, or use of EHI (by the patient or by anyone else who may, under applicable law, access, exchange, or use the patient's EHI for permissible purposes), the actor's practice must meet the applicable conditions of the exception at all relevant times. We refer readers to 45 CFR 171.201 for the full conditions of the Preventing Harm Exception, and those seeking additional information about those conditions to their preamble discussion in the ONC Cures Act Final Rule (85 FR 25821 to 25844).

¹⁰ 45 CFR part 160 and subparts A and E of 45 CFR part 164.

“substantial harm” standard that applies under the HIPAA Privacy Rule to a HIPAA covered entity’s denial of a personal representative’s access of an individual’s PHI on “reviewable grounds” (see 45 CFR 164.524(a)(3)(iii)).¹¹ “Substantial harm” includes “substantial physical, emotional, or psychological harm” (see, for example, HIPAA Privacy Rule preamble at 65 FR 82556). We have published an illustrative chart of the patient access cases where the Preventing Harm Exception recognizes “substantial harm,” in a frequently asked question (IB.FAQ42.1.2022FEB) that is available at: <https://www.healthit.gov/faq/which-patient-access-cases-does-preventing-harm-exception-recognize-substantial-harm>.¹²

Comment. One commenter noted that information blocking could seriously harm the free market and the health care services market if left unchecked. The commenter expressed that the information blocking provisions set the country up for the future by promoting innovation, while simultaneously ensuring lawful access, exchange, and use of electronic health information. The commenter noted that the inclusion of information blocking provisions ensures that barriers to entry are not created for competing technologies, allowing for competition and unhindered development of improved technologies.

Response. We agree with and appreciate the commenter’s feedback.

Comments. Multiple commenters requested clarification or sought additional education on a variety of topics related to information blocking or to information sharing. One commenter sought guidance on how to understand information blocking concepts and relationships between concepts. They suggested that we provide decision trees, relationship diagrams, or possibly supplemental educational materials. A commenter requested a concerted effort by key HHS entities, including the Office for Civil Rights (OCR) and ASTP/ONC, to bolster patient and provider community education about the HIPAA Privacy Rule, its updates, and related information blocking exceptions. This commenter emphasized the importance of patient understanding in assuring

¹¹ The “substantial harm” standard also applies to denial of access to PHI that references another person (other than a health care provider), see 45 CFR 164.524(a)(3)(ii).

¹² This FAQ can also be found, alongside others about the Preventing Harm Exception, other exceptions, and other topics, on HealthIT.gov’s Information Blocking FAQs page (https://www.healthit.gov/faqs?%5B0%5D=term_parent%3A7011).

data sharing consent is true, informed consent. The commenter encouraged us to continue investing in the education of individuals whose data is exchanged in support of patient and population health goals, especially as data sharing becomes more widespread under TEFCA and other frameworks.

Another commenter urged that we place a special emphasis on educating consumers and other parties about limitations in the ability for long-term and post-acute care (LTPAC) providers to furnish some information electronically due to current standards limitations. This commenter expressed concerns regarding legitimate circumstances where certain patient health information from LTPAC providers is not currently feasible to be exchanged via a portal or third-party app and how this could potentially result in a high volume of avoidable consumer information blocking complaints and investigations directed at LTPAC providers. Another commenter expressed that it is important to promote interoperability and exchange between LTPAC providers and the EHRs of patients’ doctors.

Response. We thank commenters for requesting these clarifications. We note that we have offered information sessions and published sub-regulatory guidance documents, fact sheets, and frequently asked questions to provide supplemental information about the information blocking regulations.

We agree that it is important to educate patients about data sharing and its implications. However, discussion of specific additional investment in educational initiatives, as one commenter suggested, is beyond the scope of this final rule. Similarly, we recognize the importance of educating consumers about the limitations of EHI exchange, including particular care and practice settings (such as LTPAC) where the functionalities supported by currently deployed health IT may be more variable than in other settings (such as acute-care hospitals or physician practices). However, providing such education is not in scope for this final rule and would be more effective, we believe, in different contexts than this final rule. We refer readers seeking resources and information for LTPAC providers to advance their adoption and use of interoperable health IT and health information exchange to support care coordination and outcomes to ASTP/ONC’s official website, HealthIT.gov. We offer a range of resources for health care providers across a broad array of care settings online, free of charge. (Start at <https://www.healthit.gov/topic/>

[health-it-health-care-settings/health-it-health-care-settings](https://www.healthit.gov/topic/health-it-health-care-settings/health-it-health-care-settings)). For example, we offer an educational module for LTPAC providers¹³ and our Health IT Playbook (<https://www.healthit.gov/playbook/>) has implementation resources for LTPAC providers.¹⁴ From an information-blocking perspective, information resources currently available at <https://www.healthit.gov/informationblocking> are relevant to actors, including LTPAC and other health care providers.¹⁵ We will continue to look for ways to engage and educate the health IT community, including patients, about our regulations.

Comment. One commenter suggested requiring exam room laptops to be locked after every patient. They expressed concerns about patient record visibility between visits, noting that physicians should be required to enter their passwords to access the information when they enter the room.

Response. Although the concern raised by this comment is beyond the scope of the HTI–2 Proposed Rule, we thank the commenter for their feedback. We strive to promote and recommend best practices for securing EHI. Additional privacy and security information, resources, and tools for both consumers and health care providers are available through ASTP/ONC’s official website, HealthIT.gov.¹⁶

B. Exceptions

1. Privacy Exception Updates

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-

¹³ https://www.healthit.gov/sites/default/files/ltpac_healthit_educationmodule_8-7-17_ecm.pdf.

¹⁴ <https://www.healthit.gov/playbook/care-settings/>.

¹⁵ In addition to fact sheets, FAQs, blogs, we offer recorded webinars, including a three-webinar series designed for the health care provider audience as a whole and one that we designed for and delivered to an LTPAC audience. The LTPAC webinar slides are available at: https://www.healthit.gov/sites/default/files/2024-03/InformationBlockingPresentationPDF_LTPAC_2.22.24.pdf (A link to view the recorded webinar is available from <https://www.healthit.gov/topic/information-blocking>).

¹⁶ <https://www.healthit.gov/topic/privacy-security-and-hipaa>.

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 proposed 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-referenced to the definition of “individual” as defined in the HIPAA Privacy Rule at 45 CFR 160.103. In § 171.202(a)(2)(ii), we provided a second definition: “any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.”¹⁷ Then, in (a)(2)(iii), (iv), and (v), we expanded 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 referenced 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 ONC Cures Act 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.

We stated in the HTI–2 Proposed Rule (89 FR 63620) that 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 proposed the technical correction in the revised text of 45 CFR 171.202 (89 FR 63803) to reflect the correct reading and intent (89 FR 63620).

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 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) (89 FR 63620 to 63621). As we explained in the HTI–2 Proposed Rule (89 FR 63621), this is because 45 CFR 164.502(g) pertains to 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 160.103 for purposes of the HIPAA Privacy Rule.¹⁸ 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 proposed 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, the proposal would simplify the regulatory text without changing what the § 171.202(a)(2) definition of “individual” means or how it applies in practice.

Comments. We received two comments stating support for the proposal and none opposing. We received one comment questioning whether “personal representative” (§ 171.202(a)(iii)) is different from “legal representative” (§ 171.202(a)(iv)) and requesting that we provide an example of someone who is not a personal representative under § 171.202(a)(2)(iii) but is a legal representative who can make health care decisions under § 171.202(a)(2)(iv). This comment stated that the clarification would be useful to all actors.

Response. We appreciate commenters taking the time to provide feedback on this proposal. Having reviewed and considered all comments received on the § 171.202(a)(2) technical correction, we have finalized it as proposed.

We also appreciate the opportunity to explain again the difference between a “personal representative” (§ 171.202(a)(iii)) and a “legal representative” (§ 171.202(a)(iv)). As explained in the ONC Cures Act Final Rule (85 FR 25847), “§ 171.202(a)(2)(iii) encompasses only a person who is a personal representative as defined under the HIPAA Privacy Rule.” As revised by this final rule, that subparagraph reads, in its entirety: “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).” Thus, § 171.202(a)(iii) refers specifically, and only, to a person who is a “personal representative”

¹⁷ 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. 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). Consistent with the § 171.102 definition of “person” by cross-reference to the definition of “person” in 45 CFR 160.103, “natural person” in context of the information blocking regulations means “a human being who is born alive.”

¹⁸ In the second sentence that begins on page 89 FR 63621 in the HTI–2 Proposed Rule, the reference to “45 CFR 170.103” instead of “45 CFR 160.103” was a typographical error. Other references to the HIPAA Privacy Rule’s definition of “individual” in the HTI–2 Proposed Rule correctly reference 45 CFR 160.103, including the reference in the first sentence of the paragraph in which the “45 CFR 170.103” typographical error appears. In this summary of our explanation at 89 FR 63620 through 63621, we have used the correct reference (45 CFR 160.103) rather than reproducing the error that appeared at 89 FR 63621.

consistent with 45 CFR 164.502(g).¹⁹ We refer readers interested in learning more about personal representatives under the HIPAA Privacy Rule to 45 CFR 164.502(g), 45 CFR 164.524, and to guidance provided in the OCR section of the Department's official website, *HHS.gov*.²⁰

We distinguish a "personal representative" under the HIPAA Privacy Rule (specifically, consistent with 45 CFR 164.502(g)) from all other persons who are *legal* representatives and who can make health care decisions on behalf of the individual who is the subject of EHI (whether or not that EHI is also PHI). We include reference to § 171.202(a)(i) in § 171.202(a)(iv) because—in limited circumstances as permitted under State law, or Tribal law where applicable—a family member may be the *legal* representative to act on behalf of a patient to make health care decisions in emergency situations even if that family member may not be the "personal representative" of the individual in accordance with 45 CFR 164.502(g).

Comments. We received several comments requesting that we clarify how or where the HTI–2 Proposed Rule treats an actor that is a covered entity differently than an actor that is not a covered entity.

Response. It is not clear whether these comments refer to all or only some of the information blocking enhancement proposals in the HTI–2 Proposed Rule (89 FR 63616 through 63643 and 89 FR 63802 through 63805). Therefore, to ensure it is easy for readers to map our answer to each of the proposals finalized in this rule, we summarize and respond to these comments in context of each of the enhancements finalized in this final rule.

The definition of "individual" in § 171.202(a)(2) applies for purposes of all of the sub-exceptions (paragraphs (b), (c), (d), and (e)) of the Privacy Exception (§ 171.202). This definition explicitly includes both "individuals" as defined in 45 CFR 160.103 (§ 171.202(a)(2)(i)) and "any other natural person who is the subject of the electronic health information being accessed, exchanged, or used"²¹ (§ 171.202(a)(2)(ii)). Thus,

¹⁹ 45 CFR 164.502(g) sets forth the HIPAA Privacy Rule's "personal representative" standard and implementation specifications.

²⁰ <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html>

²¹ 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. The § 160.103 definition of "person" clarifies the meaning of "natural person" within it. We use "natural person" with that same meaning in

the definition of "individual" is constructed to account for both § 171.102 "actors" who are, and § 171.102 "actors" who are not, subject to the HIPAA regulations in 45 CFR parts 160, 162, and 164.

Comments. We received several comments requesting or recommending that we clarify or reaffirm what "natural person" means when used in defining "individual" or "patient" for purposes of the information blocking regulations.

Response. Although the comments requesting clarification of what "natural person" means within the definition of "individual" did not specifically connect the request to the Privacy Exception, § 171.202(a)(2) is the only place in 45 CFR part 171 where we have codified a definition of the word "individual." That definition includes at § 171.202(a)(2)(ii) "any other natural person who is the subject of the electronic health information being accessed, exchanged, or used." Therefore, we believe responding to comments requesting clarity or confirmation of what "natural person" means within the definition of "individual" in context of the technical correction to § 171.202(a)(2) will make it easier for actors to find when they need it to understand and, if they choose to, apply the Privacy Exception (§ 171.202).

Consistent with the § 171.102 definition of "person" by cross-reference to the definition of "person" in 45 CFR 160.103, "natural person" in context of the information blocking regulations means "a human being who is born alive." In 2002, Congress enacted 1 U.S.C. 8, which defines "person," "human being," "child," and "individual." The statute specifies that these definitions shall apply when determining the meaning of any Act of Congress, or of any ruling, regulation, or interpretation of the various administrative bureaus and agencies of the United States. When used in any definition of "patient" outlined in 45 CFR part 171, the term "natural person" has the same meaning that it has within the definition of "person" in § 171.102, and in the definition of "individual" in § 171.202(a)(2)(ii), which is a human being who is born alive. The term "patient" was included in the proposed Protecting Care Access Exception (§ 171.206), which is finalized in this final rule. We therefore address other comments regarding the meaning of

§ 171.202(a)(2) and throughout this discussion of § 171.202(a)(2). Consistent with the § 171.102 definition of "person" by cross-reference to the definition of "person" in 45 CFR 160.103, "natural person" in context of the information blocking regulations means "a human being who is born alive."

"patient" in the context of § 171.206 in the section of this rule's preamble that is specific to the Protecting Care Access Exception.

b. Privacy Sub-Exception—Individual's Request Not To Share EHI

In the HTI–2 Proposed Rule, we proposed to slightly modify the header of § 171.202(e) for ease of reference to "individual's request not to share EHI" (89 FR 63622). More importantly, we proposed to revise the sub-exception to remove a limitation that applied the exception only to individual-requested restrictions on EHI sharing where the sharing is not otherwise required by law. Thus, we proposed to 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 the 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 original 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 established, 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 federally protected constitutional right to abortion and altered the legal and health care landscape.²² Since the Court's decision, across the United States, a variety of states have newly enacted or are newly enforcing restrictions on access to abortion and other 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.²³

In light of the changing landscape and the limitation of § 171.202(e) as

²² See 142 S. Ct. 2228.

²³ 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#%3Atext=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.)

established by the ONC Cures Act Final Rule (85 FR 25958), we noted in the HTI–2 Proposed Rule our concern 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 (89 FR 63622). Due to that uncertainty, 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 the individual’s requests in the face of demands for disclosure that *might* ultimately be enforced in a court of competent jurisdiction. In particular, as we noted at 89 FR 63622, we were and are concerned that actors may be unwilling to consider granting individuals’ requests for restrictions to sharing their EHI, or may prematurely terminate some or all requested restrictions, based on uncertainty as to whether information blocking penalties or appropriate disincentives might be imposed if the actor ultimately is required by another law to disclose the information. 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, we proposed to remove the “unless otherwise required by law” limitation from § 171.202(e) to help address actors’ uncertainty about various state laws’ applicability as they relate to information blocking (89 FR 63622).

We explained in the HTI–2 Proposed Rule (89 FR 63622) that the proposed revision to § 171.202(e) could serve as a useful complement to the Precondition Not Satisfied sub-exception (§ 171.202(b)). We also noted in the HTI–2 Proposed Rule, and reaffirm here, that the § 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, State, or Tribal laws. For actors’ and

other interested parties’ clarity regarding the relationship between paragraphs (b) and (e) of § 171.202, we now also note that each sub-exception under the Privacy Exception (§ 171.202) stands alone and operates independently of each other sub-exception. Thus, an actor’s practice that fully meets the requirements of *any one* sub-exception (paragraph (b), (c), (d), or (e) of § 171.202) need not also satisfy any other sub-exception (any other of paragraphs (b) through (e) within § 171.202) in order to be covered by the Privacy Exception (§ 171.202).

We noted in the HTI–2 Proposed Rule that the proposed revision to § 171.202(e) would not operate to override other law compelling disclosure against the individual’s wishes (89 FR 63622). The revision is intended to offer actors who elect to honor an individual’s 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 any other law in fact applies to any given actor and compels production of any EHI (or other data) is beyond the scope of this final rule.

If a law requires a particular actor to fulfill a request to access, exchange, or use 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 has been the case since the first eight information blocking exceptions were finalized in the ONC Cures Act Final Rule (85 FR 25642) and will continue to be the case despite the revision to § 171.202(e) proposed in the HTI–2 Proposed Rule (89 FR 63622 and 63803) and finalized in this final rule.

We reiterate here for emphasis the reminder we included in the HTI–2 Proposed Rule (89 FR 63622) that HIPAA covered entities and business associates must comply with the HIPAA Privacy Rule, including privacy protections in the “HIPAA Privacy Rule to Support Reproductive Health Care Privacy” final rule (89 FR 32976, April 26, 2024) (2024 HIPAA Privacy Rule) and any other applicable Federal laws that govern the use of EHI. 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 complying with 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.

Comments. The overwhelming majority of comments supported the proposed revisions to § 171.202(e) and provided multiple reasons for their support. Many commenters specifically agreed with our reasoning that in the current environment, actors may be unwilling to consider granting individuals’ requests for restrictions on sharing of their EHI, or may prematurely terminate requested restrictions, due to uncertainty about whether laws might exist that would override the individual’s requested restrictions and fear of resulting information blocking penalties or appropriate disincentives.

Several commenters stated that the proposed revisions will offer meaningful protections against criminalization risks faced by patients and give greater certainty to health care providers who otherwise might deny an individual’s requested restrictions on sharing their EHI due to uncertainty about laws that could supersede these requests. Several commenters specifically highlighted uncertainty regarding potential legal risks related to reproductive health care as reasons for supporting the proposed revisions. Several commenters stated that the proposed revisions will give physicians and other actors the confidence to delay the disclosure of EHI in accordance with this sub-exception when they are aware that a court order is being contested. One commenter noted that currently, confusion and concern about withholding EHI at the request of a patient due to a contested court order leads physicians and other actors to disclose EHI against a patient’s wishes out of fear of information blocking accusations or penalties.

Several commenters stated that the proposed revisions would benefit actors by reducing information blocking compliance burdens, noting that the proposed revisions reduce burden and costs by simplifying the analysis of whether the sub-exception is applicable. One commenter also stated that the proposed revisions are needed to align with the proposed Protecting Care Access Exception given the variability regarding what information must be disclosed in connection with reproductive health care services in different jurisdictions. Some commenters stated that the proposed revisions would provide actors with greater flexibility in managing EHI sharing. Additionally, commenters stated that clarifying the applicability of various laws related to information blocking through the proposed revisions

will protect patients and physicians, encourage the use of health IT, and support care coordination.

Several commenters in support of the proposed revisions stressed that the revisions would help maintain and strengthen a patient's ability to trust their providers and would improve the patient-provider relationship, as patients and providers would be empowered to discuss and determine the level of risk a patient is willing to take. Commenters stated that patient preferences should always be the priority when providers are faced with an EHI disclosure request. One commenter noted the proposed revisions balance ensuring patient autonomy over their EHI while upholding existing legal frameworks for EHI disclosure.

Response. We appreciate the many comments in favor of the proposed revisions to § 171.202(e) and recognition of the benefits that we outlined in the HTI-2 Proposed Rule (89 FR 63622). Having reviewed and considered all comments received relevant to this sub-exception, we have finalized the revision to the Privacy sub-exception "individual's request not to share EHI" in § 171.202(e) as proposed in the HTI-2 Proposed Rule (89 FR 63803).

Comments. Several commenters expressed concerns about potential unintended legal consequences for actors who restrict the sharing of EHI under the information blocking regulations when it is contrary to an existing law. These commenters generally did not support the proposed revisions and recommended that ASTP/ONC maintain the existing limitation allowing the use of this sub-exception unless disclosure is required by law. One commenter stated that not allowing reliance on this sub-exception when the disclosure is required by law would align the sub-exception with HIPAA and thus reduce complexity for actors and serve public policy since restricting the sharing of EHI could adversely affect patient care in cases such as emergency treatment.

Response. We appreciate these comments and reiterate that the finalized revisions to § 171.202(e) do not override other laws compelling disclosure against the individual's wishes, as we noted when we proposed them (89 FR 63622). As we stated in the HTI-2 Proposed Rule, where there may be a law requiring a particular actor to fulfill a request to access, exchange, or use 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 (section

3022 of Title XXX of the PHSA) and 45 CFR part 171 (89 FR 63622).

Knowing that the exception does not override any other law(s) with which an actor knows they must comply, any actor can choose to honor an individual's request to the extent that they are able under such law(s) and can choose how to communicate to the individual the limits of the actor's ability to honor that request under such law(s). For example, an actor that is also required to comply with the HIPAA Privacy Rule with respect to an individual's information could choose to agree to honor requests for restrictions on disclosures of PHI that the HIPAA Privacy Rule does not require (see 45 CFR 164.502(a)(2) "Covered entities: Required disclosures"). Such an actor could also choose how to communicate to an individual that the actor is able to honor the request for restrictions only to the extent that the restrictions do not prevent the actor from disclosing PHI as required under 45 CFR 164.502(a)(2).

The § 171.202(e) sub-exception applies to requests that an actor chooses to honor and that the HIPAA Privacy Rule *permits* (but does not *require*) the actor to honor, as well as to scenarios where the actor is not required to comply with the HIPAA Privacy Rule. We remind readers that where an actor that is subject to the HIPAA Privacy Rule is required to agree to an individual's requested restriction on use or disclosure of PHI that is also EHI, such as where 45 CFR 164.522(a)(1)(ii) and (vi) applies, the actor's agreeing to and applying such restrictions is "required by law."²⁴ The revisions to § 171.202(e) finalized in this rule are intended to address concerns of actors who are worried about potential implications specific to the information blocking regulations (45 CFR part 171) of attempting to honor an individual's request (that they want to agree to honor) in the face of uncertainty about whether some statute they are not certain is applicable, or some other legally enforceable mandate (such as a contested court order), may or may not ultimately compel them to make EHI available for access, exchange, or use.

Regarding potential adverse impacts of restricted sharing based on the individual's request that some or all of

²⁴ Where applicable law prohibits a specific access, exchange, or use of information, the information blocking regulations consider the practice of complying with such laws to be "required by law." Practices that are "required by law" are not considered "information blocking" (see the statutory information blocking definition in section 3022(a)(1) of the PHSA and the discussion in the HTI-1 Final Rule at 89 FR 1351 and in the ONC Cures Act Final Rule at 85 FR 25794).

their EHI not be shared for certain or any purpose(s), it is important to recognize that the sub-exception is not intended to create an affirmative obligation on the part of any actor to agree to honor any particular individual request(s) that the individual's EHI not be shared to the full extent permitted by applicable law (HIPAA Privacy Rule, other Federal law that may apply such as 42 CFR part 2, or, where applicable, State or Tribal laws). Moreover, as we explained when we originally finalized this sub-exception in the ONC Cures Act Final Rule, we recognize that an individual's requested restriction may need to be compromised in emergency treatment situations and therefore we provided for the ability of an actor to terminate an individual's requested restriction under limited circumstances (85 FR 25859). We did not propose, nor have we finalized, any revisions to the termination provisions of this sub-exception in § 171.202(e)(4).

Comments. Several commenters expressed concerns that the proposed revisions to § 171.202(e) may undermine information sharing and interoperability of EHI as well as inhibit sharing for treatment and other allowable purposes. One commenter provided examples to illustrate the concern, including: if a patient requests that EHI from a visit with a specialist be restricted from their primary care provider; restricting EHI needed for coordinated care and safe medication management; and limiting the sharing of health information used for operational purposes such as teaching that are permitted under HIPAA.

Response. We appreciate the opportunity to clarify why we do not agree that the proposed revisions to this exception would inhibit information sharing or interoperability of EHI on the whole. To satisfy the existing requirements in § 171.202(e)(3), which we did not propose to revise and have not revised in this final rule, the actor's practice must be implemented in a consistent and non-discriminatory manner. As we noted when we originally finalized the sub-exception in the ONC Cures Act Final Rule, this provides basic assurance that the practice is directly related to the risk of disclosing EHI contrary to the wishes of an individual and is not being used to interfere with access, exchange, or use of EHI for other purposes (85 FR 25857). We further noted that this condition requires that the actor's privacy-protective practice must be based on objective criteria that apply uniformly for all substantially similar privacy risks (85 FR 25857).

Specific to concerns about an individual potentially requesting restrictions on EHI sharing that an actor believes would, if implemented, compromise the patient's health or care, we emphasize that the § 171.202(e) sub-exception, like all information blocking exceptions, is voluntary. Exceptions are intended to offer actors certainty that the practices in which they choose to engage consistent with the conditions of an exception will not be considered information blocking, but they are not intended to create, and do not create, an affirmative obligation for any actor to choose to engage in all of the practices that could potentially be covered by any given exception(s). If an actor is unwilling to agree to an individual's requested restrictions on sharing the individual's EHI for teaching or another permitted purpose, nothing in 45 CFR part 171 is intended to obligate the actor to honor the individual's request. We note, however, that an actor's practice to honor or decline individual requests for restrictions in a discriminatory manner—such as based on whether the individual's other health care provider(s) or those providers' health IT developer(s) were competitor(s) or affiliate(s) of the actor—would be inappropriate and could implicate the information blocking definition.

Comments. Several commenters focused on minor patients' EHI and the applicability of the sub-exception in proxy situations. One commenter stated that it is important to consider who is making the request not to share EHI. The commenter noted that there may be times when the adolescent is making the request not to share information and times when the parent is making the request, stating that it would be helpful for ASTP/ONC to explicitly clarify that an adolescent's request not to share information is allowed under the sub-exception unless otherwise prohibited by State law. Another commenter stated that ASTP/ONC must ensure that providers have flexibility to address the confidentiality needs of minor patients and reflect specific state or local requirements, noting the variation in federal and state rules and regulations around parent/guardian access to adolescent data. Other commenters sought clarification that this sub-exception would apply to proxy consent situations.

Response. We clarify that, as proposed (89 FR 63622) and finalized, the revisions to § 171.202(e) offer actors who elect to honor an individual's request not to share EHI certainty that applying the requested restrictions on sharing will not be considered information blocking so long as the

actor's practices in doing so satisfy the requirements of the § 171.202(e) Privacy sub-exception. We did not propose, nor are we finalizing, any revisions to the requirements of the § 171.202(e) Privacy sub-exception that would categorically limit application of the sub-exception to only requests from individuals who are not unemancipated minors. Thus, it is possible that the exception could apply to some scenarios where a parent seeks access, exchange, or use of a non-emancipated minor's EHI when an actor has agreed to the request of the minor (as the individual as described in § 171.202(a)(2)(i) or (ii)) that the EHI not be made available to the minor's parents or other representatives. However, we remind actors and other interested parties that where an actor's practice meets the sub-exception's requirements, the revised § 171.202(e) Privacy sub-exception (like any Privacy sub-exception or any other exception codified in subparts B, C, or D of 45 CFR part 171), simply offers actors assurance that the practice will not constitute "information blocking" under 45 CFR part 171. We emphasize that the revisions to § 171.202(e) do not change how the HIPAA Privacy Rule, or other Federal, State, or Tribal law, applies to adults or minors. In various circumstances, one or more of such other laws may require disclosure of all of an unemancipated minor's health information to the minor's personal representative (consistent with 45 CFR 164.502(g)) or other legal representative as established by applicable law. We also refer readers to the information about how the HIPAA Privacy Rule applies to minors that can be found at 45 CFR 164.502(g) and on the OCR website.²⁵ We also note that revisions to § 171.202(e) do not change how any other Federal, State, or Tribal law applies to proxy requests. We stress that the revisions to § 171.202(e) do not override other law compelling disclosure against the individual's wishes, and whether courts will or should apply any particular Federal, State, or Tribal law to any actor to compel disclosure of any type of information to any requestor for any purpose is beyond the scope of this final rule.

Comments. A couple of commenters expressed concern that patients requesting restrictions on sharing of EHI may lack an understanding of the

²⁵ See <https://www.hhs.gov/hipaa/for-professionals/faq/personal-representatives-and-minors/index.html>, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>, and <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html>.

potential safety impact of not sharing complete health information with their other providers as well as the feasibility of the request to not share information. These commenters generally recommended that if finalized as proposed, ASTP/ONC should provide education on these issues for patients and other interested parties.

Response. We reiterate that the § 171.202(e) Privacy sub-exception does not create an affirmative obligation for any actor to agree to any individual's request for restrictions on access, exchange, or use of the individual's EHI. Where no other applicable law *requires* the actor to agree to an individual's requested restriction, the actor would have discretion to discuss the potential implications of a requested restriction on the availability of information to the individual's other health care providers before agreeing to the request, to not agree to apply restrictions the actor believes introduce unacceptable risks to the patient's health or safety, and to explain to the individual why the actor will not honor the individual's request(s) to which the actor chooses not to agree. We reiterate, however, that if an actor's practice specific to granting individual requests for restrictions is implemented in an inconsistent or discriminatory manner, that practice would not meet the § 171.202(e)(3) requirements, would therefore not be covered by the Privacy Exception (§ 171.202), and could implicate the information blocking definition in § 171.103.

We also appreciate the opportunity to remind readers of our continued commitment to support EHI sharing consistent with patient preferences and applicable law. Whether received through the public comments process for a proposed rule or through informal channels, we appreciate the feedback and questions we receive. They help to inform our development of information resources that we make publicly available on *HealthIT.gov*. Informal channels include, for example, the Health IT Feedback and Inquiry Portal²⁶ that is available year-round and not tied to the comment period for a proposed rule.

Comments. A couple of commenters expressed concern about the feasibility of actors implementing individuals' requested restrictions on the sharing of EHI, and some stated that the technology to operationalize segmentation of data does not exist. One commenter recommended that if revisions to the Privacy Exception are

²⁶ To find the portal, please click, paste, or search <https://www.healthit.gov/feedback>

finalized as proposed, ASTP/ONC should pursue certification program initiatives to create the needed technology. Another commenter recommended that ASTP/ONC help ensure that operationalizing data segmentation is an immediate priority for health IT developers by offering financial incentives for developers enabling restrictions on sharing of EHI.

Response. We appreciate these comments regarding segmentation technology relevant to circumstances where an actor may wish to agree to an individual's request that only some of the individual's EHI not be shared. In proposing to revise § 171.204(e), we recognized the importance of data segmentation technology for exchanging sensitive health data and enabling access, exchange, and use of EHI (89 FR 63634). We also noted our awareness of the limitations of current health IT capabilities for data segmentation and of external efforts to develop technical standards that over time may result in increasingly advanced data segmentation capabilities in EHR systems and other health IT (89 FR 63634). These statements are also relevant in the context of the § 171.202(e) Privacy sub-exception and an actor's practice of implementing restrictions requested by an individual on the access, exchange, or use of the individual's EHI. As we indicated in the HTI-1 Final Rule (89 FR 1301), we continue to encourage and engage with industry and standards development community efforts to advance standards supporting privacy workflows and to monitor the continued evolution of relevant standards to consider in new or revised criteria in future rulemaking. In the HTI-1 Final Rule, we specifically discussed the HL7 data segmentation for privacy (DS4P) implementation guides (89 FR 1301). It is not clear from the comments we received what mechanism(s) the commenters may have envisioned ASTP/ONC using to make data segmentation innovation and advancement an immediate priority for health IT developers, or to offer financial incentives to developers.

In the HTI-1 Proposed Rule, we made several proposals related to the ONC Health IT Certification Program to support additional tools for implementing patient requested privacy restrictions. We proposed a new certification criterion in § 170.315(d)(14), an addition to ASTP/ONC's Privacy and Security Framework under the Program in § 170.550(h), and a revision to an existing "view, download, and transmit to 3rd party" certification criterion in § 170.315(e)(1) (88 FR 23822 through 23824). We

sought public comment on these proposals—the new criterion in § 170.315(d)(14), the inclusion of the request capability for patients in § 170.315(e)(1), and the requirements with the Privacy and Security Framework in § 170.550(h)—both separately and as a whole. We specifically sought comment on the feasibility of each part in terms of technical implementation and usefulness for patients and covered entities using these capabilities. We proposed and sought comment on several alternatives which would add standards to the proposed new certification criterion and would specifically leverage HL7 DS4P IGs for the new certification criterion in § 170.315(d)(14). We also proposed and sought comment on alternate proposals that looked exclusively at the HL7 Privacy and Security Healthcare Classification System (HCS) Security Label Vocabulary within the HL7 DS4P IGs for a source taxonomy for the "flag" applied to the data (88 FR 23822). We sought comment on the health IT development burden associated with implementation of the capabilities including for the individual certification criterion referenced in the Privacy and Security Framework in § 170.550(h). As noted in the HTI-1 Final Rule, we also expressed our concerns about feasibility, timelines, and the overall complexity of the workflows and the related capabilities associated with this right as well as our intent to propose several options for consideration by the health care and health IT communities (89 FR 1301). We refer readers to the HTI-1 Final Rule for discussion of these proposals and of public comments received in response to the primary and alternative proposals we made specific to functionalities supporting individuals' requests for restrictions (89 FR 1298 through 1305).

The *segmentation* condition (§ 171.204(a)(2)) of the Infeasibility Exception specifies a condition²⁷ under which an actor who is not able to segment EHI that the actor must²⁸ or may have chosen to withhold²⁹ from other EHI that the actor could share with a requestor (or various requestors) for permissible purposes can ensure that

²⁷ The actor would still need to meet the requirements of § 171.204(b) for the Infeasibility Exception to apply.

²⁸ An example of when an actor must withhold EHI would be if an individual chose not to give consent that is a pre-requisite for a particular access, exchange, or use to be permissible under applicable State or Tribal law.

²⁹ An example of when an actor may have chosen to withhold EHI would be if an actor chose to agree to an individual's request that the individual's EHI not be shared.

not fulfilling a request to access, exchange, or use the requested EHI is not information blocking. The § 171.204(a)(2) *segmentation* condition has applied, since it was established in the ONC Cures Act Final Rule (85 FR 25867 and 25958), where the actor cannot fulfill a request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI from EHI that cannot be made available due to an individual's preference, cannot be made available by law, or that may be withheld in accordance with § 171.201.

In the HTI-2 Proposed Rule, we proposed to explicitly reference the entire § 171.202 Privacy sub-exception in our revisions to § 171.204(a)(2) and noted that this would ensure that the *segmentation* condition would continue to apply where the actor cannot segment EHI which the actor has chosen to withhold in honoring an individual's request not to share EHI consistent with § 171.202(e) (89 FR 63623). In another section of this final rule preamble, we discuss the revisions we have finalized to § 171.204(a)(2), including a reference to the entire § 171.202 Privacy sub-exception in § 171.204(a)(2)(ii). We also refer readers to the discussion in the HTI-1 Final Rule of how "stacking" of exceptions may occur where an actor may wish to engage in one or more practice(s) that are covered in part, but not fully covered, by one exception (such as the Privacy Exception). The HTI-1 Final Rule discussion (89 FR 1353 and 1354) includes an illustrative example where the actor has elected to grant an individual's request consistent with § 171.202(e).

Comments. A couple of commenters expressed a need for clarification on how the proposed revisions to this sub-exception work. These commenters asked for examples of use cases and urged ASTP/ONC to develop comprehensive guidance to ensure actors understand when and how the sub-exception applies. One commenter recommended that ASTP/ONC work across agencies and with other parties, including payers, to provide more clarity around the sub-exception to help ensure it is not overinterpreted or used to limit sharing of EHI unnecessarily. Specific areas where clarity was requested included standards for segmenting clinical data, differences in clinical versus claim codes, how third-party, non-HIPAA regulated entities can be held to standards, including standards required under TEFCA, and how entities can rely on the stated purpose of the information request.

Response. We appreciate the comments and offer the following use

cases as illustrative examples, while reminding readers that this is *not* an exhaustive list. The revised § 171.202(e) Privacy sub-exception could also be met in other scenarios (use cases) not specifically discussed here.

One use case where the revised § 171.202(e) Privacy sub-exception is intended to apply is where an actor is concerned about implicating the information blocking definition by delaying a disclosure of EHI pursuant to a court order that the actor is aware is being contested (89 FR 63622). In this use case, the actor could choose to meet the requirements of the revised Privacy sub-exception in § 171.202(e) in order to have assurance that it will not be “information blocking” to delay release of EHI in compliance with an individual’s request for restrictions while waiting to see if the order will eventually 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).

Another use case to which the revised § 171.202(e) Privacy sub-exception would apply is where an actor is inclined to grant an individual’s request for restrictions but is uncertain whether other authority might compel the actor to provide access, exchange, or use of EHI despite the individual’s wishes and is concerned about potentially implicating the information blocking definition if, after granting the request, the actor learns of or confirms that such other authority compels provision of access, exchange, or use of EHI contrary to the individual’s expressed wishes. (We discussed this use case, in explaining the need for this revision, in the HTI–2 Proposed Rule at 89 FR 63622). In this use case, an actor could choose to meet the requirements of the revised Privacy sub-exception in § 171.202(e) and have assurance that honoring the individual’s request and applying those restrictions in the interim or for other requestors will not be considered information blocking even if other law ultimately compels disclosure to specific requestor(s) (for permissible purposes)³⁰ against the individual’s wishes.

³⁰ For purposes of the information blocking regulations (45 CFR part 171), “permissible purpose” is defined in § 171.102. Notably, the § 171.102 definition of “permissible purpose” would *not* apply to a purpose for which access, exchange, or use of EHI is prohibited by Federal or, where applicable, State or Tribal law. Examples of such federal law prohibitions are not limited to but do include the HIPAA Privacy Rule’s prohibition of the use and disclosure of genetic information for underwriting purposes (45 CFR 164.502(a)(5)(i) and the HIPAA Privacy Rule’s prohibition of using or disclosing reproductive health care information for

However, we reiterate that a practice satisfying the conditions and requirements to be covered by any exception to the information blocking definition simply means HHS will not consider the practice to be “information blocking” under 45 CFR part 171 or the information blocking statute (PHSA section 3022). We emphasize, again, that the revisions to § 171.202(e) do not operate to override other law compelling disclosure against the individual’s wishes, and if a court with jurisdiction over the actor and subject matter enforces, via court order, a law that requires a particular actor to fulfill access, exchange, or use of EHI without the individual’s authorization, permission, or consent, the actor would be compelled to comply with that law independent of the information blocking statute and 45 CFR part 171.

The specific requests for clarity on segmentation standards, other standards-related issues, TEFCA, and reliability of information requests are beyond the scope of the proposal to revise § 171.202(e). We refer readers to our official website, *HealthIT.gov*, for more information on the ONC Health IT Certification Program, TEFCA, and a wide variety of other health IT topics in addition to information blocking and note that we continue to work alongside federal partners and other interested parties, including providers and payers, to serve as a resource to the entire health system in support of the adoption of health information technology and the promotion of nationwide, standards-based health information exchange to improve health care.

Comments. A couple of commenters expressed concern that not sharing EHI could be a default position for actors and stated that sharing of data in the spirit of the information blocking rules should be the default position. These commenters sought clarification that an actor must receive a specific request from an individual in order to trigger this exception.

Response. An actor’s practice of honoring an individual’s request not to share EHI will be covered by the § 171.202(e) Privacy sub-exception only so long as the practice satisfies the requirements found in § 171.202(e)(1)–(4). The requirements in § 171.202(e)(1)–(4), to which we did not propose changes and have made no changes, include that “the individual requests that the actor not provide such access, exchange, or use of electronic health information without any improper

the activities identified in 45 CFR 164.502(a)(5)(iii)(A)(1)–(3) (subject to paragraphs (B) and (C) of 45 CFR 164.502(a)(5)(iii)).

encouragement or inducement of the request by the actor” (§ 171.202(e)(1)). We also remind readers that the term “individual” is defined for purposes of the Privacy Exception in § 171.202(a), as discussed in this final rule.

We appreciate the opportunity to emphasize that the revised § 171.202(e) Privacy sub-exception remains specific to restrictions on individual requests and that are applied on an individual basis. We emphasize that in order to be covered by the § 171.202(e) Privacy sub-exception, an actor’s practice of restricting the access, exchange, or use of any individual’s EHI must be triggered by a request consistent with § 171.202(e)(1) from the individual (as described in § 171.202(a)(2)(i) and (ii)) or their representative (as described in § 171.202(a)(2)(iii) or (iv)) or a person having authority to act on behalf of a deceased person (as described in § 171.202(a)(2)(v)).

Comments. Several commenters requested that we clarify how or where the HTI–2 Proposed Rule treats an actor that is a covered entity differently than an actor that is not a covered entity.

Response. It is not clear whether these comments refer to all or only some of the information blocking enhancement proposals discussed in the HTI–2 Proposed Rule (89 FR 63616). Therefore, to ensure it is easy for readers to map our answer to each of the proposals finalized in this rule, we summarize and respond to these comments in the context of each of the enhancements finalized in this final rule.

The § 171.202(e) (individual’s request not to share EHI) sub-exception is applicable to any actor’s practice that meets its requirements. The § 171.202(e) sub-exception is available, and all of its requirements apply equally, to any actor’s practice without regard to whether the actor also happens to be a HIPAA covered entity or business associate.

Please see our additional responses addressing these comments in other sections of this final rule.

Comments. Several comments received were beyond the scope of the proposed revisions to the sub-exception. One commenter commented on the documentation provisions in § 171.202(e)(2), which we did not propose to revise. The commenter noted that the current language requires documentation of the request not to share EHI in a timely manner and stated that if an actor fails to do so, then the actor could be subject to an information blocking claim for not sharing the information and the individual requesting the restriction would suffer unintended consequences of an actor’s

oversight. One commenter expressed concern about verbal requests, which were not an aspect of the proposed revisions to § 171.202(e). Another commenter recommended that ASTP/ONC and the HHS Office of Inspector General begin investigations into information blocking no earlier than January 1, 2027, if the provider claims they are protected under the Privacy Exception, in order to give providers at least one year to integrate the new patient requested restrictions technology into their practices.

Response. We appreciate these comments, however we did not propose or solicit comment on any potential revision(s) to the request provisions of § 171.202(e)(1), which do not mention verbal requests, or the documentation provisions of § 171.202(e)(2). We also did not propose to establish a moratorium on OIG investigating any claim of information blocking, or on ASTP/ONC reviewing potential non-conformities of ONC-Certified Health IT with ONC Health IT Certification Program (Program) requirements—such as a Program-participating developer’s potential non-compliance with § 170.401 Information Blocking Condition and Maintenance of Certification requirements. We do not believe such moratorium is necessary. Like all other information blocking exceptions, the Privacy Exception and each of its sub-exceptions is *voluntary* and does not require an actor to deploy or use specific technology(ies) as a condition of a practice by the actor being covered by the exception.

We recognize that it may be easier or more efficient for an actor to engage in practices covered by some exceptions if they have more comprehensive or advanced technological capabilities than if they have only limited or outdated technological capabilities. For example, for an actor to conform practices to § 171.202(e) if they have efficient electronic workflows for receiving (or otherwise logging) individuals’ requests that the individual’s EHI not be shared, identifying whatever subset of such requests as applicable law(s) require the actor to honor,³¹ and considering whether the actor is willing to agree to other individual-requested restrictions. However, as we have maintained since establishing the first eight exceptions in

the ONC Cures Act Final Rule, “failure to meet the conditions of an exception does not automatically mean a practice constitutes information blocking” (85 FR 25649).³² Although we encourage actors to voluntarily conform their practices to the conditions of an exception suited to the practice and its purpose, an actor’s choice to do so simply provides them an enhanced level of assurance that the practices do not meet the definition of information blocking. If subject to an investigation by OIG, each practice that implicates the information blocking provision would be analyzed on a case-by-case basis (*see, e.g.,* 85 FR 25842). Each information blocking case, and whether the actor’s practice would meet all conditions of an exception, will depend on its own unique facts and circumstances (85 FR 25868). We refer any party interested in a short, easy-to-read explanation of how any claim or report of information blocking would be evaluated to the following FAQ available on ASTP/ONC’s website, HealthIT.gov: “How would any claim or report of information blocking be evaluated?”³³

2. Infeasibility Exception Updates

In the ONC Cures Act Final Rule, we 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 the § 171.204(b) *responding to requests* condition and any one of the conditions in § 171.204(a).

In the HTI–1 Final Rule (89 FR 1373 through 1387 and 1436), 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 the HTI–2 Proposed Rule (89 FR 63623), we proposed to modify:

- the § 171.204(a)(2) *segmentation* condition as described in the HTI–2 Proposed Rule (89 FR 63623 through 63624);
- the § 171.204(a)(3) *third party seeking modification use* condition as described in the HTI–2 Proposed Rule (89 FR 63624 through 63625); and
- the § 171.204(b) *responding to requests* condition as discussed in the HTI–2 Proposed Rule (89 FR 63625 through 63627).

In this final rule, we have finalized modifications to the § 171.204(a)(2) *segmentation* condition of the Infeasibility Exception. We do not address in this final rule our HTI–2 Proposed Rule proposals to revise § 171.204(a)(3) and (b). We may address in a future final rule revisions to the Infeasibility Exception that we do not address in this final rule.

In the HTI–2 Proposed Rule, we explained that the § 171.204(a)(2) *segmentation* condition 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 (89 FR 63623). We noted that 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 the individual’s EHI; an individual’s authorization or consent is a prerequisite for a particular use or disclosure of the individual’s 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 individual’s EHI.

In the HTI–2 Proposed Rule (89 FR 63623 through 63624), we proposed updates to the *segmentation* condition to enhance clarity and certainty, and to provide for its application to additional situations. We proposed to update how the text of § 171.204(a)(2) describes why certain EHI cannot or will not be made available, including more specific cross-

³¹ For example, an actor that is subject to the HIPAA Privacy Rule is required to agree to an individual’s requested restriction on use or disclosure of PHI where 45 CFR 164.522(a)(1)(ii) and (vi) apply. (As noted earlier in this discussion, where that is the case and the PHI is also EHI, the actor’s agreeing to and applying such restrictions we would consider to be “required by law.”)

³² *See also, e.g.,* IB.FAQ29.2.2024APR: “If an actor does not fulfill a request for access, exchange, and use of EHI in “any manner requested” that they have the technical capability to support, is the actor automatically an information blocker unless they satisfy at least one of the information blocking exceptions?”

³³ IB.FAQ46.1.2022FEB, FAQ-specific URL: <https://www.healthit.gov/faq/how-would-any-claim-or-report-information-blocking-be-evaluated>.

references to relevant provisions within 45 CFR part 171.

In the HTI–2 Proposed Rule (89 FR 63623), we noted that the *segmentation* condition references EHI that cannot be made available due to an individual’s preference or by law in § 171.204(a)(2)(i), and EHI that the actor may choose to withhold in accordance with the Preventing Harm Exception in § 171.204(a)(2)(ii). We proposed 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 stated that focusing § 171.204(a)(2)(i) solely on EHI that an actor is not permitted by applicable law to make 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 (89 FR 63623). Under the revision we proposed 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. We noted in the HTI–2 Proposed Rule that 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 (89 FR 63623).

We explained that the proposed revision to § 171.204(a)(2) would retain in subparagraph (ii) the explicit reference to the Preventing Harm Exception (§ 171.201). Thus, we noted that 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) (89 FR 63623).

We proposed to explicitly add reference to § 171.202 in our revision to subparagraph (ii) of § 171.204(a)(2) in order to ensure that the *segmentation* condition would continue to apply in scenarios where the actor cannot unambiguously segment other EHI they could lawfully make available from the EHI that the actor has chosen to honor the individual’s request not to share (consistent with § 171.202(e) sub-exception). In addition, we noted that 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). We explained that by referencing all of the Privacy Exception (§ 171.202), the proposed revision to § 171.204(a)(2)(ii) would allow the Infeasibility Exception’s *segmentation* condition to apply in scenarios where an actor 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). Specifically, the condition would apply when such an actor cannot unambiguously segment EHI for which a more restrictive precondition has not been met from other EHI that the actor could lawfully share in jurisdictions with less restrictive preconditions.

We also noted (89 FR 63623) that by referencing all of the Privacy Exception (§ 171.202), the proposed revision would 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.”

In the HTI–2 Proposed Rule (89 FR 63623 and 63624), we 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. We noted that 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, we explained that 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 (89 FR 63624).³⁴ We noted that 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 invited commenters to share any concerns or other perspectives they may wish to share relevant to this issue. We also proposed 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. We noted that including this alternative proposal in the HTI–2 Proposed Rule meant 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)).

We noted (89 FR 63624) that 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). We explained that 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).)

We noted that because the § 171.202(c) sub-exception is applicable only where a health IT developer of certified health IT is not required to

³⁴ 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.

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 stated that 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. We noted that in such situations, a State or Tribal law may operate to provide the individual a right to access their health information that the actor has.³⁵ We explained that 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). We noted that 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 requested comments 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. We also asked if 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 also included an alternative proposal to reference in the revised § 171.204(a)(2)(ii) *segmentation* condition only the Privacy Exception sub-exceptions *other than* § 171.202(c) "health IT developer of certified health IT not covered by HIPAA" sub-exception (89 FR 63624).

We noted that as discussed in the HTI-2 Proposed Rule (89 FR 63624), 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 proposed to reference § 171.206 in the 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. We noted that 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). We explained that, therefore, 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) from other EHI that they could lawfully make available.

In the HTI-2 Proposed Rule (89 FR 63624), we noted that 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, were discussed in detail in the HTI-2 Proposed Rule preamble (89 FR 63627 through 63639). Similarly, we discuss comments received and the finalized requirements for the new § 171.206 exception in this final rule's preamble.

Comments. The majority of commenters supported our proposal to focus subparagraph (i) of § 171.204(a)(2)(i) *segmentation* condition to continue to apply to EHI that is not permitted by applicable law to be made available, stating that the proposed revision provides clarity and certainty for actors who choose to withhold certain patient EHI. Commenters also stated that the proposed revision reduces burden on actors when determining whether and which EHI may meet the Infeasibility Exception and mentioned that providers currently must use extensive time and resources to redact sensitive information before disclosure. Commenters expressed support for the proposal, asserting that the revision addresses technical health IT systems issues (*i.e.*, where systems do not have the

capabilities to unambiguously segment EHI). Commenters further noted that our proposal would result in improved patient experience, engagement, and safety. Several commenters applauded ASTP/ONC for our proposal noting that it allows individuals more control over their health data.

Response. We thank commenters for their support and have finalized § 171.204(a)(2)(i) as proposed. Subparagraph (i) of the *segmentation* condition (§ 171.204(a)(2)) of the Infeasibility Exception (§ 171.204), as revised, focuses solely on EHI that is not permitted by applicable law to be made available for a requested access, exchange, or use.

Comment. We did not receive substantive feedback regarding our proposal to retain explicit cross-reference § 171.201 Preventing Harm Exception, now shown in subparagraph (ii) of § 171.204(a)(2).

Response. Therefore, we have finalized, as proposed, retention of the explicit cross-reference to § 171.201 Preventing Harm Exception in subparagraph (ii) of § 171.204. The § 171.204(a)(2) *segmentation* condition continues to apply where an actor cannot unambiguously segment other EHI from EHI that the actor has chosen to withhold in accordance with the Preventing Harm Exception (§ 171.201).

Comments. The majority of commenters strongly supported our proposal to explicitly add a cross-reference in § 171.204(a)(2)(ii) to the entirety of § 171.202 Privacy Exception, noting that it safeguards patient privacy and sensitive health information, enhances clarity and certainty, provides flexibility, reduces compliance burden on actors, and accounts for health IT system limitations until *segmentation* capabilities are more mature.

Commenters commended ASTP/ONC for the proposal, noting that the provisions are a positive step that allow providers to prioritize caring for patients and will significantly improve patient and family experience, engagement, and safety.

Many commenters endorsed the proposal to expand the *segmentation* condition's coverage stating that it would lead to improved patient privacy and provided several examples of situations where health care providers are unable to segment granular health data. Some commenters specifically referenced the benefits of the proposal for health care providers who treat patients exposed to violence and who request to keep their sensitive information private. Commenters also noted that it would help patients with stigmatizing diagnoses keep their

³⁵ Determining what other laws may operate, or how, in specific circumstances is beyond the scope of this final rule.

information private. Another commenter pointed to their support for the proposed revised *segmentation* condition as it relates to the continued expansion of USCDI data elements and the implications on patient privacy and the potential harm of releasing sensitive information.

Commenters commended ASTP/ONC for the clarity and certainty that our proposal provides for actors to confidently withhold EHI without fear of an information blocking claim or risks of an information blocking determination. For example, one commenter noted that many laboratories do not have the technology to keep certain sensitive results separate, and this proposal would allow laboratories to confidently not share this data without fear of violating information blocking regulations. Commenters also stated that the proposal would have the benefit of providing additional necessary protections and assurances for health care providers who seek to not share a patient's EHI due to risks of an information blocking claim or determination. Commenters asserted that the proposal ensures that actors have clarity that use of exceptions to prevent the disclosure of specific EHI is not considered information blocking. One commenter noted that the proposal is especially helpful for health care providers who lack resources and access to more sophisticated health IT systems.

Many commenters stressed that current health IT systems cannot provide the level of segmentation that is required to safeguard patient data. Commenters specifically noted that health IT systems lack the necessary data segmentation capabilities to map to how Local, State, Federal, and Tribal health data privacy laws are written and cannot apply the variation on disclosure requirements. Commenters stressed that it is technically impossible for EHRs to segment EHI that is protected and treated differently by various privacy laws depending on the jurisdiction and circumstances. Many commenters who endorsed the proposal stated that the *segmentation* condition is necessary in the interim until technology that can separate and sequester sensitive data is available. Commenters stressed that the proposal ultimately eases the burden on actors, especially health care providers, associated with compliance with the information blocking regulations given there are factors outside of their control, like the limited segmentation capabilities in EHRs.

Some commenters specifically supported the proposal to reference the entirety of the Privacy Exception in the Infeasibility Exception's *segmentation*

condition because it would expand the applicability of the *segmentation* condition to health IT developers of certified health IT that are not required to comply with the HIPAA Privacy Rule.

The majority of commenters recommended that we finalize subparagraph (ii) of the *segmentation* condition (§ 171.204(a)(2)) to cross-reference the entirety of the Privacy Exception as proposed.

Response. We thank commenters for their support to expand subparagraph (ii) of the *segmentation* condition (§ 171.204(a)(2)) to cross-reference the entirety of the Privacy Exception (§ 171.202). We also appreciate commenters concerns that technology does not currently have the capability to sequester EHI that is protected and treated differently by laws in various jurisdictions. In the HTI-2 Proposed Rule we noted the importance of data segmentation, our awareness of the limitations of current health IT capabilities for data segmentation and of external efforts to develop technical standards that over time may result in increasingly advanced data segmentation capabilities in EHR systems and other health IT, and the variability in health IT products capabilities to segment data (89 FR 63634). We agree with commenters that revisions to the *segmentation* condition are necessary to provide for circumstances where an actor cannot sequester EHI from other EHI that is treated differently depending on the jurisdiction and circumstances. Therefore, after consideration of the comments and the strong support for the *segmentation* condition proposal to include the entirety of the § 171.202 Privacy Exception, we have finalized, as proposed, subparagraph (ii) of the *segmentation* condition (§ 171.204(a)) of the Infeasibility Exception to cross-reference the entirety of the Privacy Exception (§ 171.202).

We discuss comments specific to cross-referencing § 171.202 Privacy Exception in the *segmentation* condition (§ 171.204(a)(2)(ii)) in more detail below.

Comments. No commenters supported our alternative proposal to reference the 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 in response to our alternative proposal request for comment.

Response. We have not finalized the alternative proposal. We have finalized § 171.202(a)(2)(ii) to include a cross-reference to the entirety of § 171.202. By referencing all of the Privacy Exception (§ 171.202), the *segmentation*

condition's coverage includes 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."

Comments. Some commenters supported our alternative proposal to reference in subparagraph (ii) of the revised *segmentation* condition (§ 171.204(a)(2)) the Privacy Exception sub-exceptions other than § 171.202(c) "health IT developer of certified health IT not covered by HIPAA" sub-exception instead of the entirety of § 171.202. Commenters expressed concern that expanding the 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 could lead health IT vendors to abuse the Infeasibility Exception by inappropriately limiting the format, volume, and categories of health care data because they have deliberately designed their health IT system to limit shared data. Some commenters referred to the practice as "infeasibility by design" and urged ASTP/ONC to clarify that actors may not use the Infeasibility Exception's *segmentation* condition in this manner.

Some commenters expressed their concern that some organizations rely on the *segmentation* condition as a shield to not share EHI for purposes of business expediency instead of separating discrete data that an entity has requested for a legitimate business purpose. The commenters asserted that actors understand that segmentation capabilities are not available in most EHRs, and the *segmentation* condition provides a justification for not sharing EHI when sharing is legally permissible. One commenter expressed concerns with including the Privacy Exception sub-exceptions other than § 171.202(c) "health IT developer of certified health IT not covered by HIPAA," yet acknowledged that the *segmentation* condition is necessary until more robust segmentation capabilities are available. The commenter stated that it was "not clear how to provide the environment, incentives, and potential penalties" to ameliorate the behavior of actors that abuse the *segmentation* condition.

Another commenter expressed concerns that including the § 171.202 Privacy Exception cross-reference in its entirety could inadvertently create challenges for third-party companies to

access and utilize patient data, and result in incentives to limit the development of health care solutions that could improve experiences for providers, patients, and payers.

Response. We thank commenters for their input addressing the alternative proposal. After consideration of the comments received, we have not adopted the alternative proposal. We have finalized the *segmentation* condition (§ 171.204(a)(2)) revision as proposed at 89 FR 63803.

We understand and appreciate commenters' concerns about expanding the *segmentation* condition to include an explicit cross-reference to the entirety of § 171.202 in § 171.204(a)(2), however we are not convinced that these concerns outweigh, at this point in time, the need for including a cross-reference to the entirety of Privacy Exception (§ 171.202) in the *segmentation* condition (§ 171.204(a)(2)(ii)). A large number of comments received in response to the proposals addressed in this final rule expressed concerns and stated it is a reality that many actors use health IT that cannot currently, due to technology limitations, unambiguously segment from other EHI the EHI that they must withhold under laws that apply to them or that they may choose to withhold in accordance with another information blocking exception (such as § 171.202(e), which is available to all actors). Adopting the cross-reference to the entirety of the Privacy Exception (§ 171.202) in the *segmentation* condition in § 171.204(a)(2), provides certainty and clarity for all actors that they can both avoid committing information blocking and protect individuals' privacy interests in accordance with the laws that apply to them—be those laws Federal, State, or Tribal—even if the actor that is unable to unambiguously segment their EHI is a health IT developer of certified health IT not covered by HIPAA. Finalizing the revisions to § 171.204(a)(2) as proposed (89 FR 63803) also avoids adding further complexity because it more precisely identifies for actors the practices that would not be considered information blocking without treating certain actors differently, thus the revisions do not create additional burden for health IT developers not covered by HIPAA that would not likewise apply to actors covered by HIPAA. Additionally, we are not persuaded that it is necessary to exclude non-covered actors in finalized § 171.204(a)(2)(ii), given the relatively small subset of actors and circumstances where the distinction between including or excluding § 171.202(c) from the cross-reference in § 171.204(a)(2)(ii) is likely

relevant because the vast majority of health IT developers of certified health IT operate as business associates or covered entities under HIPAA. We agree with commenters that it is important to ensure that non-covered actors that offer products or services not regulated by the HIPAA Privacy Rule, and are still subject to the information blocking provisions, should have the ability to seek coverage under the provisions finalized in § 171.204(a)(2)(ii) due to the limitations of current segmentation capabilities in health IT.

We note, however, that any abuse of the *segmentation* condition of the Infeasibility Exception (or any component of any information blocking exception) would be of concern to ASTP/ONC, and we plan to continue monitoring for any signals that this may be occurring. We would anticipate taking appropriate educational, outreach, and (where applicable) enforcement steps in response to such signals and may consider future rulemaking, as necessary, to amend any provision in 45 CFR part 171 in response to changing market conditions.

We also plan to continue to engage with the health IT, standards, health care provider, and patient advocacy communities to encourage innovative approaches to development and implementation of more granular and interoperable segmentation capabilities. We encourage anyone who believes they may have experienced or observed information blocking by any health care provider, health IT developer of certified health IT, or HIN or HIE to share their concerns with us through the Information Blocking Portal on ASTP/ONC's website, *HealthIT.gov*. Information received by ASTP/ONC through the Information Blocking Portal as well as the Health IT Feedback and Inquiry Portal helps inform the development of resources we make publicly available on ASTP/ONC's website, *HealthIT.gov*.

Comments. A small number of commenters opposed our proposal to include the cross-reference in the *segmentation* condition (§ 171.204(a)(2)(ii)) to any sub-exception within the Privacy Exception (§ 171.202) because they believed ASTP/ONC could accomplish the same objectives by adding functionality or requirements similar to our proposed "patient right to request a restriction on use or disclosure" certification criterion requirement in the ONC Health IT Certification Program (Program). These commenters opposed any revisions to the Infeasibility Exception's *segmentation* condition in § 171.204(a)(2).

Response. We thank the commenters for their concerns and recommendation, but we did not propose changes to the ONC Health IT Certification Program related to segmentation capabilities in the HTI-2 Proposed Rule. The proposals related to actors lacking segmentation capabilities in the HTI-2 Proposed Rule are related to information blocking. These comments are out of scope of this final rule. In addition, we note that information blocking provisions are relevant where actors deploy a wide range of health IT beyond what is currently certified under the ONC Health IT Certification Program. We refer readers to the HTI-1 Final Rule (89 FR 1298 through 1305) for an explanation on our decision to decline adopting our proposal for a "patient right to request a restriction on use or disclosure" certification criterion in the Program, most notably because of limited developer capabilities to manage the complexities of every patient request and a lack of configured privacy and security systems for this data, which can lead to unintended consequences on patient data.

As mentioned above, we plan to continue to engage with the health IT, health care provider, and patient advocacy communities to encourage innovative approaches to development and implementation of more granular and interoperable segmentation capabilities.

Comments. Some commenters expressed support for expanding the *segmentation* condition to include the entirety of the Privacy Exception because it would protect the EHI of survivors of violence. Some commenters endorsed modifying the Infeasibility Exception's *segmentation* condition to explicitly account for circumstances where the provider cannot comply with a request without disclosing exposure to violence. One commenter expressed concern that clarifying the *segmentation* condition by adding a cross-reference to the Privacy Exception may not be adequate to address a patient's privacy concerns with respect to exposure to violence. The commenter claimed that due to the complexity of information blocking rules, health care providers do not understand or employ the existing *segmentation* condition or the currently codified Privacy Exception adequately, risking harm to the patient. The same commenter stated that our proposal is a step in the right direction regarding protecting sensitive medical information, but the commenter expressed concern that in practice, providers are not aware of how to apply the Privacy Exception and instead share private patient information in fear of

information blocking accusations. Commenters urged ASTP/ONC to clarify the information blocking requirements regarding releasing sensitive patient data in online portals as it relates to the Privacy Exception and the Infeasibility Exception's *segmentation* condition.

Response. We thank the commenters for their support and for bringing to our attention their concerns about health care providers not withholding EHI due to fear of information blocking accusations even when the Privacy Exception would apply if the actor chose to withhold some or all of the patient's EHI. In the HTI-2 Proposed Rule, we proposed to revise the § 171.202(e) Privacy sub-exception (89 FR 63622). We have finalized the § 171.202(e) revision in this rule. We believe the revision will make it easier for actors to feel confident in their ability to satisfy the § 171.202(e) Privacy sub-exception if the actor chooses to honor an individual's request not to share EHI. The Privacy sub-exception "individual's request not to share EHI" (§ 171.202(e)) is agnostic as to why the individual wants to restrict sharing of their EHI, and as to what topics or other subset of their EHI the individual might ask an actor not to share. Thus, § 171.202(e) is not limited to situations where an individual asks an actor not to share information about the individual's exposure to violence, but it would apply where the individual requests that the actor not share that information.

We are aware that adding a cross-reference in § 171.204(a)(2)(ii) to the entirety of § 171.202 does not expand the Privacy Exception's coverage for an actor's electing to withhold exposure to violence or other information that an actor may consider sensitive where none of the sub-exceptions in § 171.202(b), (c), (d), or (e) is applicable. We did not propose in the HTI-2 Proposed Rule such an expansion of the Privacy Exception, nor of any other exception. Where no applicable law requires, and no other exception applies to an actor's choosing to, withhold EHI indicating exposure to violence from access, exchange, or use permitted by applicable law, the Infeasibility Exception's *segmentation* condition will not operate to cover the actor's withholding of such EHI or of other EHI that the actor may be unable to unambiguously segment from it. We did not propose in the HTI-2 Proposed Rule to modify § 171.204(a)(2) so that it could operate in such a manner. Therefore, any expansion of the Infeasibility Exception or another exception to cover actors' electing to withhold EHI indicating exposure to violence or other EHI on the basis that the actor finds it

to be sensitive would be beyond the scope of this rule (or another final rule addressing any other proposals made in the HTI-2 Proposed Rule). We refer commenters and other interested parties to 45 CFR part 171 for the full conditions of all information blocking exceptions, and to ASTP/ONC's official website, *HealthIT.gov*, for the array of resources (such as FAQs, fact sheets, and webinars) we have published about information blocking exceptions. As additional resources become available, including for the newly finalized Protecting Care Access Exception, we anticipate making them available at *HealthIT.gov*.

We note that some actors may operate under one or more laws that restrict information about individuals' exposure to violence in ways that the HIPAA Privacy Rule does not. We also appreciate the opportunity these commenters have provided us to remind all actors that where applicable law prohibits a specific access, exchange, or use of information, complying with such laws is "required by law" for purposes of the information blocking regulations. Practices that are "required by law" are not considered "information blocking" (see, for example, 89 FR 1351 and 85 FR 25794). As we noted in the HTI-2 Proposed Rule (89 FR 63623 through 63624), focusing subparagraph (i) of § 171.204(a)(2) solely on EHI that applicable law prohibits an actor from making 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 prohibits the actor from making covered information available.

We also appreciate the opportunity to remind readers of our continued commitment to support EHI sharing consistent with patient preferences and applicable law. Whether received through the public comments process for a proposed rule or through informal channels, the feedback, and questions we receive are appreciated and help to inform our development of information resources that we make publicly available on *HealthIT.gov*. Informal channels include, for example, the Health IT Feedback and Inquiry Portal that is available year-round and not tied to the comment period for a proposed rule. To find the portal, please click, paste, or search <https://www.healthit.gov/feedback>.

Comment. One commenter urged ASTP/ONC to exercise caution as it considers policies about segmenting patient data that could be necessary to provide patient care. The commenter expressed concerns over the potential for patient harm with competing State

and Federal laws and regulations and noted that segmentation could lead to incomplete clinical information.

Response. We thank the commenter for their perspective. As we have stated, all information blocking exceptions are voluntary; the existence of an exception that could apply to an actor's choice to withhold EHI from access, exchange, or use under the exception's conditions is not intended to create an affirmative obligation that any actor do so. For example, if an actor believes that withholding EHI in accordance with the Preventing Harm Exception (§ 171.201) would in fact create more risk to the patient than would be prevented—either by application of § 171.201 alone or in combination with the Infeasibility Exception due to the actor's lack of segmentation capabilities—then we presume the actor would not choose to withhold the EHI just because an exception (or combination of exceptions) exists that could apply if the actor did choose to withhold the EHI.

We recognize that the landscape of Federal, State, and (where applicable) Tribal laws that affect when sharing patient health information is not permitted, conditionally permissible, permitted, or required is complex. Resolving that complexity would be beyond the scope of this final rule. We plan to continue working with the health care, health IT, patients, and privacy advocate communities in the hopes of encouraging innovation that will advance availability and use of increasingly granular, interoperable, and flexible data segmentation capabilities to help actors safeguard patients' privacy interests and comply with various applicable laws while optimizing data sharing to promote care coordination, safety, and quality.

Comment. One commenter acknowledged their support for the overall intent of the proposal but stated that ASTP/ONC should leave the definition as described in the HIPAA policy. The commenter recommended that ASTP/ONC clarify this definition to fit "the TEFCA rule."

Response. It is unclear to us which specific HIPAA definition the commenter is referring to and therefore it is not clear how they may have envisioned us incorporating such a description into the *segmentation* condition (§ 171.204(a)(2)). It is also not clear from the comment what the commenter was referring to as "the TEFCA rule" or how they intended to suggest the infeasibility exception might, in the commenter's view, better align with whatever aspect of TEFCA the commenter may have intended to reference. We could interpret the

comment as suggesting that ASTP/ONC should finalize our proposed revisions to the *segmentation* condition of the Infeasibility Exception because the prior references in § 171.204(a)(2)(i) and (ii) (before this final rule) may have, in the commenter's assessment, not made it as easy for an actor to know when the *segmentation* condition would apply to a specific situation. We would agree that the original scope of § 171.204(a)(2)(i) and (ii) can be presented in a way that is easier to read, and to that end we proposed the improved wording and structure of § 171.204 in the HTI-2 Proposed Rule alongside the proposal to reference all of the Privacy Exception and the new Protecting Care Access Exception.

In light of the ambiguity of the comment, we note that information blocking regulations are issued under separate statutory authority from HIPAA regulations and TEFCA. We work to ensure the regulations do not conflict with one another and align requirements where practical given the different purpose and function of the information blocking regulations in comparison to the HIPAA Privacy Rule or TEFCA.

Additionally, we do not define terms, nor did we propose to define terms in the *segmentation* condition (§ 171.204(a)). The proposed (and finalized) subparagraph (ii) of the *segmentation* condition (§ 171.204(a)(2)(ii)) adds the cross-reference to § 171.202 where we define the term "HIPAA Privacy Rule." As noted in the HTI-2 Proposed Rule (89 FR 63624), the HIPAA Privacy Rule definition in § 171.202(a)(1), as used in § 171.202, "HIPAA Privacy Rule" means 45 CFR parts 160 and 164 (§ 171.202(a)(1)). Given the ambiguity of the comment and our interpretation, we decline to consider aligning the definition in § 171.202(a)(1) to other definitions discussed in the HTI-2 Proposed Rule.

Comments. In general, commenters expressed strong support to expand explicit application of the *segmentation* condition to the Privacy Exception to account for certain situations where an actor is subject to multiple laws with conflicting or inconsistent preconditions, noting that it provides clarity and is helpful. Commenters expressed appreciation for the expansion because it allows providers to enact uniform policies that outline their inability to segment data, and justify their nondisclosure, allowing providers to prioritize the important work of caring for patients.

Response. We thank commenters for their support and have finalized, as proposed, § 171.204(a)(2)(ii).

Comments. A few commenters seemed to misinterpret our proposal to expand the *segmentation* condition, as well as the existing codified requirements of the *segmentation* condition in § 171.204(a)(2) that we did not propose to revise in the HTI-2 Proposed Rule. Commenters cited the OCR "Privacy Rule to Support Reproductive Health Care Privacy" Final Rule's valid attestation requirements as a pre-condition that must be satisfied by the health care provider before disclosing specific EHI. The commenters suggested that the proposed revised *segmentation* condition would now apply if a physician does not receive a valid attestation, and it would allow the physician or their EHR developer to withhold most of the medical record if prohibited from sharing specific EHI based on OCR, State, or other privacy regulations.

Response. As discussed above, the expanded *segmentation* condition applies where an actor 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) but 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. We refer readers to the HTI-2 Proposed Rule (89 FR 63627 through 63642) for a discussion of the new Protecting Care Access Exception (§ 171.206) and alignment with the 2024 HIPAA Privacy Rule.

Comments. Commenters had differing views on whether expanding the *segmentation* condition's coverage could affect the speed with which actors move to adopt or improve segmentation capabilities. Most commenters stated that expanding the *segmentation* condition's coverage would not discourage health IT developers from developing segmentation capabilities or health care providers from adopting the technology. Several commenters stated that including the entirety of § 171.202 would not cause a delay in development or adoption of segmentation capabilities. Commenters noted that health care providers would welcome the technology and acknowledged that some health IT developers are working to improve segmentation capabilities, but that the availability of the *segmentation* condition is necessary in the interim until health IT capabilities mature. Commenters stated that the

§ 171.204(a)(2)(ii) *segmentation* condition would improve interoperability, and in turn patient safety and privacy, until health IT capabilities fully support more granular segmentation.

One commenter suggested that ASTP/ONC should not be concerned if the expanded *segmentation* condition disincentivizes the development of data segmentation capabilities because there are other policy avenues to address these concerns, notably through certification criteria requirements and Centers for Medicare & Medicaid Services (CMS) regulations that incorporate by reference the technical standards needed for segmentation. The commenter believed that addressing these concerns through other federal regulations would lead to speedier adoption of segmentation capabilities. The commenter further stated that the interests of interoperability are not advanced by denying actors—particularly those that do not develop or control the health technologies—the protection of the *segmentation* condition given the realities of current health IT capabilities and third-party payer systems.

However, some commenters expressed concerns that expanding the *segmentation* condition's coverage would encourage the health IT industry to delay development and adoption of robust segmentation capabilities at the peril of promoting interoperability and possibly patient safety. One commenter stated that the expansion would result in incentives to limit the development of health care solutions that could improve experiences for providers, patients, and payers. Another commenter stated that the entire health IT industry is delaying the development of segmentation capabilities, regardless of whether a health IT developer is required to comply with the HIPAA Privacy Rule.

Response. We thank commenters for their suggestions and insights in responding to our question on the expansion of the Infeasibility Exception's *segmentation* condition in § 171.204(a)(2)(ii) and whether there are potential effects on the speed with which actors move to adopt or improve segmentation capabilities. As commenters noted, the health IT that is currently available cannot easily sequester granular data. To the extent that adopting the expanded *segmentation* condition's coverage does or does not affect the speed with which actors move to adopt or improve segmentation capabilities, we agree that the availability of the *segmentation* condition is necessary, at this time,

until health IT capabilities mature, and more interoperable and granular segmentation capabilities improve. We recognize the need to promote interoperability, but we also consider patient privacy and safety when promoting interoperability. We thank commenters for sharing their thoughts on how the Infeasibility Exception's *segmentation* condition provides an interim solution for actors to limit sharing sensitive EHI without violating the information blocking regulations.

We appreciate the commenter's observations that policy development and requirements in other Federal programs could encourage the development of data segmentation capabilities and that our proposal would not disincentivize these developments. As stated, we plan to continue to engage with the health IT, standards, health care provider, and patient advocacy communities, as well as our Federal partners, to encourage innovative approaches to development and implementation of more granular and interoperable segmentation capabilities. We will continue to monitor and analyze approaches by health IT developers for real world implementation of segmentation capabilities and the adoption of the technology by health care providers.

Comment. One commenter urged ASTP/ONC to examine how it can spur action to respond to growing threats to patient privacy, the patient-physician relationship, and patient and clinician safety.

Response. Although the comment is beyond the scope of this final rule, we thank the commenter for sharing their thoughts. We recognize these topics are important to patients, physicians, other clinicians, and the health care system as a whole. ASTP/ONC plans to continue our efforts to foster development of a nationwide health IT infrastructure in a manner consistent with, among other important goals, improving health care quality, reducing medical errors, reducing health disparities, and advancing the delivery of patient-centered medical care while ensuring that each patient's health information is secure and protected in accordance with applicable law. As we mention above, whether received through the public comments process for a proposed rule or through informal channels, the feedback, and questions we receive are appreciated and help to inform our development of information resources that we make publicly available on *HealthIT.gov*. Informal channels include, for example, the Health IT Feedback and Inquiry Portal that is available year-round and not tied to the

comment period for a proposed rule. To find the portal, please click, paste, or search <https://www.healthit.gov/feedback>.

Comments. We received several comments requesting that we clarify how or where the HTI-2 Proposed Rule treats an actor that is a covered entity differently than an actor that is not a covered entity.

Response. As we previously noted in our discussion of the Privacy Exception in this final rule, it is not clear whether these comments refer to all or only some of the information blocking enhancement proposals in the HTI-2 Proposed Rule (89 FR 63498). With respect to our proposals regarding the Infeasibility Exception, the proposal in § 171.204(a)(2)(ii) expands the application of the Infeasibility Exception's *segmentation* condition to all situations where an actor is unable to segment EHI from other requested EHI that the actor has chosen to withhold consistent with the Privacy Exception (§ 171.202) or Protecting Care Access Exception (§ 171.206). The information an actor is prohibited by applicable law from making available may vary based on what laws, including the HIPAA Privacy Rule, do or do not apply to the actor. However, the Infeasibility Exception's *segmentation* condition does not have different requirements based on whether an actor must also comply with the HIPAA Privacy Rule.

Because the finalized *segmentation* condition (§ 171.204(a)(2)) adds a cross-reference to the entirety of the Privacy Exception, we remind readers that the § 171.202(e) sub-exception's alignment with the individual's right under the HIPAA Privacy Rule to request restrictions does not limit the sub-exception's availability to actors who are also subject to the HIPAA Privacy Rule's requirements (89 FR 1353). We refer readers to the HTI-2 Proposed Rule (89 FR 63620 through 63622) for further discussion of the Privacy sub-exception "individual's request not to share EHI" (§ 171.202(e)).

Comments. Commenters commended ASTP/ONC for expanding the *segmentation* condition to specifically cross-reference the proposed Protecting Care Access Exception in § 171.206 noting that it logically aligns with the cross-reference in § 171.204(a)(ii) to § 171.201 and the proposed cross-reference to § 171.202. Commenters noted that the reference to the Protecting Care Access Exception in the *segmentation* condition of § 171.204(a)(2)(ii) is a positive revision because it allows actors to consider segmentation limitations when

evaluating whether the withholding of reproductive health information was properly tailored. Commenters stated that it is technically difficult for health care providers to fulfill requests without sharing protected reproductive health information, making it necessary for the new Protecting Care Access Exception cross-reference in the Infeasibility Exception's *segmentation* condition. Commenters appreciated the flexibility the proposal provides for health care providers declining to share reproductive health information without facing information blocking consequences. Commenters stated that ASTP/ONC should not penalize health care providers for honoring patients' preferences to refrain from sharing EHI or to withhold EHI that could expose patients to legal consequences for receiving lawful reproductive care when segmentation of that data is not feasible.

Response. We thank commenters for their support and have finalized, as proposed, the cross-reference to the Protecting Care Access Exception (§ 171.206) in the subparagraph (ii) of the *segmentation* condition of the Infeasibility Exception (§ 171.204(a)(2)(ii)).

We explained in the HTI-2 Proposed Rule (89 FR 63624) that the § 171.206 Protecting Care Access Exception applies 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 have finalized the cross-reference to the Protecting Care Access Exception (§ 171.206) in the *segmentation* condition (§ 171.204(a)(2)(ii)) because the finalized § 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 does 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 reference to § 171.206 in the finalized § 171.204(a)(2)(ii) accommodates circumstances where an actor lacks the technical capability to unambiguously segment the EHI the actor has chosen to withhold consistent with the finalized Protecting Care Access Exception (§ 171.206) from other EHI that they could lawfully make available. The

requirements for an actor's practice to satisfy the new finalized Protecting Care Access Exception (§ 171.206), including the § 171.206(a) *threshold* condition that is 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 the HTI-2 Proposed Rule (89 FR 63633 through 63638).

3. New 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 health care quality and efficiency, accelerate research and innovation, and provide greater value and choice to health care 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 that the information blocking provision of the 21st Century Cures Act works to deter practices that “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 (89 FR 1437)). 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).

Between when the first eight regulatory exceptions to the information blocking definition were finalized in 2020 and the proposal of the Protecting Care Exception in the HTI-2 Proposed Rule (89 FR 63627 through 63639 and 63804), the legal landscape had 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. The 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 noted in the HTI-2 Proposed Rule (89 FR 63627), 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 part on services or supports from other persons, such as a spouse, partner, or friend.

In the current legal environment, various jurisdictions are enforcing laws, or contemplating legislation, 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 is lawful under the circumstances in which it was provided, may impact people’s willingness to provide or assist in reproductive health care.

On April 26, 2024, OCR issued the 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 May 13, 2024, blog post titled “Supporting Information Privacy for Patients, Now and Always: Four Reminders of How HHS Information Blocking Regulations Recognize Privacy Rules,”³⁶ on and after the 2024 HIPAA Privacy Rule’s effective date, a HIPAA covered entity’s or business associate’s practice of denying a request for a use or disclosure of PHI where the use or disclosure is prohibited under that rule is excluded from the information blocking definition (45 CFR 171.103) because that denial 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.

As we noted in the HTI-2 Proposed Rule (89 FR 63628), the 2024 HIPAA Privacy Rule also established 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; 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.³⁷

³⁶ This HealthITbuzz blog post is available at <https://www.healthit.gov/buzz-blog/information-blocking/supporting-information-privacy-for-patients-now-and-always-four-reminders-of-how-hhs-information-blocking-regulations-recognize-privacy-rules>.

³⁷ We did not propose in the HTI-2 Proposed Rule, nor have we finalized in this final rule, any changes to the Privacy Exception’s Precondition Not Satisfied sub-exception (§ 171.202(b)). As the

In preamble discussion of the background and purpose of the proposed Protecting Care Access Exception (89 FR 63628), we observed that 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), although 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 allow 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 could be implicating the information blocking definition unless another applicable law requires the denial, or another regulatory exception applies. Similarly, an actor conditioning fulfillment 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.

In the HTI-2 Proposed Rule (89 FR 63628), we provided a brief review of how the information blocking regulations, which are based on statutory authority separate from

National Coordinator had reminded interested members of the public prior to HHS releasing the HTI-2 Proposed Rule: "the information blocking regulations are designed to consider applicable law, including HIPAA rules." (Tripathi, M, "Supporting Information Privacy for Patients, Now and Always: Four Reminders of How HHS Information Blocking Regulations Recognize Privacy Rules," HealthITbuzz blog dated May 13, 2024, available at: <https://www.healthit.gov/buzz-blog/information-blocking/supporting-information-privacy-for-patients-now-and-always-four-reminders-of-how-hhs-information-blocking-regulations-recognize-privacy-rules>.)

HIPAA, operate (independently of regulations promulgated under HIPAA). This background information is repeated here because it may help readers understand how and why an actor may be concerned about potentially implicating the information blocking definition (and civil monetary penalties or appropriate 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 or business associate 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)). 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" without meeting the "health IT developer of certified health IT" definition, 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.)

As we explained in the HTI-2 Proposed Rule (89 FR 63629), we 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, as we noted in the preamble discussion of the proposed Protecting Care Access Exception (89 FR 63629), 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.

As we reiterated in the HTI–2 Proposed Rule (89 FR 63629), the information blocking statute is separate from the HIPAA statute and 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 proposed 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 HIPAA Privacy Rule merely permits.³⁸ Actors 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) have long been 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. We noted this in the HTI–2 Proposed Rule (89 FR 63629) and emphasize again here that such other exceptions remain available to all actors. Each of the information blocking exceptions codified in subparts B, C, and D of 45 CFR part 171 applies under the conditions specified in the exception.

In the HTI–2 Proposed Rule (89 FR 63629), we noted that there were at that time no exceptions in 45 CFR part 171

³⁸ The HIPAA Privacy Rule does *not* generally require uses and disclosures of PHI but merely permits uses and disclosures for various purposes. Disclosures that *are* required under the HIPAA Privacy Rule are identified in 45 CFR 164.502(a)(2).

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 from³⁹ 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 exceptions, we noted, were 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.⁴⁰ Thus, we explained that 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 the Privacy Exception (§ 171.202) or Preventing Harm Exception (§ 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 constitute information blocking (89 FR 63629). 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 discussed in the HTI–1 Final Rule preamble (see 89 FR 1351–1354) and in information resources available on ASTP/ONC’s

³⁹ For purposes of this discussion and of the proposed Protecting Care Access Exception, we noted that 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.

⁴⁰ 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.

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.

In proposing the Protecting Care Access Exception (§ 171.206), we noted (89 FR 63629) that it would be available to any actor, regardless of whether the actor is also a HIPAA covered entity or business associate. The exception was proposed to apply regardless of whether another exception could also apply to an actor’s practice(s) assuming that the applicable conditions were satisfied. Also, we noted in the HTI–2 Proposed Rule that other exceptions would continue to be available in circumstances where the conditions of the Protecting Care Access Exception cannot be met but the conditions of the other exception(s) can be met (89 FR 63629).

At the bottom of 89 FR 63629 (in the last column as printed in the **Federal Register**), the HTI–2 Proposed Rule included a reminder that each information blocking exception and each provision of each exception is designed to stand independent of any and every other exception unless, and to the extent that, any specific provision of an exception explicitly references another exception. Even in instances with such references, the dependency is limited to the exact provision or function of the provision that relies upon the cross-reference. Thus, we explained in proposing the Protecting Care Access Exception that the exception would operate independently of any provision of any other exception in part 171 and any provision in 45 CFR 171 that does not reference it (89 FR 63629). We stated in proposing the Protecting Care Access Exception that it was our intent that if any provision in § 171.206 were 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 § 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 (89 FR 63629 and 63630). It continues to be HHS’s intent that if any provision of § 171.206, as finalized in this final rule, were 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 § 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 final rule.

As we noted in the HTI–2 Proposed Rule (89 FR 63630), 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, we stated (89 FR 63630), a new exception was 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. We stated that this exception (§ 171.206) is important and intended to ensure health care providers do not feel the need to adopt paper or hybrid recordkeeping methods in place of fully electronic, interoperable formats (89 FR 63630).⁴¹ We explained that 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 (89 FR 63630). We clarified that creating an information blocking exception that would exclude from the information blocking definition an actor’s restricting EHI sharing under the conditions of the Protecting Care Access Exception (§ 171.206) is necessary to preserve and promote public trust in health care

⁴¹ 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) regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103.

professionals, health care, and the health information infrastructure.

The Protecting Care Access Exception (§ 171.206), as proposed (89 FR 63630) and as finalized in this final rule, is intended to address actors’ concerns about potentially implicating the information blocking definition if they choose not to share EHI in a 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 the mere fact that reproductive health care was sought, obtained, provided, or facilitated (89 FR 63632). Under the *patient protection* condition (§ 171.206(b)), the exception is also intended to address such concerns and belief, on the part of the actor, specific to EHI indicating a patient has health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated.

The HIPAA Privacy Rule does not prohibit the use or disclosure of PHI that indicates or is potentially related to “reproductive health care” as defined in 45 CFR 160.103 if the use or disclosure is not for a purpose described at 45 CFR 164.502(a)(5)(iii) and the use or disclosure is otherwise required or permitted by the HIPAA Privacy Rule. Therefore, the 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 information blocking implications of limiting sharing of EHI when the actor believes such limits could reduce a risk of potential exposure to legal action (as defined in § 171.206(e)) in connection with an access, exchange, or use of such EHI for a permissible purpose.

We recognize that no information blocking exception can address all concerns a person may have about potential legal action for the mere act of seeking, obtaining, providing, or facilitating reproductive health care. However, we clarify that, to the extent such concerns may be mitigated by an information blocking exception that applies where an actor chooses to withhold 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 an exception that applies to such withholding of EHI is reasonable and necessary. We noted our concern 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 the 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.⁴² This may also be true of trust in other types of health care professionals, such as nurses, physician assistants, pharmacists, or organizational providers such as hospitals or long-term/post-acute care facilities. Thus, we believe that addressing actors’ uncertainty specific to information blocking with the 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.

As we noted in the HTI–2 Proposed Rule (89 FR 63630), 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.⁴³ Thus, we clarified that the

⁴² Birkhäuser, J., Gaab, J., Kossowsky, J., Hasler, S., Krummenacher, P., Werner, C., & Gerger, H. (2017). Trust in the health care professional and health outcome: A meta-analysis. *PLoS one*, 12(2), e0170988. <https://doi.org/10.1371/journal.pone.0170988>.

⁴³ Iott, B.E., Campos-Castillo, C., & Anthony, D.L. (2020). Trust and Privacy: How Patient Trust in Providers is Related to Privacy Behaviors and Attitudes. *AMIA . . . Annual Symposium proceedings. AMIA Symposium, 2019*, 487–493 <https://pmc.ncbi.nlm.nih.gov/articles/PMC7153104/>.

Protecting Care Access Exception in § 171.206—which would apply under specified conditions to actors’ practices of choosing not to share specific EHI (where such sharing would be otherwise lawful)—is reasonable and necessary to preserve patient trust in the health IT infrastructure and information sharing, as well as to protect the availability and safety of care, and to promote better care outcomes (89 FR 63630).

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 of 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 other 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 in the current environment. 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 in the absence of the Protecting Care Access Exception. 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 consistent with 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.

As we discussed in the HTI–2 Proposed Rule and in the preceding paragraphs, we stated that, for the reasons discussed at 89 FR 63627–63631, we believe actors’ practices of limiting EHI sharing under the conditions of the Protecting Care Access Exception are reasonable and necessary to preserve advances in digitization, interoperability, and public confidence in the nationwide health information technology infrastructure. We noted that actors selectively withholding EHI that indicates or is potentially related to

reproductive health care (as applicable) under the conditions of the proposed exception 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.

In the HTI–2 Proposed Rule (89 FR 63631), we noted that 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 was, however, intended to stand alone and independent of other exceptions. We note that through a typographical error, the word “exceptions” was omitted from the HTI–2 Proposed Rule preamble at the end of the second sentence at 89 FR 63631. We also stated that 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, we stated that 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.

In the HTI–2 Proposed Rule (89 FR 63631), we also noted that 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 (§ 171.202). 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)).

The § 171.202(e) 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 proposed to strengthen and simplify the § 171.202(e) Privacy sub-exception as discussed in the HTI-2 Proposed Rule (89 FR 63622). Finalization decisions specific to that proposed revision to the § 171.202(e) Privacy sub-exception are discussed in this final rule preamble, above. 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. The § 171.202(e) sub-exception does not—and will not as revised by this final rule—rest on why the individual may prefer that some or all of their EHI not be shared. But, as we noted in proposing the Protecting Care Access Exception, the § 171.202(e) sub-exception only applies to scenarios where the individual requests the restrictions (89 FR 63631). As we noted in the HTI-2 Proposed Rule (89 FR 63631), there may be circumstances where an individual does not request the restriction, but when it would be reasonable and necessary for an actor to interfere with access, exchange, or use of EHI for the purpose of addressing individuals' (or providers' and others') risk of potential exposure to legal action that could discourage availability, access, and choice of medically appropriate reproductive health care.

We stated in the HTI-2 Proposed Rule (89 FR 63631 and 63632) that 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, we noted that 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, we observed that 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 (89 FR 63631 and 63632).

We explained (at 89 FR 63632) that 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, we stated that 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 stated (89 FR 63632) our belief that 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 conditions specified in the exception. Therefore, we proposed a new Protecting Care Access Exception (§ 171.206) for the information blocking definition (89 FR 63632 through 63640 and 63804). We stated that when its conditions were met, the proposed 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 exception as proposed to apply, we explained that the potential exposure to legal action that the actor believes could be created would need to 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 noted 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 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 appropriate disincentives as applicable, under HHS information blocking regulations based specifically on those practices.

As is the case with exceptions already established in 45 CFR part 171, the proposed Protecting Care Access 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.⁴⁴

⁴⁴ 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. The § 160.103 definition of “person” clarifies the meaning of “natural person” within it. We noted that we use “natural person” with that same meaning in § 171.206(b)(3) and throughout the discussion of § 171.206. Consistent with the § 171.102 definition of “person” by cross-reference to the definition of “person” in 45 CFR 160.103, “natural person” in context of the information

We emphasized 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.

We noted that 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, the 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 reproductive health care, subject to the exception's conditions.

We explained that for the proposed 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 (89 FR 63633). We clarified that an actor's practice could satisfy both conditions (b) and (c) at the same time, but the minimum requirement for the proposed exception to apply would be that the practice satisfy at least one of these two conditions in addition to the *threshold* condition in paragraph (a) (89 FR 63633).

We discuss the proposed conditions of the proposed Protecting Care Access Exception, and the comments we received specific to them, in detail in below.

Comments. In general, many commenters expressed strong support for the proposed Protecting Care Access Exception and endorsed the necessity of an exception that applies to withholding of specific EHI that indicates or is potentially related to reproductive health care in circumstances where the exception applies. Many commenters stated that the proposed exception will facilitate patients' access to care, and health care providers' willingness to provide such care to patients who are seeking it. Several commenters also stated that the proposed exception would provide clarity and certainty for actors, including clarity for health care providers who are seeking to understand their responsibilities under the information blocking regulations in light of varying laws regarding reproductive health information in different jurisdictions. Some commenters stated that the proposed exception would encourage the continued use of electronic methods for sharing health information, so that some actors would not feel that they needed to revert to paper records to protect their patients' privacy. Several commenters noted the importance of trust in the patient-provider relationship to support health care and interoperability including one commenter who noted that this exception would protect the sanctity of the patient-physician relationship.

Many commenters stated that the proposed exception would support communication and trust in the patient-provider relationship, and that such

trust is essential to provide care to patients. One commenter stated that "many clinicians have resorted to keeping paper charts" and that "it is essential that ASTP/ONC enable us to better protect our patients from unintended disclosure of their legally sensitive health information." Many commenters supported finalization of the exception as proposed. Two commenters stated that HIEs have direct experience with states and localities implementing laws that would invoke other exceptions to information blocking, leading to potentially less interoperability and data exchange, in order to address concerns that actors would otherwise run afoul of information blocking regulations if they did not exchange reproductive data. These commenters stated they, therefore, appreciate this exception.

Response. We appreciate the support for this exception expressed by many commenters. Having considered all comments received in response to the proposed Protecting Care Access Exception (§ 171.206), we have finalized the exception as proposed and provide additional responses to specific comments below.

Comments. Several commenters expressed support for the exception's intent or effect but advocated reducing the conditions that need to be met for the exception to apply, eliminating documentation requirements, or both. Some of these comments advocated an exception that would apply broadly where a health care provider believes withholding any EHI could protect patient privacy or protect patients or others from exposure to potential legal action on bases beyond those addressed in the proposed exception.

Response. We appreciate the commenters' support for the exception. We have finalized the exception's conditions as proposed because we believe they strike the best balance we can attain at this time between the interests of actors and patients in protecting reproductive health care availability and patients' reproductive health privacy with the interests of actors, patients, and others in maintaining and building upon progress made to date toward EHI interoperability and a norm of information sharing that includes individuals being able to easily access, exchange, and use their EHI however and whenever they want. We have not adopted any of the alternative proposals on which we sought comments that would have added complexity to the exception in an effort to maintain this balance of interests. We do not believe it is necessary to reduce the conditions

blocking regulations means "a human being who is born alive."

that need to be met to satisfy the exception, or to eliminate its documentation requirements, because doing so would not strike the best balance between the aforementioned interests of actors and patients.

We have adopted the “good faith belief” standard that considers what potential risk of exposure to legal action the actor honestly believes could be reduced by their practice likely to interfere with access, exchange, or use of EHI. By relying on a subjective standard, the § 171.206(a)(1) belief requirement supports the policy goal of this exception being efficient for actors to use, because the *threshold* condition’s subjective standard does not require the actor to track or analyze in detail all the laws of the various jurisdictions across the country in order to hold a belief in good faith. Thus, the subjective “good faith belief” requirement ensures the Protecting Care Access Exception can be used easily and with confidence even by single-physician practices and small rural hospitals or LTPAC facilities; these providers need not understand all of the various laws in order to hold an honest belief.

Where an actor chooses to satisfy the § 171.206(a)(3) implementation requirement by implementing a practice based on a case-by-case determination, they would need to document the determination consistent with paragraph (a)(3)(ii). Within that, we note that although subparagraph (D) calls for the documentation to “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,” the identification need only describe the risk of potential exposure to legal action that the actor believes the interference with EHI access, exchange, or use could reduce. To satisfy the § 171.206(a)(3) implementation requirement through an organizational policy (paragraph (a)(3)(i)) or case-by-case determination (paragraph (a)(3)(ii)), an actor would *not* need to catalog potential sources of legal risk comprehensively or to a high degree of specificity. Further, we note that if an actor chooses to satisfy the § 171.206(a)(3) implementation requirement by implementing a practice consistent with paragraph (a)(3)(i), all that is expressly required to be in writing is an organizational policy with the characteristics identified in subparagraphs (a)(3)(ii)(A) through (E). None of the subparagraphs in (a)(3)(i) specify that the policy call for creation of particular documentation every time the practice implemented based on the

policy may interfere with someone’s access, exchange, or use of relevant EHI.

Broadening the Protecting Care Access Exception (§ 171.206) to apply when an actor has a good faith belief that sharing EHI could create risk of potential exposure to legal action based on anything other than the mere act of seeking, obtaining, providing, or facilitating “reproductive health care” (using the definition of reproductive health care as defined at § 171.102) would be beyond the scope of the proposal. We also remind readers that other exceptions may apply in a variety of circumstances where the finalized Protecting Care Access Exception (§ 171.206) does not apply. For example, the Privacy sub-exception “individual’s request not to share EHI” (§ 171.202(e)) is *not* limited or specific to concerns related to any specific type(s) of health care, health condition(s) or history, or reasons why an individual may be concerned about sharing some or all of their EHI with whomever the individual does not want to have access, exchange, or use of that EHI. As we noted in the HTI–1 Final Rule (89 FR 1353): the § 171.202(e) Privacy sub-exception does not specify that the individual requesting restrictions should have particular reasons for requesting restrictions or be required to share their reasoning with the health care provider or other actor of whom they make the request. As we observed in the HTI–1 Proposed Rule (88 FR 23874), out of respect for the patient’s privacy and autonomy and fostering trust within the patient-provider relationship, a provider might choose to honor a patient’s request for restrictions on sharing of their EHI even if the provider did not *know* the patient’s specific reasons for the request. As originally codified, and as revised by this final rule, the § 171.202(e) Privacy sub-exception applies to an actor’s practice that meets its requirements—regardless of *why* the individual may have made a request consistent with § 171.202(e)(1) or what EHI the individual may not want shared. (As we have repeated in the HTI–2 Proposed Rule and this final rule, however, we remind actors and other readers that none of the exceptions established or revised by this final rule, and none of the other six exceptions codified in 45 CFR part 171, are intended to override any other applicable law that compels access, exchange, or use of EHI.)

Comments. Some commenters did not support the proposal. Two of these commenters expressed concern that the proposal could impede enforcement of, or investigations into possible violations of, Federal and State laws such as those

regulating reproductive health care. One commenter stated that the exception is not reasonable and necessary as required by the Cures Act and is arbitrary and capricious in violation of the Administrative Procedure Act. One of these commenters connected opposition to the proposal to the commenter’s view that actors should not be expected to evaluate or determine the lawfulness of others’ actions. Other commenters expressed concern that the proposal could give actors too much power to withhold or limit access to information, that EHR developers would disproportionately benefit from the proposal, or that EHR developers might use the Protecting Care Access Exception to limit data sharing in a way that benefits them and harms patients. One commenter generally opposed the exception and stated that the use of pronouns other than those connoting a person is male or female, or pronouns not matching the patient’s sex assigned at birth, could lead to a lower quality of medical care. A few commenters stated that their concerns about the proposed exception should be addressed by placing control with providers as to whether the exception applies, prohibiting actors from using the exception for commercial gain, or ensuring that patients understand when their data is requested, disclosed, or protected by the exception. Other commenters suggested that health IT developers of certified health IT should be required to enable a user to restrict uses or disclosures when requested by the patient, stating this requirement would help reduce “overly broad” restrictions on interoperability or EHI sharing.

Response. Having considered all comments received, in context of the totality of feedback on the proposed exception, we have concluded that finalizing the exception as proposed is consistent with identifying, through notice and comment rulemaking, reasonable and necessary activities that do not constitute information blocking. We do not believe the exception impedes investigation or enforcement of independent laws enforceable against any actor in a court with jurisdiction over the actor and subject matter. As we have repeatedly reminded actors in this final rule and as is the case with exceptions previously established in 45 CFR part 171, the Protecting Care Access Exception (§ 171.206) 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. Moreover, the Protecting Care Access Exception, like all information blocking exceptions, is voluntary. It is not intended to create an affirmative obligation for an actor to evaluate whether a risk of potentially exposing anyone to legal action from any particular EHI access, exchange, or use scenario(s) might occur.

Because the Protecting Care Access Exception is unrelated to the use of pronouns in medical documentation, and does not require any actor to withhold any of a patient's EHI from any health care provider treating the patient, a health care provider's use of pronouns or any other demographic data is outside the scope of this exception.

Commenters' suggestions that health IT developers of certified health IT should be required to enable a user to restrict uses or disclosures when requested by the patient are beyond the scope of this exception. As we explained earlier in this final rule's preamble, in discussing the finalized revision to sub-exception (e) of the Privacy Exception at § 171.202, suggestions that ASTP/ONC mandate health IT include particular functionalities are outside the scope of any enhancement to the information blocking regulations (45 CFR part 171) included in the HTI-2 Proposed Rule. The Infeasibility Exception's *segmentation* condition (§ 171.204(a)(2)) accommodates actors who are unable to unambiguously segment data they have chosen to withhold consistent with another applicable exception—such as § 171.202(e) (“individual's request not to share EHI”)—from other EHI they could share with a requestor. We discuss earlier in this preamble revisions to § 171.204(a)(2) that include adding explicit reference to the Protecting Care Access (§ 171.206). We refer readers interested in learning more about how information blocking exceptions may be used in complement when an actor wishes to engage in a practice that is not fully covered by a single exception to the discussion of that topic in the HTI-1 Final Rule (89 FR 1353 and 1354).

In finalizing the initial information blocking exceptions in the ONC Cures Act Final Rule, we stated that we were guided by three overarching policy considerations: that exceptions are limited to certain activities that we believe are important to the successful

functioning of the U.S. health care system, that exceptions are intended to address a significant risk that regulated individuals and entities will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking, and that each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt (85 FR 25649).

This finalized exception aligns with these same policy considerations. As we explained in the HTI-2 Proposed Rule, we had at that time come to understand that some health care providers and other actors had 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 remain permissible under applicable law (89 FR 63629). We believe that the many comments we received in support of finalizing the Protecting Care Access Exception, as proposed or with various adjustments to make it easier for actors to use, validate our balancing of actors' concerns. Information provided in such comments supports our belief that actors' and patients' response to these concerns in the absence of the Protecting Care Access Exception has contributed to patients withholding information from their health care providers and health care providers avoiding creation of EHI, such as through use of paper recordkeeping; both of these solutions we believe have a much greater negative impact than this narrowly tailored information blocking exception could on care quality, coordination, and advancement of an interoperable nationwide health information infrastructure where sharing EHI consistent with applicable law and patient preferences is the norm and withholding EHI is the exception.

We believe that addressing actors' uncertainty specific to information blocking by finalizing the Protecting Care Access Exception will 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. We noted this belief in proposing this new exception (89 FR 63620). By addressing an actor's concern about potential exposure to legal action flowing from an access, exchange, or use of EHI related to reproductive health care, the exception addresses the risk that actors such as

health care providers may be unable to provide care that will best meet the patient's needs (89 FR 63631), among other risks we describe in the HTI-2 Proposed Rule's preamble (89 FR 63630). The exception is also tailored to limit its application to the reasonable and necessary activities enumerated within the exception, consistent with our approach to establishing the initial eight information blocking exceptions (89 FR 63632).

We plan to remain alert for signals that any type(s) of actor—not just health IT developers of certified health IT—may be attempting to misuse any of the exceptions in 45 CFR part 171. We would anticipate engaging in education and outreach as well as (where applicable) enforcement steps in response to such signals and may consider future proposals for 45 CFR part 171 in response to changing market conditions.

Comments. One commenter stated that it is not the responsibility of the health IT developer or health care provider to assess the motivations of an otherwise legal request for information, or to take actions to restrict data sharing that could be unlawful in some states. One commenter expressed concern about setting a precedent where an actor's practice is not considered information blocking but may still be a violation of another law.

Response. For an actor's practice to be covered by the finalized Protecting Care Access Exception, there is no specific requirement that the actor must assess the motivations of any request for EHI access, exchange, or use for permissible purposes. The finalized exception in no way requires any actor to take any action that would violate any law enforceable against the actor.

All information blocking exceptions are voluntary. They offer actors assurance that a practice consistent with one or, where applicable, more exceptions will not meet the “information blocking” definition (in § 171.103 or PHSA section 3022(a)) even if such practice is not required by law and is likely to interfere with access, exchange, or use of EHI. The Protecting Care Access Exception is responsive to concerns we have heard from the regulated community; it is intended to address these concerns for actors who choose to limit EHI sharing under the exception's conditions. The Protecting Care Access Exception is not intended to create a mandate that an actor engage in any practice(s) the exception would cover if the actor does not want to engage in such practice(s). Also, actors who may choose to limit availability of applicable EHI under the conditions of

the finalized Protecting Care Access Exception will nevertheless continue to be subject to other Federal laws, and to State and Tribal laws. We emphasized in the HTI–2 Proposed Rule that this would be the case if the Protecting Care Access Exception were to be finalized (89 FR 63632) and noted this is also the case with exceptions that had previously been established in 45 CFR part 171. We reiterate that the Protecting Care Access Exception does *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. Because we have explicitly, and repeatedly, reminded actors in the HTI–2 Proposed Rule⁴⁵ and this final rule⁴⁶ that information blocking exceptions do not override such obligations, we presume such actors will, therefore, account for this reality in their approach to maintaining compliance with the laws to which they are subject.

Comments. Some commenters stated that the proposed exception would be difficult to implement because the actor's staff may have different interpretations of potential legal risk or because there are not existing technical standards which could be leveraged to support the exception's implementation, particularly the ability to identify and segment relevant EHI.

Response. If an actor is concerned about different members of their staff having different understandings of legal risks or when the exception would apply, we refer the actor to the finalized conditions of the exception. These include an option to satisfy the § 171.206(a)(3) implementation requirement by implementing practices consistent with an organizational policy that meets subparagraph (i) of § 171.206(a)(3). It has been our observation that developing and training relevant staff on written organizational policies is a strategy that helps an organization's personnel understand how to proceed, and to act consistently, in relevant scenarios.

We recognize that the capabilities of existing health IT continue to evolve, and that there is variation in health IT products' ability to segment EHI that a health care provider or a patient may wish to withhold from various access, exchange, or use scenarios from other EHI with the levels of precision and automation that providers and patients would prefer. In the HTI–2 Proposed

Rule, we stated that because there is a potential that some actors who may wish to withhold specific EHI under the conditions specified in the 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, we proposed 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 (89 FR 63634). We refer readers to the section of this final rule preamble where we discuss the finalized revision to the Infeasibility Exception's *segmentation* condition (§ 171.204(a)(2)).

Comments. One commenter encouraged ASTP/ONC to engage in further discussions with stakeholders to refine the proposals and to align them further with HIPAA and other HHS regulations rather than adopting the proposed exception. Some commenters suggested that ASTP/ONC require health IT developers of certified health IT enable a user to implement a process to restrict uses or disclosures of data in response to a patient request when such restriction is necessary, citing 88 FR 23822. Another commenter encouraged ASTP/ONC to strengthen certification criteria for capabilities to allow clinical users to tag and withhold data from exchange.

Response. We recognize that no information blocking exception can address all of the concerns a person may have about potential exposure of various persons to legal action for the mere act of seeking, obtaining, providing, or facilitating reproductive health care (as we noted in the HTI–2 Proposed Rule at 89 FR 63630). While we appreciate the commenters' suggestions, their requests specific to imposing certain requirements on developers of certified health IT, which appear to refer to ASTP/ONC's proposal in the HTI–1 Proposed Rule to adopt a new certification criterion "patient requested restrictions" in § 170.315(d)(14) which was not finalized in the HTI–1 Final Rule (89 FR 1301), are outside the scope of this rulemaking. We will continue to work with our federal partners to promote alignment on, and understanding of, regulations which support the lawful access, exchange, and use of electronic health information. We also note that we may consider amending relevant ONC Health

IT Certification Program or information blocking regulations in future rulemaking in response to changing market conditions.

Comments. Several commenters requested that we develop guidance, education, examples, and training materials on the Protecting Care Access Exception, including for specific situations and fact patterns and materials for both providers and patients. For example, one commenter requested guidance specifically on how health care practices who serve patients who live in a different state can protect the information of their patients. Some commenters stated that actors such as health care providers have sometimes been hesitant or fearful to use information blocking exceptions, and that guidance and educational materials from ASTP/ONC are essential. Several commenters also noted the need for health care providers to engage with a variety of internal and external partners and entities in the implementation of their policies to comply with the information blocking regulations. One commenter requested that ASTP/ONC include examples, objective criteria for assessing legal risks, and best practices for documentation and patient communication in its guidance. Another commenter asked ASTP/ONC to include use cases in this final rule to help actors operationalize it. One commenter stated that ASTP/ONC should undertake education on information blocking more broadly. One commenter recommended, as part of implementation of the Protecting Care Access Exception, education for providers about the exception (and other information blocking exceptions) and best practices to protect sensitive health information and facilitate care coordination that supports confidentiality, safety, and autonomy for individuals.

Response. The requests and recommendations for additional guidance, training, examples, and educational materials on the information blocking exceptions are appreciated. We have not provided criteria for assessing legal risks in this final rule because we have finalized, as proposed, the subjective "good faith" standard for the § 171.206(a)(1) belief requirement. An actor would be free to reference or apply objective legal risk assessment criteria in determining whether they wish to engage in a practice the Protecting Care Access Exception would cover, if that is how the actor prefers to make such decisions. But we emphasize that because the finalized belief standard is a subjective standard it does *not* require an actor to reference or apply objective risk

⁴⁵ 89 FR 63509, 89 FR 63622, 89 FR 63632, 89 FR 63637, and 89 FR 63639.

⁴⁶ In addition to the reminder in this paragraph, we have reiterated it multiple times in this final rule preamble.

assessment criteria; any actor who wishes to do so could implement a practice consistent with the *threshold* condition (§ 171.206(a)) without having applied objective legal risk assessment criteria.

As part of our ongoing outreach and education, all feedback and information we receive helps to inform our consideration and ongoing development of resources such as webinar presentations, fact sheets, guidance, and frequently asked questions (FAQs). As new resources become available, they are publicly posted on ASTP/ONC's internet website: <https://www.healthit.gov>. Actors and other interested parties who would like to do so can also subscribe to ASTP/ONC email updates and be among the first to hear about newly posted resources and opportunities to register for upcoming webinars. (A subscription can be created or updated through ASTP/ONC's online Email Subscription Preference Center; for which the URL as of the date this final rule is published is: https://www.healthit.gov/PreferenceCenter?qs=1&form=HealthIT_PreferenceCenter&height=1100&mbreak=800&mheight=1600.)

Comments. Some commenters stated that ASTP/ONC and OIG should focus on enforcement with corrective action plans as opposed to the imposition of civil monetary penalties. One commenter stated that ASTP/ONC should exercise enforcement discretion for medical groups.

Response. Details of the enforcement process for actors who may be found to have engaged in information blocking, including imposing corrective action programs, are outside the scope of this rulemaking. In light of the many comments calling for ongoing education and information about all aspects of information blocking, we remind readers that ASTP/ONC has authority to review claims of potential information blocking against health IT developers of certified health IT that may constitute a non-conformity under the ONC Health IT Certification Program. Separately, OIG has authority to investigate claims of potential information blocking across all types of actors: health care providers, health information networks and health information exchanges, and health IT developers of certified health IT. We refer readers seeking additional information about the "OIG Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules" final rule (OIG Final Rule) implementing information blocking civil monetary penalties (88 FR 42820) to OIG's website (<https://>

oig.hhs.gov/reports-and-publications/featured-topics/information-blocking) and those seeking more information about the "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" final rule (Information Blocking Provider Disincentives Final Rule) (89 FR 54662) to ASTP/ONC's website (<https://www.healthit.gov/informationblocking>). ASTP/ONC's website also provides information on how to submit an information blocking claim and what happens to a claim once it is submitted.

Comments. A few commenters stated that they did not support adding any additional or alternative conditions or requirements to the Protecting Care Access Exception. Some of these commenters stated that additional conditions or requirements would make the exception more complex, and that complying with various State or Federal laws relating to reproductive health care is already complex for health care providers. Some commenters also stated that adding additional conditions to the exception would not reduce the risk of information blocking or improper use of the exception or were unnecessary because other laws such as HIPAA already have their own requirements or enforcement mechanisms. One commenter asked that the exception consist of only the good faith belief condition, stating that the additional requirements created uncertainty and documentation burden.

Response. We appreciate the concerns raised by the commenters. We have not finalized any additional or alternative conditions or requirements for the Protecting Care Access Exception at this time. We will continue working with the regulated community and other interested parties to promote awareness of all of the information blocking exceptions.

We recognize that the health care and health privacy legal landscape is complex for reasons outside the scope of this final rule. However, we do not believe that an exception consisting of only the good faith belief portion of the threshold condition would provide patients or health care providers with adequate assurance that actors (including other health care providers) implement practices under the exception fairly, consistently, and with appropriate consideration of risks of legal action based on the mere fact that someone sought, obtained, provided, or facilitated (or, for the patient protection condition, may have sought, obtained, or needed) reproductive health care that was lawful under the circumstances.

As we stated in the HTI-2 Proposed Rule on how the information blocking regulations operate, the information blocking regulations operate both separately and differently from the HIPAA regulations (89 FR 63629). The information blocking regulations are based on statutory authority separate from HIPAA. 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 and the discussion in the HTI-2 Proposed Rule at 89 FR 63628 through 89 FR 63633.

We have finalized the exception's conditions as proposed because we believe they strike the best balance we can attain at this time between the interests of actors and patients in protecting reproductive health care availability and patients' reproductive health privacy with the interests of actors, patients, and others in maintaining and building upon progress made to date toward EHI interoperability and a norm of information sharing that includes individuals being able to easily access, exchange, and use their EHI however and whenever they want. We will remain alert for signals that any type(s) of actor—not just health IT developers of certified health IT—may be attempting to misuse any of the exceptions in 45 CFR part 171. We would anticipate engaging in education and outreach as well as (where applicable) enforcement steps in response to such signals and may consider future proposals for 45 CFR part 171 in response to changing market conditions.

Comments. A few commenters stated that it is important for ASTP/ONC to address that public health use cases for reproductive health data remain relevant while that data is also protected by the Protecting Care Access Exception. The commenters stated that there may be important reasons to send reproductive health data to public health entities while at the same time segmenting that data from being used for other purposes, because that data may be critical to public health functions. Some of these commenters stated they favor provisions to ensure that reproductive health data transmitted electronically is restricted to public health use cases and may not be reused later for non-public-health purposes.

Response. We appreciate the comments. We emphasized in the HTI–2 Proposed Rule (at 89 FR 63632) that actors would continue to be subject to other Federal laws, and to State and Tribal laws. With regard to public health reporting, we stated in an information blocking FAQ (IB.FAQ43.1.2022FEB)⁴⁷ that where a law requires actors to submit EHI to public health authorities, an actor’s failure to submit EHI to public health authorities could be considered an interference under the information blocking regulations. For example, many states legally require reporting of certain diseases and conditions to detect outbreaks and reduce the spread of disease. Should an actor that is required to comply with such a law fail to report, the failure could be an interference with access, exchange, or use of EHI under the information blocking regulations.⁴⁸

Establishing or explaining which use cases represent permissible purposes for access, exchange, or use of reproductive health care EHI (or any other EHI) under independent laws that may apply to various actors in various circumstances is beyond the scope of this final rule. We refer readers to the definition of “public health” in 45 CFR 160.103, and extensive interpretation in the 2024 HIPAA Privacy Rule (89 FR 32976) clarifying that activities such as investigation, intervention, or surveillance in the public health context do not encompass conducting a criminal, civil, or administrative investigation into any person, or imposing criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating health care, or identifying any person for such activities, including those for which use or disclosure of PHI is prohibited by 45 CFR 164.502(a)(5)(iii).

Comment. One commenter asked that we clearly state that information blocking requirements do not apply to non-clinical public health (e.g., disease surveillance programs).

Response. Opining or advising on whether a particular type of organization or function would or would not meet the § 171.102 “actor” definition is beyond the scope of this final rule.

Comments. Several commenters expressed concern about their ability to “comply” with the proposed Protecting Care Access Exception “requirement,”

citing a lack of capability or conflicts with state laws.

Response. Information blocking exceptions are voluntary as we have stated repeatedly over time, including in the ONC Cures Act Final Rule (85 FR 25892), HTI–1 Final Rule (89 FR at 1353, 1378, 1383, and 1392) and the HTI–2 Proposed Rule (89 FR 63638). The information blocking exceptions defined in 45 CFR part 171 offer actors certainty that any practice meeting the conditions of one or more exceptions would not be considered information blocking, but they are not mandatory.

The use of the word “requirement” in describing any provision of any information blocking exception in 45 CFR part 171 is not intended to imply that actors must satisfy the provision regardless of whether they wish to engage in a practice to which the exception applies. We refer to “requirements” as the way(s) to satisfy a condition of an exception only to make it clear that if an actor’s practice does not meet what is specified (i.e., required), then the actor’s practice will not be covered by that exception. For example, if an actor wants to share all the EHI that they have and all laws and regulations that apply to the actor and the EHI permit it to be shared with any requestor, then no exception in 45 CFR part 171 is intended to create an affirmative obligation that the actor instead withhold EHI. Rather, an exception offers an actor who chooses to engage in a practice meeting the exception’s conditions assurance that such practice will not be “information blocking” even though the practice may be likely to interfere with access, exchange, or use of EHI for purposes permissible under all applicable law (such as the HIPAA Privacy Rule, State or, where applicable, Tribal privacy laws).

Comment. One commenter was concerned that the regulation did not mention a date when information blocking exceptions would be “enforceable.”

Response. The information blocking regulations in 45 CFR part 171, including the first eight exceptions, first became effective on April 5, 2021 (85 FR 70068 and 70069) and actors were subject to the regulations upon the effective date. The OIG Final Rule provisions implementing information blocking penalties (88 FR 42826) have been in effect since September 1, 2023. The Information Blocking Provider Disincentives Final Rule (89 FR 54662) became effective as of July 31, 2024.

The Protecting Care Access Exception will be available to actors on and after the effective date of this final rule. The

finalized revisions to § 171.202(e) and § 171.204(a)(2) will also be effective on and after that date.

Comments. Several commenters made statements about what the HIPAA Rules require, permit, and do not permit with respect to sharing information related to reproductive health, and how HIPAA relates to the Protecting Care Access Exception. Some commenters encouraged working with OCR and across HHS to align the information blocking regulations with the HIPAA Rules. One commenter requested clarification that ASTP/ONC has considered and accounted for any disclosure consent that is required under changes to HIPAA as it relates to reproductive health care. One comment sought clarification of how a health care provider could get or share EHI without being a HIPAA covered entity.

Response. As we stated in the HTI–2 Proposed Rule on how the information blocking regulations operate, the information blocking regulations operate both separately and differently from the HIPAA regulations (89 FR 63629). The information blocking regulations are based on statutory authority separate from HIPAA. 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 and the discussion in the HTI–2 Proposed Rule at 89 FR 63628 through 89 FR 63633. The 45 CFR 164.509 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 is discussed at 89 FR 63628. We plan to continue to work with our federal partners, including OCR, to maintain alignment on, and promote understanding of, regulations which support the lawful access, exchange, and use of electronic health information.

Interpreting the HIPAA regulations in 45 CFR parts 160 and 164, such as by offering guidance as to when or how a health care provider might be capable of or engaged in getting or sharing EHI without also being a HIPAA covered entity, is outside the scope of this rule. We therefore refer readers with questions about HIPAA covered entities to the guidance and informational resources available from both the OCR website: (<https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>) and the CMS website

⁴⁷ <https://www.healthit.gov/faq/would-not-complying-another-law-implicate-information-blocking-regulations>.

⁴⁸ *Ibid.*

(<https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/hipaa/covered-entities>). Additional information about HIPAA transactions is available via the following section of the CMS website: <https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification>.

Comments. A few commenters requested that ASTP/ONC clarify the intersection of the proposed Protecting Care Access Exception with state laws and other laws such as 42 CFR part 2 or the HIPAA Privacy Rule. These commenters expressed the importance of safeguarding information concerning seeking care for substance use disorder during pregnancy.

Response. We appreciate the comments received and the insights they offer into the challenges associated with managing information concerning seeking care for substance use disorder during pregnancy. We emphasize that where otherwise applicable law prohibits a specific access, exchange, or use of information, an exception to part 171 is not necessary due to the exclusion of “required by law” practices from the statutory information blocking definition—as we have previously noted (for example, at 85 FR 25825).

Any changes to or interpretation of 42 CFR part 2, which is issued by the Substance Abuse and Mental Health Services Agency (SAMHSA) pursuant to statutory authority separate from the information blocking statute, are out of scope for this final rule. Similarly, interpretation of any State or Tribal law (statute or regulation) is outside the scope of this final rule.

Interpreting or otherwise providing guidance on the HIPAA regulations in subchapter C of subtitle A of title 45 of the CFR is outside the scope of this final rule. We therefore refer readers with questions about HIPAA covered entities to the guidance and informational resources available from both the HHS OCR (<https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>) and the CMS website (<https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification/hipaa/covered-entities>). Additional information about HIPAA transactions is available via the following section of the CMS website: <https://www.cms.gov/priorities/key-initiatives/burden-reduction/administrative-simplification>.

As noted above, 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 and the discussion in the HTI–2 Proposed Rule at 89 FR 63628 through 63633. We will continue to work with our federal partners, including OCR, to promote alignment on, and understanding of, regulations which support the lawful access, exchange, and use of electronic health information.

Comments. One commenter appreciated that ASTP/ONC recognized the interplay between the proposed Protecting Care Access Exception, the existing Infeasibility Exception (particularly, the Segmentation sub-exception) and the Privacy Exception (specifically, Individual’s Request Not to Share EHI sub-exception) given that advanced capabilities to easily segment data are not uniformly available for all EHR and health IT systems. Another commenter asked ASTP/ONC to clarify how the Protecting Care Access Exception would intersect with the Infeasibility Exception. Noting that the proposal indicated that the redacted information must only be that which is believed to put an individual at risk of legal action, the commenter stated it was unclear whether the Infeasibility Exception could be used with this exception when segmentation is not available and asked ASTP/ONC to clarify whether such a combination of exceptions is permitted.

Response. We appreciate the comment. As discussed above, the HTI–2 Proposed Rule’s proposed revisions to the Infeasibility Exception’s *segmentation* condition (§ 171.204(a)(2)) included addition of an explicit cross-reference to the Protecting Care Access Exception (§ 171.206) (89 FR 63623). In various circumstances, an actor may wish to engage in one or more practice(s) that are covered in part, but not fully covered, by the Protecting Care Access Exception. In some of these situations, such an actor may want to consider the potential certainty that could be available by satisfying a combination of the Protecting Care Access Exception and the Infeasibility Exception (§ 171.204). (We note that this is only one example where “stacking” of exceptions may occur; there may be a wide variety of scenarios where “stacking” other combinations of various exceptions with one another—or with restrictions on use or disclosure of EHI under applicable law—may occur, as we discussed in more detail in the HTI–1 Final Rule preamble, 89 FR 1353 through 1354).

The information blocking exceptions operate independently. In the HTI–2

Proposed Rule, we stated that 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 (89 FR 63631). 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 (89 FR 63631).

b. Threshold Condition and Structure of Exception

We proposed that the § 171.206(a) *threshold* condition’s requirements must be satisfied in order for any practice to be covered by the exception (89 FR 63633). To meet the condition’s subparagraph (a)(1) belief requirement, we proposed that the practice must be undertaken based on a good faith belief that:

- the person(s) seeking, obtaining, providing, or facilitating reproductive health care is 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)), we proposed that the actor’s belief need not be accurate but must be held in good faith. We also sought 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 requested input from commenters regarding concerns they might 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.

We also sought comment about setting the belief standard at “belief” or “honest belief” as alternatives to the good faith standard, and whether those standards might help to reduce misunderstanding of § 171.206(a). We sought comment on whether to add to § 171.206 a provision to presume an actor’s belief met the standard unless we have or find evidence that an 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,” each of “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 belief,” neither “belief” nor “honest belief” is a particularly long established and widely used legal standard. However, we requested input 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.

We noted that 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 proposed 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 proposed in § 171.206(e) (89 FR 63804) to define “legal action” for purposes of the Protecting Care Access Exception to 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 (89 FR 63639). We emphasized 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 (89 FR 63639).

We emphasized 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)).⁴⁹ Thus, a practice could satisfy the exception as proposed *only if* implemented based on an actor’s good faith belief that access, exchange, or use potentially creates or increases anyone’s risk of facing legal action that would be specifically 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 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)) was proposed to 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 particular access, exchange or use of specific EHI that is affected by the practice. We stated (89 FR 63634) that 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,

⁴⁹ 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.

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, we noted that 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.

We noted that 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 noted in the HTI–2 Proposed Rule at 89 FR 63634 that we were aware of the external efforts to innovate and further develop consensus technical standards, and we are hopeful that this will foster routine inclusion of advanced data segmentation capabilities in 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 and 23875) that

indicates 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 proposed elsewhere in the HTI-2 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 (89 FR 63633 and 63634).

We stated (89 FR 63634) that 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 proposed 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 or relationship 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.

We stated that 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. To clarify, we note that a policy would need to specify the facts and circumstances under which the policy would apply to 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.

We noted (89 FR 63634) that 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 at § 171.102. However, we did 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 noted that we believed 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. As we discussed (89 FR 63635), 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 (89 FR 63634 and 63635). 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 (89 FR 63635).

We explained (89 FR 63635) that 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 also sought comment (89 FR 63635) on 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 proposed 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).

The following is a summary of the comments we received and our responses, organized by specific subparagraph within the § 171.206(a) *threshold* condition.

Threshold Condition, General

Comments. One commenter advocated a two-step approach so the actor who "owns" the EHI would be the first to decide whether to invoke the exception. If such actor decided to withhold EHI based on the exception, then the commenter stated a business associate or other actor performing services on behalf of the "owning" actor should be bound by that decision because it is acting on behalf of the "owning" actor. The commenter stated that if the "owning" actor does not invoke the exception, the business associate or other actor performing services should be able to make an independent decision as to whether to invoke the exception. Some commenters suggested that only actors who are health care providers should be able to utilize the exception although they did not expressly address whether they believed another actor who holds EHI on behalf of such a provider would be required to follow the provider's decision.

Response. We appreciate the opportunity to clarify that, like all information blocking exceptions, the Protecting Care Access Exception, as proposed and as finalized, is voluntary for any actor. We interpret the one commenter's references to an actor "owning" EHI as the commenter's shorter way of saying the actor who maintains EHI on or on whose behalf another actor maintains or otherwise handles EHI. We decline to adopt at this time a requirement that an actor performing services on behalf of another follow the decision of the actor who maintains EHI, or on whose behalf EHI is maintained, to withhold EHI consistent with the Protecting Care Access Exception. A *mandate* that any actor conform their practices to an exception based on another actor's choice to do so would be both unprecedented in 45 CFR part 171 and beyond the scope of any alternative provision for § 171.206 on which we

solicited comments in the HTI-2 Proposed Rule.

We proposed, and have finalized, the Protecting Care Access Exception to be available to all actors. We did not propose an option or alternative for the exception to be available only to certain type(s) of actor. Moreover, we believe that making the Protecting Care Access Exception available only to health care providers would add unnecessary complexity to the information blocking regulations while potentially failing to support providers' ability to implement practices consistent with the exception. If the Protecting Care Access Exception were not equally available to health IT developers of certified health IT and HINs/HIEs on whom health care providers often rely for many or all of their health IT, these actors would be left with the same uncertainty they have experienced to date about potentially implicating the information blocking definition. For example, a health IT developer of certified health IT or a HIN/HIE would be left with uncertainty about implicating the information blocking definition if they were to limit access, exchange, or use of reproductive health care EHI at the direction of a health care provider, but the Protecting Care Access Exception were applicable only to practices undertaken by health care providers.

Comments. Several comments requested that we indicate whether care would or would not be lawful in a variety of scenarios involving various intersections of Federal law with State(s)' laws, State(s)' law with Tribal law, or Federal and Tribal law with State(s)' law. One commenter suggested that carefully defining these would ensure that the exception is carefully targeted in scope. One commenter suggested we remove references to care being lawful where furnished, citing scenarios where a patient may seek lawful follow-on care for complications of self-administered care that the commenter asserted is not required to be reported to law enforcement under state law.

Response. Opining on what care is or is not lawful under what specific circumstances, or advising on which laws take precedence in any specific fact pattern, is beyond the scope of this final rule. The exception is designed to accommodate the wide variety of scenarios where reproductive health care is (or the actor may for purposes of the exception presume it is) lawful under the circumstances in which it is provided. We decline at this time to remove references to care being lawful where furnished, because such references provide clarity to actors

regarding our intent with regards to the applicability of the Protecting Care Access Exception. For example, we noted in the HTI-2 Proposed Rule that the exception is not intended to apply, and as finalized in this rule it does not apply, to an actor's attempt to avoid consequences for the actor's own wrongdoing (89 FR 63636) or limit 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 to a patient (or their representative) alleges was negligent, defective, substandard, or otherwise tortious (89 FR 63632).

Threshold Condition—Belief Requirement

Comments. Many commenters supported the proposed exception, explicitly as proposed or without further comments. Some of them expressly supported the good faith belief standard. A few commenters noted that "good faith belief" is a subjective standard and supported the use of a subjective standard. A few commenters expressed support for the alternative standard of "belief" or "honest belief" rather than "good faith belief" for purposes of the *threshold* condition at § 171.206(a)(1). These commenters stated that using "belief" or "honest belief" as the standard would reduce potential misunderstandings while encouraging appropriate use of the exception by providing actors with as much flexibility as possible to protect patients and providers. One commenter suggested that good faith belief and honest belief were synonymous but in either case, ASTP/ONC should state that the standard is subjective. A few commenters asked for outreach and education to promote accurate understanding of the standard and actor confidence in their ability to use the exception.

Response. We thank commenters for their feedback. Having reviewed and considered all comments received in response to the proposal, we have finalized § 171.206(a)(1) as proposed. As we stated in the HTI-2 Proposed Rule, to satisfy the § 171.206(a)(1) belief requirement, the actor's belief need not be accurate (89 FR 63633). We have updated the regulatory text to state that for purposes of the Threshold Condition, an actor who is a business associate of or who otherwise maintains EHI on behalf of another actor may rely on the good faith belief (consistent with § 171.206(a)(1)) and organizational policy (consistent with § 171.206(a)(3)) of the actor on whose behalf the relevant EHI is maintained. As noted in the HTI-

2 Proposed Rule and above, unlike “good faith,” neither “belief” nor “honest belief” is a particularly long established or widely used legal standard (89 FR 63633). We also affirm that the finalized “good faith belief” standard is a subjective standard. As we noted in the HTI–2 Proposed Rule preamble, the alternatives (“belief” and “honest belief”) were, like the “good faith belief” standard, subjective standards (89 FR 63633). Also, we provide in response to other comments (below) additional discussion to help actors understand what it means, in specific context and for the specific purpose of an actor’s practice meeting the § 171.206 exception’s conditions, to hold a belief in good faith.

Comments. Several comments supported adding a provision to presume an actor’s belief met the standard unless we have or find evidence that an actor’s belief did not meet the standard at all relevant times. Commenters stated that this provision would promote alignment with HIPAA, reduce confusion in light of rapidly shifting state laws, and strengthen the protections of this new exception. One commenter asked that this presumption of good faith would only be able to be rebutted with clear and convincing evidence, which they noted is a well-established legal standard.

Response. We appreciate the comments advocating for a presumption provision for “good faith belief.” Commenters did not supply reasons supporting the assertion that a presumption provision for “good faith belief” would align with HIPAA as there is no generally applicable presumption of good faith in the HIPAA Rules. Having reviewed and considered all comments received in response to the proposed Protecting Care Access Exception, we have decided not to adopt in regulation an explicit presumption for “good faith belief” at this time. Instead, we emphasize, as we stated in the HTI–2 Proposed Rule, that “good faith belief” is a subjective standard. To meet this standard for purposes of an actor’s practice meeting the conditions of the finalized Protecting Care Access Exception, an actor’s belief need not ultimately be accurate; it only need to be held in good faith. In response to concerns about how an actor would demonstrate good faith, we note that the § 171.206(a) *threshold* requirement is designed to function as a cohesive whole, within which one of the functions of the paragraph (3)(i) requirement that an organizational policy be in writing is to document what the actor believes. This includes identifying the connection between the

particular access, exchange, or use scenarios for specific EHI with which the practice based on the policy interference and the risk of potential exposure to legal action the actor has a good faith belief could be created by such access, exchange, or use of that EHI. The paragraph (3)(ii) requirement that any case-by-case determination be documented either before or contemporaneous with the actor beginning to engage in any practice(s) based on the determination serves the same purpose.

We also note that whether a belief is held in good faith for purposes of § 171.206(a) may be partly proven by the absence of indicators of bad faith, such as indicators that the actor’s claim of having met the exception may in fact be pretextual. One illustrative example or indicator of bad faith (of which there could be many more) would be if the actor in practice only withholds EHI based on their purported belief when the EHI is requested by a competitor or potential competitor of the actor, while not withholding EHI from otherwise similarly situated non-competitor requestors. By contrast, indicators of good faith would include, among others, that the actor applies the same practices to all requests from any and all similarly situated requestors, with no difference in applying the practice to requests from competitors or potential competitors in comparison to affiliates or other non-competitors. For these reasons, we have decided that that the subjective “good faith belief” standard we have finalized properly accommodates actors who are unsure of their risks.

Comments. One commenter suggested that the subjective good faith standard should be harmonized with the objective standard used in the 2024 HIPAA Privacy Rule. One commenter stated that the “good faith belief” threshold was not high enough, especially when EHI is requested for treatment.

Response. While “good faith belief” is a subjective standard (89 FR 63633), we believe that a subjective standard is important to offer actors, including health care providers, the flexibility they need to care for their patients through promoting effective relationships with them based on mutual trust. Given the substantive policy approach differences between information blocking exceptions and the HIPAA Privacy Rule’s permitted and prohibited uses and disclosures, we note that use of a subjective standard for this voluntary exception within the information blocking regulations is fully compatible with the HIPAA Privacy Rule’s use of objective standards in

prohibiting the use or disclosure of PHI for specific activities. The Protecting Care Access Exception is intended to be available and usable for all actors, including small actors with limited resources (such as safety net health care providers) who might struggle to evaluate the many particular EHI sharing scenarios that they encounter against an objective standard. Moreover, the exception is not relevant where the EHI involved is also PHI subject to a prohibited use or disclosure under the HIPAA Privacy Rule. This is because where applicable law prohibits a specific access, exchange, or use of information, the information blocking regulations consider the practice of complying with such laws to be “required by law.” Practices that are “required by law” are not considered “information blocking” (see the statutory information blocking definition in section 3022(a)(1) of the PHS Act and the discussion in the ONC Cures Act Final Rule at 85 FR 25794).⁵⁰

Comments. One commenter stated that they approve of ASTP/ONC’s choice of “could reduce that risk” rather than “would,” “likely would,” or “should,” in paragraph (a)(1)(ii) of the Protecting Care Access Exception, referring to the practice undertaken based on the actor’s good faith belief that specific practices likely to interfere with access, exchange, or use of electronic health information could reduce the risk of being potentially exposed to legal action. The commenter stated that the approach differs from ASTP/ONC (and often CMS and other HHS partners’) practice of trying to maximize data sharing while considering privacy concerns that might inhibit sharing because using the words “could reduce that risk” make it less likely that data will be shared, compared to using words such as “would,” “likely would,” or “should.”

Response. We appreciate the comments and the commenter’s support. As we explained above, 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

⁵⁰ We refer readers interested in learning more about the interaction of the information blocking regulations with the HIPAA Rules and other laws protecting individuals’ privacy interests to the discussion of the Privacy Exception in the ONC Cures Act Final Rule (85 FR 25642, 85 FR 25845 through 25859) and the discussion of this topic in the HTI–1 Final Rule preamble (89 FR 1351 through 1354). We also highlight the availability of additional resources through our website (to quickly navigate to the information blocking section of HealthIT.gov, the following URL can be entered into a browser address bar or search bar: <https://www.healthit.gov/informationblocking>).

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.

Comments. No comments were received on the possible alternative proposal that each actor be required to rely only on its own good faith belief.

Response. We have finalized, as proposed, that where an actor is a business associate of another actor or otherwise maintains EHI on behalf of another actor, the Protecting Care Access Exception applies (where its requirements were otherwise fully satisfied) 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 (89 FR 63633). As discussed in the HTI–2 Proposed Rule, this means that where an actor is a business associate or otherwise maintains EHI on behalf of another actor, the finalized Protecting Care Access Exception (§ 171.206) will be applicable (where its requirements are otherwise fully satisfied) 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 have clarified this finalized policy by adding this wording as § 171.206(a)(4), so that this flexibility is immediately clear to actors from the face of the regulatory text.

We clarify, however, that where an actor is a business associate or otherwise maintains EHI on behalf of an entity that is not an actor (as defined in § 171.102), the Protecting Care Access Exception's *threshold* condition (§ 171.206(a)) will be satisfied only where the actor who maintains EHI holds a good faith belief consistent with § 171.206(a)(1) and implements a practice consistent with either § 171.206(a)(2)(i) or (ii). We specifically proposed that an actor could rely on the good faith belief and organizational policy or case-by-case determinations of another § 171.102 actor (89 FR 63633). We did not propose that an actor could rely on belief, policy, or case-by-case determination of any entity on behalf of whom the actor may maintain EHI. An entity that is not an actor subject to the information blocking regulations may be unlikely to address information blocking regulations in any of their policies, procedures, or regulatory compliance plans. Therefore, we believe that, *when* an actor is maintaining EHI on behalf of a non-actor entity, limiting

application of the finalized Protecting Care Access Exception to practice(s) undertaken based on the actor's own good faith belief and implemented consistent with the actor's own organizational policy or case-by-case determination is an important safeguard against attempts to misuse the exception (by accident or otherwise).

i. Threshold Condition—Tailoring Requirement

Comment. One commenter noted that requiring the practice be no broader than necessary to reduce the risk seemingly preempts health care providers from leveraging organization wide policies in order to avail themselves of this exception.

Response. The tailoring requirement in § 171.206(a)(2), like similar provisions in other exceptions, ensures that the exception will 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 access, exchange, or use of the specific portion(s) of the EHI that pose the risk. Individuals' EHI will often include a wide range of care types, many of which an actor would seem unlikely to have a good faith belief could expose anyone involved in the care to a risk of legal action *as defined in § 171.206(e)*. We emphasize that the finalized Protecting Care Access Exception does *not* 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 conduct *other than* the mere act of seeking, obtaining, providing, facilitating, or (where the *patient protection* condition applies) potentially needing, reproductive health care that under the circumstances was, or (where the *patient protection* condition applies) would have been, lawful.

When read as a whole, including the option for an actor's practice to satisfy the § 171.206(a)(3) implementation requirement by implementing the practice based on an organizational policy consistent with § 171.206(a)(3)(i), we believe the finalized *threshold* condition (§ 171.206(a)) provides adequate flexibility for actors who wish to do so to implement a practice based on organizational policy. As we

explained in the preamble proposing § 171.206(a)(3)(i), a policy's specifications need not be particularized to individual patients (89 FR 63634). We clarify that an organizational policy's specifications would also not need to be particularized to individual requests for access, exchange, or use of EHI in order to satisfy the requirements of § 171.206(a)(3)(i). For additional explanation of § 171.206(a)(3)(i) and (ii), we refer readers to the HTI–2 Proposed Rule preamble at 89 FR 63634 through 63635.

Comments. One commenter generally supported the Protecting Care Access Exception but expressed concern about how the tailoring requirement may be interpreted and enforced given the broad definition of reproductive health care. The commenter asserted that nearly every patient record contains information about reproductive health care under the HIPAA definition, which may make it difficult to tailor EHI. The commenter therefore asked that ASTP/ONC be flexible in its interpretation and enforcement of the tailoring practices, considering the breadth of the new HIPAA regulatory amendments and the state laws at issue. If ASTP/ONC is expecting hospitals to tailor their practices in a certain manner, the commenter asked ASTP/ONC to provide further information and resources on what constitutes tailoring. The commenter also noted the limited feasibility of data segmentation. Another commenter acknowledged the potential challenges for Health IT developers in generating the technological capabilities to meet the requirements of the Protecting Care Access Exception including that the practice is tailored to be no broader than necessary to reduce the risk of potential legal exposure.

Response. In context of the comment about whether ASTP/ONC may be expecting hospitals to tailor their practices in a certain manner, we interpret "manner" to mean particular health IT functionalities or workflows. We do not read "manner" in this context to mean by way of value set(s) within data elements specifically because we had indicated in the HTI–2 Proposed Rule that we did not propose to limit the application of the Protecting Care Access Exception to any specific value set(s) (89 FR 63634). We have not specified that any actor have or use certain functionalities or workflows in order to satisfy the § 171.206(a)(2) tailoring requirement. We refer readers to our explanation in the HTI–2 Proposed Rule (89 FR 63633) that the (§ 171.206(a)(2)) tailoring requirement is intended to restrict the exception's coverage to

practices that are no broader than necessary to reduce the risk of potential exposure to legal action.⁵¹ We emphasize that, 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.

In our discussion of the § 171.206(a) *threshold* condition's tailoring requirement (§ 171.206(a)(2)) in the HTI-2 Proposed Rule, we noted the importance of data segmentation for exchanging sensitive health data and enabling access, exchange, and use of EHI (89 FR 63634). We stated that 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 (89 FR 63634). At the same time, we also stated that public feedback has indicated 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. Given this varying capability, we acknowledged 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 (89 FR 63634). We therefore proposed 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. We refer

⁵¹ The tailoring requirement of the § 171.206(a) threshold condition does not include specifications that vary based on whether the actor falls into a specific category (such as health care provider) or is of a particular type of entity within any given category (such as "hospital" or "skilled nursing facility" within the health care provider category).

readers to discussion of the finalized § 171.204(a)(2) modification of this final rule preamble. We also refer readers, as mentioned previously, to the discussion in the HTI-1 Final Rule of how combination(s) of exceptions may be used when an actor wishes to engage in one or more practices that are covered in part (but not fully covered) by one exception (89 FR 1353 and 1354). We will continue working with interested parties and the regulated community to promote understanding and foster all actors' compliance with the information blocking regulations. Details of the enforcement process for actors who may be found to have engaged in information blocking are outside the scope of this rulemaking.

ii. Threshold Condition— Implementation Requirement

Comments. One comment noted the importance of a provider being able to implement the exception as part of an organizational policy because it is infeasible and a paperwork burden for providers to individually mark charts or data elements as sensitive. Another comment expressed appreciation that providers would be able to limit access to reproductive EHI as part of following organizational policies that are based on their expertise and suit their circumstances (such as technological capabilities, staffing, and the types of scenarios they have experienced or expect to experience) in addition to the case-by-case basis. Another commenter thought that the language of the exception contemplates workflows where actors are making manual decisions to withhold or release data but suggested that in practice, most of these decisions are likely to be made programmatically by EHRs and other certified health IT noting that the actors would be constrained by their technology.

Response. We appreciate the comments. We agree on the importance of having the option of implementing the exception as a part of an organizational policy. We explained (89 FR 63634) that 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 have finalized subparagraph (a)(3) of the *threshold* condition as proposed (89 FR 63804). We refer readers to our discussion of what an organizational policy needs to specify, which also notes that a policy

need not be particularized to individual patients in order to be consistent with subparagraph (a)(3)(i). Furthermore, we discussed in the HTI-2 Proposed Rule that we recognize there is currently significant variability in health IT products' capabilities to segment data and thus we finalized in this final rule modifications to 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 the Protecting Care Access Exception (§ 171.206) from the EHI for which this exception is not satisfied.

iii. Reproductive Health Care Definition

In the HTI-2 Proposed Rule, we proposed that the exception would rely on the "reproductive health care" definition in 45 CFR 160.103 and therefore proposed to add to § 171.102 the following: "Reproductive health care is defined as it is in 45 CFR 160.103" (89 FR 63633). We referred readers to 45 CFR 160.103 or 89 FR 32976 for that definition, which became effective for purposes of the HIPAA Privacy Rule on June 25, 2024. (89 FR 63633).⁵² We also referred 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 (89 FR 63633).

Comments. Several commenters supported use of the substance of the 45 CFR 160.103 definition but recommended that we separately adopt the same definition for purposes of the Protecting Care Access Exception (§ 171.206), instead of cross-referencing the definition as proposed. One commenter stated that separate adoption of the same definition would improve certainty for actors. A number of commenters expressing support for adopting the definition asked that we clarify specific types of services that fall within the "reproductive health care" definition. A few comments expressing opposition to the exception also noted that the 45 CFR 160.103 definition, on

⁵² The addition of the "reproductive health care" definition to 45 CFR 160.103 was 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 the HTI-2 Proposed Rule was issued and remained available there at the time this final rule was issued. (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>.) The printed annual edition of Title 45 is revised as of October 1 of each year.

which we proposed the exception would rely, was too expansive and would encompass procedures that the commenters did not consider reproductive health care. Several commenters expressing support for the exception stated the 45 CFR 160.103 definition is appropriately broad or enables the exception to address their information blocking concerns. A few commenters asked or recommended that we clarify whether the definition of reproductive health care encompasses care that renders a person incapable of becoming pregnant, or that affects the health of individuals already incapable of becoming pregnant in matters relating to their reproductive system and to its functions and processes. Some commenters asked that we add language that outlines that any actor who, in good faith, adopts an expansive interpretation of reproductive health care be covered by the Protecting Care Access Exception.

Response. Instead of adopting the same definition by cross-reference to 45 CFR 160.103, as shown in draft regulatory text in the HTI-2 Proposed Rule (89 FR 63802), we are finalizing in § 171.102 the substance of the definition of “reproductive health care” that is in 45 CFR 160.103. By separately codifying a substantively identical definition, we are adopting the same definition we proposed to apply for purposes of the Protecting Care Access Exception but severing reliance on the text of 45 CFR 160.103.

As finalized, the “reproductive health care” definition at § 171.102 mirrors the 45 CFR 160.103 definition of “reproductive health care.” Readers may find it helpful to review the non-exhaustive list of examples that fit within the definition provided at 89 FR 33006 of the 2024 HIPAA Privacy Rule’s preamble discussion of the “reproductive health care” definition (89 FR 63633). We further note that in order to determine whether care meets the “reproductive health care” definition for purposes of applying the Protecting Care Access Exception it is not necessary to assess whether the care was appropriate. A health care professional’s or organizational health care provider’s obligations to provide clinically appropriate care according to applicable standards of care is addressed by laws separate and operating independently from 45 CFR part 171.

c. Patient Protection Condition

We explained (89 FR 63635) that the *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) or has any health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated. The HTI-2 Proposed Rule preamble inadvertently included (at 89 FR 63509 and 89 FR 63635) the words “particular demographic characteristics or” preceding “health condition(s) or history.” The words “particular demographic characteristics or” did not appear in the proposed text of 45 CFR 171.206(b)(1)(iii) (89 FR 63804) and would, we believe, be superfluous considering the proposed wording for 45 CFR 171.206(b)(1)(iii).

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:

- not prohibited by Federal law and lawful under the law of the jurisdiction in which it was provided; or
- 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.

Where care is not prohibited by Federal law and is 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).

We noted (89 FR 63635) that 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 proposed 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 (which we proposed in 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.⁵³

We clarified (89 FR 63636) 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 proposed 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 there may be times when information about a parent’s

⁵³ We stated (89 FR 63635) that 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, we noted that the proposed Protecting Care Access 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.

reproductive health care is included in the EHI of a child. (For example, a child's parent is often identified in or identifiable through the child's EHI.)

We noted that the *patient protection* condition, and generally the Protecting Care Access Exception, are not intended to permit any actor to avoid legal consequences resulting from malpractice or their own wrongdoing. The 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.⁵⁴ 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 also considered, and proposed in the alternative (89 FR 63636), 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.

We stated that 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 solicited comments on the proposed *patient protection* condition, and the Protecting Care Access Exception generally, including whether commenters would recommend we add to the Protecting Care Access Exception any or all of the potential additional limits on applicability of the proposed Protecting Care Access Exception (§ 171.206) that we proposed in the alternative.

Any actor(s) wishing to engage in any applicable practice(s) and avail themselves of the certainty offered by the Protecting Care Access Exception (§ 171.206) that such practice(s) will not be considered "information blocking" as defined in § 171.103 will need to remember that to be covered by the exception a practice meeting either (or both) of the *patient protection* (§ 171.206(b)) and *care access* (§ 171.206(c)) condition(s) of the exception must also satisfy the *threshold* condition (§ 171.206(a)) or *care access* condition. Where an actor's practice satisfies the *threshold* condition's implementation requirement ((§ 171.206(a)(3)) by being implemented consistent with an organizational policy meeting subparagraph (i) of the requirement, the actor's crafting and documentation of their policy would

present an efficient opportunity to address how, when, and by whom patients would be made aware of the actor's belief that risk(s) of potential exposure of the patient to legal action could arise from a particular access, exchange, or use of EHI and provided an opportunity to explicitly request or direct that the sharing occur despite such risk(s) to the patient of potential exposure to (§ 171.206(e)) legal action.

Comments. A few commenters asked ASTP/ONC to carefully consider the impact on a minor patient's ability to obtain reproductive health care if one or more of the alternate proposals were adopted as conditions to the Protecting Care Access Exception to prohibit actors from violating 45 CFR 164.524 with respect to individual access rights as a condition of the Protecting Care Access Exception. One commenter noted that section 164.524's requirements with respect to minor health information and personal representatives are exceedingly complex under section 164.524's access requirements and the legal standards in section 164.502(g) for personal representatives with respect to minor and parental access and control rights as they relate to underlying (and changing) state minor consent to treatment laws for reproductive health care. With this in mind, the commenter suggested that reasonable minds can differ regarding who should be treated as the "individual" under 45 CFR 164.524. Further, given the special considerations involved with reproductive health care, the commenter suggested a delay in imposing such a prohibition that could negatively affect minor patients and provider decisions relating to such care for minor patients.

Response. We thank the commenter for their feedback. Having considered all of the comments received, we have finalized the Protecting Care Access Exception as proposed. We have not attempted to infer what prohibition the commenter above may be referencing because any prohibition on sharing of EHI (of a minor or other person) would be beyond the scope of the Protecting Care Access Exception. All information blocking exceptions are voluntary. Moreover, as we noted in the HTI-2 Proposed Rule, even where an actor might choose to 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, separately, 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

⁵⁴ For purposes of the information blocking regulations, "permissible purpose" is defined in 45 CFR 171.102.

permissible purposes (89 FR 63636). Any changes to State or Tribal law that would affect if or when a non-emancipated minor can consent to or otherwise lawfully obtain any type of health care, including but not limited to reproductive health care, is beyond the scope of this final rule. Any changes or clarifications to which person(s) a HIPAA covered entity is required by 45 CFR 160.502(g) to recognize as the personal representative of an individual in what circumstances for purposes of 45 CFR 164.524, or how any paragraph of 45 CFR 164.524 applies to requests for access to an individual's PHI that may be made in any specific circumstances, is beyond the scope of this final rule. Any interpretation of such provisions of the HIPAA Privacy Rule is also outside the scope of this final rule because we did not adopt any of the HTI-2 Proposed Rule alternative proposals that would have limited the applicability of the Protecting Care Access Exception to actors' practices that fully complied with 45 CFR 164.524 in individual access scenarios to which 45 CFR 164.524 would also apply. For purposes of the Protecting Care Access Exception, an actor's practice that meets the § 171.206(a) *threshold* condition and at least one of the other conditions (§ 171.206(b) *patient protection* or § 171.206(c) *care access*) will satisfy the exception. We have finalized, as proposed, in § 171.206(b)(3) what "patient" means for purposes of § 171.206(b)(1) and (b)(2), including the § 171.206(b)(2) specification that to meet the condition an actor's practice must be subject to nullification by an explicit request or directive from the patient.

Comments. A commenter noted that a patient's ability to direct disclosure should be informed, and actors should not be penalized for seeking to ensure that patients have the relevant information available in considering whether to direct disclosure. The commenter generally supported the provisions of the HTI-2 Proposed Rule that permit actors to delay disclosure to provide 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 action and general information about privacy laws or other relevant laws that the actor believes may be relevant. The commenter suggested that the actor's permission to share such information with patients fits more logically with the patient nullification rights and should be situated in that condition.

Response. We thank the commenter for their support. We believe this comment pertains to our second proposed 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 (89 FR 63637). We have finalized the Protecting Care Access Exception as proposed and have not finalized any of our proposed alternatives to include in the *care access* condition (§ 171.206(c)) or any other conditions. We may consider further refining the exception's conditions in future rulemaking based on experience in the field with the exception as finalized in this final rule or on changes in the legal landscape or market conditions.

Comment. One commenter appreciated the reference in the patient protection condition to EHI that shows or would carry a substantial risk of supporting an inference that the patient has health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated as well as the references to having obtained or inquired about or expressed an interest in receiving reproductive health care.

Response. We appreciate the comment. We believe that addressing actors' uncertainty specific to information blocking by finalizing the Protecting Care Access Exception will 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. We noted this belief in proposing this new exception (89 FR 63630). By addressing an information blocking actor's concern about potential exposure to legal action flowing from an access, exchange, or use of EHI related to reproductive health care, the exception addresses the risk that actors such as health care providers may be unable to provide care that will best meet the patient's needs (89 FR 63631), among other risks we describe in the HTI-2 preamble (89 FR 63630).

Comments. We received several comments requesting or recommending

that we clarify or reaffirm what "natural person" means when used in defining "individual" or "patient" for purposes of the information blocking regulations. We received several comments asking that we clarify what "patient" means for purposes of this exception. We received one comment stating we should use the same "patient" as the HIPAA Privacy Rule. A couple of commenters noted that the definition of "person" under the information blocking regulations cross-referenced the definition of person in 45 CFR 160.103, indicated the clarification of "natural person" in that definition addressed their concerns about what that means and requested we provide an explanation so that it is clear to all actors.

Response. The term "individual" is not used in the text of the Protecting Care Access Exception (§ 171.206). However, references to "individual" in the preamble discussions of this exception in discussing the HIPAA Privacy Rule or individuals' privacy interests should be understood to mean what it means in 45 CFR parts 160 and 164. Where we are discussing the operation of the Privacy Exception, the term "individual" should be understood to have the meaning it is given, for purposes of the Privacy Exception, in § 171.202(a)(2). We refer readers to the section of this final rule preamble where we discuss what "individual" means in context of the Privacy Exception, § 171.202.

Second, the meaning of "patient" for purposes of the finalized Protecting Care Access Exception is specified in § 171.206(b)(3) and explained both in the HTI-2 Proposed Rule preamble and the summary of that proposal (above) in this final rule. It relies on the term "natural person" which, in context of the information blocking regulations, means "a human being who is born alive." We did not propose changes to the definition of "person" in § 171.102, which cross-references the definition of "person" in 45 CFR 160.103.

d. Care Access Condition

We stated (89 FR 63636) that the proposed *care access* condition would apply as specified in paragraph (c) of § 171.206. We clarified that the condition could be met by practices an actor implements to reduce the risk of potential exposure to legal action for persons who provide reproductive health care or are otherwise involved in facilitating reproductive health care that is lawful under the circumstances in which it is provided. We stated (89 FR 63636) that 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. We stated (89 FR 63636) that 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. We stated that 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 in the HTI–2 Proposed Rule (89 FR 63635).

To satisfy the *care access* condition in paragraph (c) of § 171.206, 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.⁵⁵

We proposed this requirement to make the exception inapplicable to other EHI that actors will often have that applicable law would also permit them to make available for permissible purposes. Such EHI to which these exceptions might not apply could include, we noted (89 FR 63637), 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

⁵⁵ We stated that 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” is 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, we noted that the proposed Protecting Care Access 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.

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 recognized 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 used “manner requested” and “alternative manner” in a sense consistent with paragraphs (a) and (b), respectively, of the Manner Exception as currently codified in § 171.301.)

We proposed 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 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 45 CFR part 171 from potentially compelling an actor to provide access, exchange, or use of EHI in a manner 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.

We stated that 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 the HTI–2 Proposed Rule (89 FR 63635), of how we would interpret “lawful under the circumstances” in which care was

provided in context of the proposed § 171.206.)

We stated (89 FR 63637) the Protecting Care Access 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. We explained that 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 (89 FR 63637). We further explained that it would 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 (89 FR 63637). Patients and their attorneys should have easy access to necessary information for considering, filing, or maintaining or pursuing such claims or complaints.

We noted (89 FR 63637) that 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 proposed as the first of several (non-exclusive) alternatives, to include in the *care access* condition (§ 171.206(c)) an additional explicit restriction of the condition to practices that do not violate 45 CFR 164.524. We stated that we might finalize this additional requirement even if we did not finalize any of the other additional requirements that we proposed to potentially apply to the Protecting Care Access Exception as a whole or to the proposed *patient protection* condition (§ 171.206(b)).

The first requirement we proposed 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 the 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 welcomed comment on this first additional potential limitation on the applicability of the proposed exception.

We proposed 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, we stated that 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 an individual's PHI in an EHR within the time period required under § 164.524. We noted (89 FR 63638) that 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, we stated that 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 considered the second proposed additional requirement for § 171.206. We noted that 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.

We stated that 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. We noted that 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. We also noted that 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 reiterated that information blocking exceptions are voluntary.

We reiterated 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 was true of the exceptions codified in subparts B, C, and D of 45 CFR part 171 as of the date of publication of the HTI-2 Proposed Rule and would also be true of the new exceptions proposed in the HTI-2 Proposed Rule in the event any of them are finalized.)

We noted that the additional requirement(s) we considered would seek to further 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 sought comment on those alternative proposals (89 FR 63638).

Comments. Several commenters expressed support for the *care access* condition and recommended finalizing the condition as proposed. These commenters stated that the condition was appropriately structured and necessary to provide protections for all individuals who may be involved in providing or facilitating reproductive health care.

Response. We appreciate the comments on this condition. This condition is intended to ensure that the Protecting Care Access Exception will address actors' concerns about potentially implicating the information blocking definition from their consideration of whether they wish to engage in practices consistent with the exception's conditions in order to reduce potential exposure to legal action (as defined in § 171.206(e), as finalized) for individuals involved in providing or facilitating reproductive health care under circumstances in which such care is lawful. Having reviewed and considered all comments received on the proposed Protecting Care Access Exception, we have finalized the *care access* condition (§ 171.206(c)) as proposed.

Comments. A commenter asked that we indicate whether facilitating care included various people engaged in various activities that may make it possible or easier for a patient to seek or obtain care: friends, family members, or other persons helping the patient find and get to a location where reproductive health care is available or was obtained; accompanying a patient to obtain care; helping a patient return home or providing support to a patient recovering after obtaining lawful reproductive health care. One commenter asked whether persons with legal authority to make health care decisions on behalf of patients, and who consent to care on behalf of patients who cannot consent due to the patient's incapacity, are considered "persons

who facilitate access to" reproductive health care for purposes of the Protecting Care Access exception.

Response. We reiterate that "facilitating reproductive health care that is lawful under the circumstances in which such health care is provided" (§ 171.206(c)) includes conduct that: facilitates a patient seeking or obtaining such care; facilitates a provider's provision of such care; or both. Each of the examples described in the paragraph immediately above would, therefore, be included. However, this is not an exhaustive catalog of all of the actions, activities, or ways in which a person might lawfully facilitate another's seeking, obtaining, or providing lawful reproductive health care. We do not believe it is necessary to catalog all of the various activities or scenarios in which persons other than those involved in providing health care make it easier or possible for patients to seek or obtain reproductive health care that is lawful under the circumstances in which it is furnished. Moreover, we decline to provide or discuss in detail any sampling of examples of conduct to which § 171.206(c) when a person is facilitating a patient's seeking or obtaining lawful reproductive health care to avoid creating a risk that such a discussion could be misconstrued as limiting the actions or activities (or scenarios within which such actions or activities) would, for purposes of paragraph (a)(1)(i) or paragraph (c) of § 171.206, qualify as facilitating reproductive health care.

Comments. One commenter, commenting on the alternative proposal specific to delaying a response to a right of access request, stated that the recognition of a potential delay in fulfilling EHI requests due to any protections afforded to information about reproductive health care is an important step in implementing information blocking and HIPAA privacy regulations. The commenter recommended finalizing this proposal as written. One commenter opposed the alternative proposals that would tie the Protecting Care Access Exception to the HIPAA right of access, stating that the proposals are unnecessary and citing HIPAA's enforcement processes. Another commenter noted that a patient's ability to direct disclosure should be informed and actors should be permitted to delay disclosure to provide in a non-discriminatory manner honest information 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, or use of EHI. This comment described the alternative proposal in

terms of permission to share information with patients and suggested this would fit more logically with the patient nullification provision.

Response. We appreciate the comments on the alternative proposal specific to individual right of access requests for access, exchange, or use of EHI. Having reviewed and considered all comments received on the Protecting Care Access Exception, we have decided not to adopt this alternative proposal. We have finalized the *care access* condition (§ 171.206(c)) as proposed (89 FR 63804).

In light of comments asking for guidance on this and other provisions within the information blocking regulations (45 CFR part 171), it may be helpful to clarify that the Protecting Care Access Exception (§ 171.206), as proposed and as finalized, applies under its codified conditions to a wide variety of practices likely to interfere with access, exchange, or use of EHI. Such practices would include, but are not limited to, an actor delaying fulfillment of a patient's request for access to their own EHI or to direct their EHI to a third party for the time needed to provide to the patient, in a non-discriminatory manner, honest information that is relevant to the actor's belief that a risk of potential exposure to legal action could be created by a particular access, exchange, or use of EHI the patient has requested, directed, or authorized. While it might be ideal for an actor to have communicated such information to a patient in advance of the patient directing or authorizing any specific access, exchange, or use of EHI, we recognize that this may not always be feasible. Therefore, the actor may need some time upon receipt of request to convey information relevant to a belief that the actor holds in good faith at that time. In this regard, we want to make clear that similar to our guidance in the ONC Cures Act Final Rule (85 FR 25642), it would not be an interference to provide a patient with information that is relevant to the actor's belief that a risk of potential exposure to legal action could be created by a particular access, exchange, or use of EHI the patient has requested, directed, or authorized. However, as we described such an approach in the alternative proposal and here, the information provided must be: (1) relevant to the actor's belief that a risk of potential exposure to legal action could be created by a particular access, exchange, or use of EHI the patient has requested, directed, or authorized; (2) honest (unbiased and based on a good faith

belief); and (3) in a nondiscriminatory manner (treat all patients the same).

We remind actors that, although we have not adopted the alternative proposal to limit the Protecting Care Access Exception's coverage of delays to individual access to such delays that are shorter than the maximum timeframes allowed under 45 CFR 164.524, all actors who are also HIPAA covered entities or business associates remain responsible for complying with the HIPAA Privacy Rule. We reiterate that ASTP/ONC partners closely with OCR to maintain alignment across the regulations issued pursuant to both HIPAA and the information blocking statute (PHSA section 3022), and also that these are *separate* regulations issued under independent statutory authorities. 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* exception(s) to the § 171.103 definition of "information blocking" with respect to some or all of the PHI they may have for any given individual (as both "protected health information" and "individual" are defined in 45 CFR 160.103).

e. Presumption Provision and Definition of "Legal Action"

i. Presumption Provision

For purposes of determining whether an actor's practice meets § 171.206(b)(1)(i) or § 171.206(c), we proposed (89 FR 63638) in § 171.206(d) to state 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. This presumption proposed in § 171.206(d) is similar to the presumption in 45 CFR 164.502(a)(5)(iii)(C) of 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 Protecting Care Access Exception (§ 171.206) is intended to operate.

First, the Protecting Care Access Exception (§ 171.206) was proposed to be voluntary (89 FR 63638). As proposed and as finalized, it is designed and intended to offer certainty that practices that meet the exception's conditions will not be considered "information blocking." Nothing in § 171.206, as proposed or as finalized, 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 Protecting Care Access Exception (§ 171.206) was proposed based on statutory authority found in section 3022 of the PHSA to identify reasonable and necessary activities that do not constitute information blocking for purposes of the PHSA section 3022 definition of the term (89 FR 63638). We did 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 (89 FR 63638 and 63639). Thus, we noted (89 FR 63639), 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 section 3022. (We noted at 89 FR 63639 that the exception would not be relevant where an actor is also a HIPAA covered entity or business associate that 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, we stated (at 89 FR 63639) that a policy goal of the 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 proposed 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 (89 FR 63639).

We stated that, as noted elsewhere, an actor's practice satisfying the new Protecting Care Access Exception would mean the practice will not be considered information blocking (89 FR 63639). 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 section 3022 for an actor determined by the HHS OIG to have committed information blocking. As we noted in proposing the new § 171.206 Protecting Care Access Exception (89 FR 63639), because the 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 stated that we believe it is important to ensure that concerns 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 (89 FR 63639).⁵⁶

The proposed § 171.206(d) presumption provision was *not* tied to a 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 (89 FR 63639). Doing so might have made the proposed Protecting Care Access Exception (§ 171.206) more difficult for actors to use and therefore discourage actors from using it (89 FR 63639). We noted in proposing the provision our concern that this difficulty could discourage use of the exception particularly by those actors—such as small and safety net health care

⁵⁶ 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 exceptions work in concert with the HIPAA Rules and other privacy laws to support health information privacy.

providers or non-profit health information networks who serve them—who may have limited ability to divert resources to these types of legal analyses (89 FR 63639). For example, this might arise in circumstances where the 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 be for a purpose other than law enforcement (89 FR 63639).

At 89 FR 63639, we proposed 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 welcomed comments on this alternative proposal.

Comments. A few comments stated that ASTP/ONC should adopt the § 171.206(d) presumption provision as proposed. One commenter stated that ASTP/ONC did not need to adopt the alternative provision to parallel the HIPAA Privacy Rule because the proposed exception is voluntary, and the information blocking rules do not preempt state law. This commenter stated that including the factual basis provision would unnecessarily preclude actors from protecting health information.

Response. We appreciate the comments on the proposed presumption provision. Having reviewed and considered all comments received on the proposed Protecting Care Access Exception, and for the reasons explained above, we have not adopted the alternative proposal to parallel the provision in 45 CFR 164.502(a)(5)(iii)(C)(2). We have finalized the § 171.206(d) presumption provision as proposed (89 FR 63804).

Comment. One comment stated that applying a clear and convincing evidence standard across the board to the Protecting Care Access exception's *threshold* condition, *patient protection* condition, and *care access* condition would be preferable to the alternative we proposed to 171.206(d) noting that the clear and convincing standard is a well-established legal standard.

Response. We did not present or solicit comment on such an alternative in the HTI–2 Proposed Rule. We have finalized 171.206(d) as proposed (89 FR 63804). As we noted in the HTI–2

Proposed Rule, we believe it would be more difficult for actors to use the Protecting Care Access Exception (§ 171.206) if the presumption only applied if the requestor supplied the information demonstrating a substantial factual basis that the reproductive health care was not lawful under the specific circumstances. We believe requiring clear and convincing evidence that care the actor did not provide was unlawful would severely limit the presumption's ability to support efficient application of the exception. Although clear and convincing evidence is a well-established legal standard, it is unclear whether small actors with limited resources, such as small and safety net health care providers, would be able to apply the type of legal analysis that would be required for them to accurately meet the Protecting Care Access Exception's conditions if it used a clear and convincing evidence standard.

Comments. One comment stated that it should not be presumed whether an abortion is lawful in any particular circumstance. This comment stated that this type of information may be sought in criminal, civil, and administrative investigations in order to determine whether the procedure was lawful. One commenter asked ASTP/ONC to clarify, potentially in conjunction with OCR, that “lawfulness” for purposes of the proposed exception should be assessed in the jurisdiction where the provider is located.

Response. The § 171.206(d) presumption provision applies “for purposes of determining whether an actor's practice meets paragraph (b)(1)(i) or (c) of” § 171.206. We remind actors and other readers that, as we noted in the HTI–2 Proposed Rule (89 FR 63639), 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 section 3022 for an actor determined by the HHS OIG to have committed information blocking. We emphasize that the 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, as we noted in proposing the exception (89 FR 63632).

Comment. One comment asked that ASTP/ONC remove the presumption of lawfulness to allow for a broader interpretation of the rule's language.

This commenter stated that lawfulness of care should not be a priority for providers whose jobs are to ensure access to health care and also noted the difficulty for patients and providers to track what and where health care may be “lawful.”

Response. We appreciate the opportunity to clarify that the § 171.206(d) *presumption* provision is designed to enable any § 171.102 actor (including any health care provider) to confidently use the exception when they did not provide the reproductive health care indicated in the EHI, or (where the *patient protection* condition applies) may not be certain what care, or whether care, may have occurred for any health condition(s) or history for which reproductive health care is often sought, obtained, or medically indicated. Where the care in question was not provided by the actor, the presumption ensures that actors need not interrogate patients, or investigate patients' EHI received from other actors, to compare available details of the patient's health and care against the often complex and nuanced details of applicable laws just because the actor wants to engage in a practice likely to interfere with access, exchange, or use of EHI with confidence that (under the conditions of the Protecting Care Access Exception) the practice will not constitute “information blocking.” Similarly, the presumption ensures that an actor can confidently use the Protecting Care Access Exception without tracking laws under which they do not operate but under which a patient may have received care from someone other than the actor.

We also reiterate that all information blocking exceptions are voluntary. The Protecting Care Access Exception does not create an affirmative obligation under the information blocking regulations for any actor to engage in any practice the exception would cover.

ii. Definition of “legal action”

We proposed in § 171.206(e) (89 FR 63804) to define “legal action” for purposes of the Protecting Care Access Exception to 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 (89 FR 63639). We emphasized 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 (89 FR 63639).

Comments. Several commenters expressed support for our proposed definition of “legal action” and noted that it covered expected concerns and risks.

Response. We appreciate the comments. We proposed the definition of “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) (89 FR 63633). Having considered all comments received in response to the proposed exception, we have finalized the “legal action” definition in § 171.206(e) as proposed (89 FR 63804).

Comment. One commenter supported the definition of “legal action” but asked that it be expanded to be parallel to HIPAA which covers uses of protected health information to identify any person for certain investigations or proceedings, noting that mere efforts to identify individuals, shy of a formal investigation or proceeding, can chill health care access and patient trust to the same degree as formal investigations and proceedings.

Response. We appreciate the comment. We did not present an expansion of the definition of “legal action” as an alternative proposal or solicit comment on such an alternative. We believe that because the Protecting Care Access Exception (§ 171.206) as proposed and finalized functions differently from 45 CFR 164.502(a)(5)(iii), the exception as a whole is sufficiently broad. Specifically, § 171.206 is not limited to uses or disclosures of EHI for specific purposes but instead relies on a good faith belief consistent with § 171.206(a)(1)(i) that specific practices likely to interfere with applicable access, exchange, or use of specific EHI could reduce that risk. Such practices could include an actor not sharing relevant EHI with entities, such as entities not regulated under the HIPAA Privacy Rule, that are known or suspected of making EHI available to data brokers or whom the actor believes in good faith would otherwise potentially expose the EHI to identification activities that could lead to a “legal action” as defined in § 171.206(e).

Comments. One commenter stated that the language on protection against potential legal action is vague and potentially overly broad, noting that under the proposed language, custody disputes could be considered legal action. The commenter stated that this could create unnecessary legal liability and a burden on stakeholders.

Response. The § 171.206(e) “legal action” definition establishes what the term “legal action” means when used in the § 171.206(a) *threshold* condition, the § 171.206(b) *patient protection* condition, and the § 171.206(c) *care access* condition. The definition is intended to encompass a broad array of criminal, civil, and administrative investigations, actions, and proceedings, but only if those investigations, actions, and proceedings are based on the mere fact that a person sought, obtained, provided, or facilitated reproductive health care.

The Protecting Care Access Exception, like all information blocking exceptions, is voluntary. It is not intended to create an affirmative obligation for an actor to evaluate whether a risk of potentially exposing anyone to legal action from any particular EHI access, exchange, or use scenario(s) might occur. It is also not intended to override an actor’s obligation to comply with other valid, applicable law compelling the actor to make the EHI available for permissible purposes.⁵⁷ An example of this that we used in the HTI–2 Proposed Rule was that an 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 therefore do not expect the definition of “legal action” in § 171.206(e), or this exception as a whole, to affect the ability of a party to a custody dispute to obtain relevant evidence in the normal course of that legal proceeding.

Comments. A few commenters sought application of the exception to any instance in which the fact of seeking or obtaining reproductive health care increases the risk of legal action, stating that some jurisdictions undermine care access by using the fact that a person obtained or sought reproductive health care as evidence of other crimes (*e.g.*, substance use during pregnancy).

⁵⁷ For purposes of the information blocking regulations, “permissible purpose” is defined in 45 CFR 171.102.

Response. The exception was proposed to address actors’ concerns about potential information blocking implications of their limiting EHI sharing when they believe such interference with sharing could reduce a risk of legal action based on the mere fact that any person sought, obtained, provided, or facilitated reproductive health care or (where the *patient protection* condition applies) may have sought or needed reproductive health care. We do not believe explicit expansion of the exception to include legal action(s) based on conduct of a pregnant person *other than* the mere act of seeking, obtaining, providing, or facilitating reproductive health care would have the effect of ensuring that health care providers are not compelled to disclose information for use in such actions. This is because, as we have repeatedly reminded actors throughout this final rule, the exception is not intended to override other laws with which the actor must comply. Such an expansion is also beyond the scope of our proposal for this exception, including all of the alternatives on which we solicited comments in the HTI–2 Proposed Rule.

IV. Severability

As we explained in the HTI–2 Proposed Rule (89 FR 63511), it was and continues to be our intent that if any provision of the proposed rule were, if or when finalized, held to be invalid or unenforceable—facially or as applied to any person, plaintiff, or circumstance—or stayed pending further judicial or agency action, such provision shall be severable from other provisions finalized, and from rules and regulations otherwise in effect, and not affect the remainder of provisions finalized. It was and continues to be 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.

This final rule finalizes provisions that are intended to and will operate independently of each other and of provisions finalized in previous rules, even if multiple of them may 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, or other regulatory

provision). Where a provision that is stayed or held invalid or unenforceable (as described in the preceding paragraph) is included in a subparagraph, paragraph, or section within 45 CFR part 171, we intend that other provisions of such subparagraph(s), paragraph(s), or section(s) that operate independently of said provision would remain in effect.

For example, if an information blocking exception, sub-exception, or condition of any 45 CFR part 171 exception were stayed or held invalid or unenforceable, the other information blocking exceptions, sub-exceptions, or conditions to an exception would continue to be available for actors. For instance, an actor's practice meets the § 171.202 Privacy Exception by satisfying all the requirements of at least one of multiple sub-exceptions (paragraph (b), (c), (d), or (e)) that are not dependent on one another. If any one of the sub-exceptions were stayed or held invalid or unenforceable, the other sub-exceptions would remain available. When an actor's practice can meet an exception by satisfying all the requirements of a combination of conditions that includes any condition picked from an array of multiple conditions that are not dependent on one another, the exception would remain available and continue to apply to any practice meeting any of the remaining conditions. The Infeasibility Exception (§ 171.204) is an example of an exception that can be satisfied by meeting one always-required condition (§ 171.204(b) *responding to requests*) plus any one of the independent conditions in § 171.204(a). It is our intent that even if one of the conditions in § 171.204(a) were stayed or held to be utterly invalid or unenforceable, the § 171.204 Infeasibility Exception would remain available, and all of the other conditions in § 171.204(a) would remain in force and available to actors.

The Infeasibility Exception's *segmentation* condition (§ 171.204(a)(2)) is an example of a paragraph within part 171 that includes provisions dependent on provisions in another section or paragraph. Specifically, § 171.204(a)(2) *segmentation* condition includes provisions that are applicable where an actor has chosen to withhold some EHI consistent with any of §§ 171.201, 171.202, or 171.206. These specific provisions are, therefore, dependent on the cross-referenced sections, while other provisions in § 171.204(a)(2) are not. It is our intent that if any provision in any paragraph in § 171.201 or § 171.202 or § 171.206 were held to be invalid or unenforceable—facially or as applied to any person, plaintiff, or

circumstance—or stayed pending further judicial or agency action, *only* the operation of the specific provision of § 171.204(a)(2) that specifically references such other section would be affected. All other provisions in § 171.204(a)(2) would remain in effect, including cross-references to other sections in 45 CFR part 171 and the § 171.204(a)(i) provision for EHI that other applicable law does not permit to be made available. For example, as noted in this rule's preamble discussion of the Protecting Care Access Exception (§ 171.206), it is our intent that if any provision of § 171.206, as finalized in this final rule, were 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 § 171.206 that do not rely upon it and from any other provision codified in 45 CFR part 171 that does not explicitly rely upon § 171.206, even if such provisions were to be established or modified through this same final rule.⁵⁸ Thus, if § 171.206 were held to be utterly invalid, unenforceable, or stayed, it is our intent that the provisions in § 171.204(a)(2) that reference and rely on §§ 171.201 and 171.202 rather than § 171.206 should be construed as fully severable from the reference to § 171.206 and retain their full applicability and effect.

Moreover, we reiterate that it is our intent that unless any provision in any section or paragraph in 45 CFR part 171 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. For example, if the Protecting Care Access Exception (§ 171.206) were held to be invalid and unenforceable with respect to its application to a specific item or service that fits the § 171.102 definition of reproductive health care, it should be upheld with respect to other items and services that also fit this definition. Similarly, if either the § 171.206(b) *patient protection* condition or § 171.206(c) *care access* condition were held to be invalid as applied to specific reproductive health care item(s) or service(s) with respect to particular person(s) or in particular circumstance(s), that condition should

⁵⁸ The reference to § 171.206 in § 171.204(a)(2) is currently the only example of a provision in any section of 45 part 171 that relies on § 171.206 in any way.

be upheld with respect to the seeking, obtaining, provision, or facilitation of such item(s) or service(s) by other persons not similarly situated or in other, dissimilar, circumstances.

Even if a paragraph or subparagraph were held to be utterly invalid or unenforceable, it is our intent that the remaining subparagraphs or paragraphs even within the same section of the CFR would remain in effect and be construed to have the maximum effect permitted by law. For example, an actor's practice can satisfy the Protecting Care Access Exception (§ 171.206) by satisfying the *threshold* condition (§ 171.206(a)) and the requirements of at least one of the *patient protection* (§ 171.206(b)) or *care access* (§ 171.206(c)) conditions. If only the *patient protection* condition (paragraph (b)) of the Protecting Care Access Exception (§ 171.206) were held to be utterly invalid or unenforceable as applied to any person or situation, it is our intent that the provision in § 171.204(a)(2)(ii) that references EHI an actor may withhold consistent with § 171.206 be construed to give § 171.204(a)(2)(ii) maximum effect permitted by law where an actor has chosen to withhold EHI consistent with the § 171.206(a) *threshold* condition and § 171.206(c) *care access* condition.

To ensure our intent for severability of provisions is clear in the CFR, we proposed (as explained at 89 FR 63511) the addition to § 170.101 (89 FR 63766), § 171.101 (89 FR 63802), and inclusion in § 172.101 (89 FR 63805), of 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. These proposals are not addressed in this final rule but are among the subjects of the HTI-2 final rule (RIN 0955-AA07), which was recently issued.

V. Waiver of Delay in Effective Date

Under the Administrative Procedure Act (APA) (Pub. L. 79-404, Jun. 11, 1946), 5 U.S.C. 553(d) mandates a 30-day delay in effective date after issuance or publication of a rule. Such a delay is not required, however, for “a substantive rule which grants or recognizes an exemption or relieves a restriction.” 5 U.S.C. 553(d)(1). Moreover, section 553(d)(3) allows that an agency may waive the 30-day delay

in effective date “for good cause found and published with the rule.” *Id.* 553(d)(3).

A delay in the effective date of the finalized provisions of this final rule is not required because this rule recognizes an exemption or relieves a restriction from the information blocking requirements that would otherwise exist in the absence of this final rule. Actors are not under any obligation to alter practices because of this final rule, as the information blocking exceptions generally, and the specific regulations finalized here, are voluntary. In addition, to the extent that a waiver of the delay in effective date would be required, there is good cause to waive the delay in the effective date for this final rule.

Because information blocking exceptions are voluntary, the expansion of the scope of provisions in § 171.202 and § 171.204, as well as the adoption of § 171.206, as finalized in this rule, do not create an obligation for any actor to begin engaging in practices to which the exceptions would apply if the actor does not want to or, if they do want to, on any particular timeframe. Therefore, because these provisions are all voluntary, we do not believe affected persons require additional time to prepare for the effective date of this final rule, to include the 30 days required by 5 U.S.C. 553(d). An actor who does need additional time could simply continue their current practices and would not be acting in contradiction to this rule. Additionally, because an actor conforming their practices to the exceptions, including those finalized in this rule, exempts those practices from the possible consequences of information blocking, this rule satisfies the requirement for an exemption from the effective date delay requirement under 5 U.S.C. 553(d)(1) (a delayed effective date after publication is not required for “a substantive rule which grants or recognizes an exemption or relieves a restriction”). This final rule exempts an actor’s conforming practices from the consequences of information blocking enforcement and does not apply or require any change in practice except to the extent that an actor wishes to undertake a practice conforming to the exceptions, thereby ensuring the actor’s exemption from civil monetary penalties or appropriate disincentives.

As we have repeatedly reminded actors, an actor’s practice that does not meet the conditions of an exception does not automatically constitute information blocking, as the practice must still meet all the elements of the information blocking definition to be

considered information blocking, including that the practice is likely to interfere with the access, exchange, or use of EHI, and that the actor acted with the requisite intent (89 FR 1378 citing 85 FR 25820). Information blocking exceptions are also voluntary; we do not intend that the existence of any exception be construed as creating a mandate for actors to engage in a practice to which the exception would apply. However, information blocking exceptions offer actors certainty that if they choose to engage in certain practices that meet the conditions of applicable exception(s), then they will not be subject to a civil monetary penalty or appropriate disincentive from HHS. Thus, an immediate effective date for the new and revised exceptions will not require any actor to take immediate action, and therefore actors do not require additional time to prepare for the effective date of this final rule.

In addition, an immediate effective date will allow actors to immediately avail themselves of the revised and new exceptions finalized in this rule upon publication of the final rule, alleviating burdens associated with the uncertainty specific to information blocking implications that the provisions finalized in this rule are designed to address. For example, actors, such as health care providers, who withhold EHI related to reproductive health care consistent with the Protecting Care Access Exception will not be subject to civil monetary penalties or appropriate disincentives under the information blocking regulations as of the date of publication of this final rule for engaging in that practice. Thus, an immediate effective date for the Protecting Care Access Exception will remove from health care providers and the other actors on whom they rely for health IT items and services the burden of weighing, for another 30 days, their uncertainty about information blocking civil monetary penalties or appropriate disincentives for withholding patients’ reproductive health care information in applicable circumstances against their belief that sharing the information in those circumstances risks potentially exposing persons to legal action as defined in § 171.206. Regardless of whether we expect, intend, or believe it is likely that HHS would seek to impose a civil monetary penalty or appropriate disincentive on any actor specifically for engaging in conduct to which § 171.206 applies, or within the expanded scope of provisions in § 171.202 or § 171.204 revised by this rule, during a 30 day period of delay between publication and effective date

of this rule, our interactions with actors since the ONC Cures Act Final Rule (85 FR 25642) appeared in the **Federal Register** leads us to expect a majority of actors would be concerned that such enforcement activity would be possible and that some significant portion of them would continue to be burdened by that concern.

In further support of waiving the delayed effective date, the public has also expressed a need to avoid delays in implementing the proposed new Protecting Care Access Exception. As discussed at the end of the Background and Purpose section of “III. Information Blocking Enhancements; *B. Exceptions*; 3. New Protecting Care Access Exception,” commenters on the HTI–2 Proposed Rule specifically stated that the information blocking provisions finalized in this final rule should be effective without procedural delay, noting that such an approach would encourage continued use of electronic methods for sharing health information and ensure that some providers would not feel a need to revert to paper records to protect patients’ privacy.

Because a disclosure—including one that is only permitted (not required) by other applicable law—is a bell that cannot be unrung, we believe it is important to mitigate the risk of actors’ fear of being subject to civil monetary penalties or appropriate disincentives under the information blocking regulations from being the sole reason that they refuse to grant individuals’ requests that their EHI not be shared or make individuals’ reproductive health care information available for an access, exchange, or use that the actor believes in good faith could potentially expose the patient, provider, or facilitator of lawful reproductive health care to legal action (as defined in § 171.206). We are concerned that providers’ uncertainties about their ability to track all laws that might be applied to them may be contributing to what some commenters on the proposed revision to § 171.204(a)(2) described as underuse of the Privacy Exception related to limited segmentation capabilities. An immediate effective date for the Protecting Care Access Exception and the revised Privacy sub-exception for individuals’ requested restrictions, and the clarified and expanded *segmentation* condition of the Infeasibility Exception (§ 171.204(a)(2)), would afford all actors the assurance they need to immediately stop erring on the side of sharing individuals’ EHI contrary to the individual’s request or in situations where § 171.206 would apply. However many disclosures actors might make during a 30-day delay in the

effective date of this rule specifically and solely because of actors' fears of being subject to civil monetary penalties or appropriate disincentives as "information blockers" represent a compromise of patients' privacy and a commensurate, avoidable impediment to restoring patients' trust that their health care provider will be able to maintain their confidence unless another law that applies to the provider compels disclosure of patients' private health information against the provider's and patient's wishes.

Because, as we have explained, actors do not require additional time to prepare for the effective date of this final rule due to the voluntary nature of the information blocking exceptions we have revised and the exception we have finalized, we believe we have satisfied the requirements in 5 U.S.C. 553(d) needed to waive the delay in the effective date of the final rule. Avoiding a delay in effective date of this final rule could also help to more quickly render unnecessary concerned actors' efforts to seek state or local enactments aimed solely at addressing actors' concerns about implicating the information blocking regulations if they do not share reproductive health care information as widely as applicable laws might permit. Thus, an immediate effective date of this rule would enable actors to set aside the burden of these efforts and refocus on other goals, such as developing or implementing improved data segmentation capabilities or other health IT or patient care advancements.

VI. Regulatory Impact Analysis

A. Statement of Need

This final rule is necessary to meet our statutory responsibility under the Cures Act and to advance HHS policy goals to promote information sharing. As discussed in this final rule, the revised Privacy sub-exception "individual's request not to share EHI" (45 CFR 171.202(e)) and new Protecting Care Access Exception (45 CFR 171.206) respond to actors' uncertainty about potentially being subject to civil monetary penalties or appropriate disincentives under the information blocking regulations (45 CFR part 171) if they engage in practices intended to protect patients' privacy, providers' willingness to furnish care that is lawful under the circumstances in which it is furnished, and patients' trust in their providers and the nation's health information infrastructure. The revision to the Infeasibility Exception's *segmentation* condition (§ 171.204(a)(2)) finalized in this rule recognizes the current variability in, and in many cases

lack of, technical capability an actor may have to segment EHI that an actor might wish to withhold under the Protecting Care Access Exception, or on "unreviewable grounds" for denial of individual access under the HIPAA Privacy Rule, from other EHI that the actor could share under applicable law. Thus, revising § 171.204(a)(2) is not only necessary to fully implement § 171.206 but also to ensure actors do not feel compelled—specifically by the information blocking regulations in combination with their inability to unambiguously segment relevant EHI—to disclose EHI in circumstances where the actor might otherwise (and a HIPAA covered entity would be permitted to) deny an individual access to their health information. Such circumstances are identified in 45 CFR 164.524(a)(2) and include those where an inmate obtaining their health information would jeopardize the health, safety, security, custody, or rehabilitation of that inmate or others, or the safety of officers or other persons at the correctional institution or involved in transporting the inmate. The revisions to the Infeasibility Exception's *segmentation* condition broadens its scope of applicability without creating a need for any actor who may already be engaged in practices that were already in conformance with the original scope of § 171.204(a)(2) to change any of their policies, procedures, or processes in order for such practices to remain in conformance with § 171.204(a)(2) as revised.

B. Alternatives Considered

In the HTI-2 Proposed Rule, we noted that we were unable to identify alternatives to our proposals that would appropriately implement our responsibilities under the Cures Act (89 FR 63662). We concluded that our proposals took the necessary steps to fulfill the mandates specified in the Public Health Service Act (PHSA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and the Cures Act, in the least burdensome way. We welcomed comments on our assessment and any alternatives we should have considered.

Comments. We received comments suggesting alternatives to our proposals. Specifically, some commenters suggested that ASTP/ONC require health IT developers of certified health IT enable a user to implement a process to restrict uses or disclosures of data in response to a patient request when such restriction is necessary, citing 88 FR 23822. Another commenter encouraged ASTP/ONC to strengthen ONC Health IT

Certification Program certification criteria for capabilities to allow clinical users to tag and withhold data from exchange. Other commenters suggested the alternative was to not adopt the proposed changes to the Privacy and Infeasibility Exceptions as well as the new Protecting Care Access Exception. These commenters supported the sharing of reproductive health information for clinical care.

Response. We appreciate the commenters' suggestions, but their requests specific to imposing certain requirements on developers of certified health IT, which appear to refer to ASTP/ONC's proposal in the HTI-1 Proposed Rule to adopt a new certification criterion "patient requested restrictions" in § 170.315(d)(14) and which was not finalized in the HTI-1 Final Rule (89 FR 1301), are outside the scope of this rulemaking. We note that we may consider amending relevant ONC Health IT Certification Program or information blocking regulations in future rulemaking in response to changing market conditions. As to the commenters' suggestions that we not adopt our proposals, we decline to do so as such action would be counter to our stated reasons for the revisions to the exceptions and the new Protecting Care Access Exception.

C. Overall Impact

1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis

We have examined the impacts of this final rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (January 18, 2011), Executive Order 14094 entitled "Modernizing Regulatory Review" (April 6, 2023), the Regulatory Flexibility Act (RFA), section 202 of the Unfunded Mandates reform Act of 1995 (March 22, 1995; Pub. L. 104-4), the Small Business Regulatory Enforcement Fairness Act of 1996 (also known as the Congressional Review Act, 5 U.S.C. 801 *et seq.*), 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 amends section 3(f) of Executive Order 12866. 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 OMB’s 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 the Executive order, as specifically authorized in a timely manner by the Administrator of OIRA in each case.

An RIA must be prepared for rules that are significant per section 3(f)(1) (annual effect of \$200 million or more in any 1 year).

OIRA has determined that this final rule is a significant regulatory action under 3(f) of Executive Order 12866, as amended by E.O. 14094. Pursuant to Subtitle E of the Small Business Regulatory Enforcement Fairness Act of 1996 (also known as the Congressional Review Act, 5 U.S.C. 801 *et seq.*), OIRA has also determined that this final rule does not meet the criteria set forth in 5 U.S.C. 804(2).

Although we did not include an assessment of the cost and benefits of the proposed information blocking enhancements in the HTI–2 Proposed Rule, we have included an assessment of the finalized information blocking enhancements in this final rule. We have finalized in this final rule preamble several enhancements with respect to the information blocking provisions in 45 CFR part 171. These include the addition of a definition of “reproductive health care” for the purpose of information blocking regulations. The enhancements also include revising the Privacy and Infeasibility Exceptions and adding a Protecting Care Access Exception in subpart B of 45 CFR part 171.

Costs

We expect ASTP/ONC to incur an annual cost for issuing educational resources related to the finalized information blocking enhancements. We estimate that ASTP/ONC would issue

educational resources each quarter, or at least four times per year. We assume that the resources would be developed by ASTP/ONC staff with the expertise of a GS–15, Step 1 federal employee(s). We calculate the hourly benefits for a federal employee to be equal to one hundred (100) percent of hourly wage. The hourly wage with benefits for a GS–15, Step 1 employee located in Washington, DC is approximately \$157.⁵⁹

We estimate it would take ASTP/ONC staff between 50 and 100 hours to develop resources each quarter, or 200 to 400 hours annually. Therefore, we estimate the annual cost to ASTP/ONC would, on average, range from \$31,400 to \$62,800.

Benefits

We anticipate that the adopted information blocking enhancements will enable actors to determine more easily and with greater certainty whether their practices (acts or omissions) that may or do interfere with access, exchange, or use of EHI (as defined in 45 CFR 171.102) meet the conditions to fall within an information blocking exception. As such, we expect these policies will further improve actors understanding of, and compliance with, the Cures Act information blocking definition. The benefits of the revisions to the Privacy and Infeasibility Exceptions and the new Protecting Care Access Exception are discussed in detail in section III.B (“Exceptions”) of this preamble.

D. Regulatory Flexibility Act

The 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.⁶⁰

In the HTI–2 Proposed Rule we noted that the entities that are likely to be directly affected by the information blocking provisions in this final rule are actors within the meaning of 45 CFR 171.102 (health IT developers of certified health IT, health information networks/health information exchanges,

⁵⁹ Office of Personnel and Management. https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2024/DCB_h.pdf. Accessed December 3, 2024.

⁶⁰ 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.

and health care providers) under the information blocking regulations (89 FR 63765). The revised and new information blocking exceptions, reflecting practices that do not constitute information blocking, will provide flexibilities and relief for actors subject to the information blocking regulations. In the HTI–2 Proposed Rule (89 FR 63765), we referred readers to our information blocking-related proposals (89 FR 63616 through 63643) and welcomed comments on their impacts on small entities.

Comments. We received no comments on our assessment.

Response. The policies in this final rule, as proposed, establish revised exceptions and a new exception to the information blocking definition that provide flexibilities and relief for actors subject to the information blocking regulations. The exceptions exist as a voluntary means for actors to gain assurance that their practice(s) does not constitute information blocking. In addition, the exceptions (reasonable and necessary activities under the statute) take into account the potential burden on small entities to meet them, such as providing actors the ability to make case-by-case determinations versus using established organizational policies under the Privacy Exception (45 CFR 171.202(b)(1)(ii)) and the new Protecting Care Access Exception (45 CFR 171.206(a)(3)(ii)).

We do not believe that this final rule would create a significant impact on a substantial number of small entities, and the Secretary certifies that this final 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 rule that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications.

Comments. We received no comments.

Response. Nothing in this final rule imposes substantial direct compliance costs on state and local governments, preempts state law, or otherwise has federalism implications.

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.

Comments. We received no comments on the application of this law to our proposals finalized in this final rule.

Response. This final rule does not impose unfunded mandates on State, Local, and Tribal governments, or the private sector.

List of Subjects in 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, Public health, Reporting and record keeping requirements, Security.

For the reasons set forth in the preamble, the Department of Health and Human Services amends 45 CFR part 171 as follows:

PART 171—INFORMATION BLOCKING

■ 1. The authority citation for part 171 continues to read as follows:

Authority: 42 U.S.C. 300jj–52; 5 U.S.C. 552.

■ 2. Amend § 171.102 by adding, in alphabetical order, the definition “Reproductive health care” to read as follows:

* * * * *

Reproductive health care means health care, as defined in 45 CFR 160.103, that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes. This definition shall not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate reproductive health care.

* * * * *

■ 3. Amend § 171.202 by revising paragraph (a)(2) and paragraph (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.

* * * * *

(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—

* * * * *

■ 4. Amend § 171.204 by revising paragraph (a)(2) 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 45 CFR 171.201, 171.202, or 171.206 of this part.

■ 5. 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 paragraphs (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 paragraphs (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.

(4) *Another actor's reliance on good faith belief.* For purposes of this section, an actor who is a business associate of, or otherwise maintains EHI on behalf of, another actor may rely on the good faith belief consistent with paragraph (a)(1) of the section and organizational policy or case-by-case determinations consistent with paragraph (a)(3) of this section of the actor on whose behalf relevant EHI is maintained.

(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 paragraph (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.

Xavier Becerra,

Secretary, Department of Health and Human Services.

[FR Doc. 2024–29683 Filed 12–16–24; 8:45 am]

BILLING CODE 4150–45–P