hfma
healthcare financial management association

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

Summary of March 9, 2020 Announcement of Final Rule

On March 9, 2020, the Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS), announced on its website a final rule to implement certain provisions of the 21st Century Cures Act (P.L 114-255). The provisions are concerned with conditions and maintenance of certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program); facilitating access by patients to their electronic health information (e.g., through application programming interfaces); voluntary certification of health IT for use in the care of children; and information blocking. The final rule also makes modifications to the 2015 Edition Health Information Technology certification criteria and to other aspects of the Program, intended to advance interoperability, enhance health IT certification, and reduce burden and costs.

Additional educational materials regarding this rule, including fact sheets and webinar presentations, are available on the ONC website: https://www.healthit.gov/curesrule/.

IMPORTANT: Because this rule has yet to be officially posted for public inspection by the *Federal Register,* it is not an official final rule. As a result, changes to effective dates and substantive policy could be made before the official release.

Table of Contents	Page

I. Introduction and Background

The position of the National Coordinator for health IT was created by Executive Order 13335 on April 27, 2004, and the ONC was established in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act (part of the American Recovery and Reinvestment Act of 2009 (ARRA)) (Pub. L. 111-5). The HITECH Act added Title XXX – Health Information Technology and Quality - to the Public Health Service (PHS) Act and provided the National Coordinator with the authority to establish a voluntary certification program for health IT (the Program). Current certification criteria, organized into eight categories, comprise the 2015 Edition.[1] The Program is intended to assure that systems composed of certified health IT modules meet HHS technological capability, functionality, and security requirements.

The 21st Century Cures Act (Cures Act), signed into law on December 13, 2016, made changes to the PHS Act related to health IT. In this final rule, ONC provides regulations targeting the following areas from Sections 4001 through 4006 of the Cures Act:

- Reduction of regulatory and administrative burden associated with the use of electronic health records (EHRs);
- Voluntary health IT certification under the Program for use in medical specialties and sites of service where technology has not been available or sufficiently integrated (e.g., pediatric care, treatment and prevention of opioid use disorder);
- Conditions and Maintenance of Certification requirements for health IT developers and their certified Health IT Modules;
- Interoperability;
- Information blocking exceptions; and
- Patient access to their electronic health information (EHI).

[1] The categories are care coordination, clinical processes, clinical quality measurement, electronic exchange, health IT design and performance, patient engagement, privacy and security, and public health.

II. Deregulatory Actions

Executive Orders 13771 (January 2017) and 13777 (February 2017) directed all agencies to review their existing regulations to identify deregulatory actions (regulatory repeal) and to make recommendations for simplification of retained regulations. In addition, the Cures Act required the Secretary to develop a strategy and recommendations to reduce the regulatory and administrative burdens associated with the use of EHRs by December 2017. In response, ONC was able to identify 6 deregulatory actions involving the ONC Health IT Certification Program (the Program) that were presented in the proposed rule.

A. Removal of Randomized Surveillance Requirements

ONC proposed that its Authorized Certification Bodies (ONC-ACBs) be permitted but no longer required to conduct random, in-the-field surveillance of certified health IT for continued conformance to certification requirements. Stakeholders had previously stated that the provider burden of random surveillance exceeded the potential benefit and supported reactive surveillance (e.g., in response to complaints) as more logical and economical. Should ONC-ACBs choose to conduct random surveillance, they would continue to employ existing methodology with respect to scope (§170.556(c)(1)), selection method (§170.556(c)(3)), and the number and types of locations.

Most commenters were supportive of the change, though several viewed the proposal as a reduction in ONC's oversight of developers and their modules. Concerns were expressed that EHR users would fail to recognize when a module was noncompliant with certification criteria and/or would not be familiar with the process for reporting noncompliance. ONC responds by reiterating its commitment to robust oversight and emphasizes that any user can readily report suspected noncompliance using ONC's Health IT Feedback Form.[2] ONC finalizes the changed surveillance requirements at §170.556(c) and §170.556(c)(2) as proposed.

ONC estimates aggregate cost savings of between $6.8 and $13.7 million in total for all stakeholders (health IT developers, providers, ONC-ACBs, ONC-ATLs, and ONC) from the removal of the requirement that randomized, in the field surveillance be performed by ONC-ACBs.

B. Removing the 2014 Edition from the Code of Federal Regulations

ONC proposed to remove the 2014 Edition in its entirety from the Code of Federal Regulations (CFR) as of the effective date of the final rule, leaving the 2015 Edition as the sole basis for health IT certification. ONC stated that a single standard would reduce burden for health IT developers, ONC-ACBs, and ONC-Authorized Testing Laboratories (ATLs) while aligning with the CMS Quality Payment Program (QPP) requirement for use of the 2015 Edition, effective for QPP performance year 2019 and subsequent years. While the 2014 Edition's certification

[2] The form is available for completion at https://www.healthit.gov/form/healthit-feedback-form .

criteria (§170.314) and its related standards, terms, and requirements found in multiple other sections of the Program would be removed, public access to attestations about products certified to the 2014 Edition would be maintained in an archive on the Certified Health IT Product List (CHPL).

Commenters were supportive and ONC finalizes the removal of the 2014 Edition's criteria, standards, terms, and requirements as proposed.

C. Removing the ONC-Approved Accreditor from the Program

ONC proposed to remove the ONC-Approved Accreditor (ONC-AA) from the program. ONC would directly provide oversight of the ONC-ACBs rather than indirectly through the ONC-AA. Additionally, ONC-ACBs would be able to obtain their accreditation from multiple entities rather than only through an ONC-AA.[3]

Nearly all commenters supported the proposed elimination of the ONC-AA from the Program. ONC finalizes the elimination through changes at §170.501-§170.506, §170.520, §170.523, and §170.575, as proposed. ONC estimates overall annual cost savings from this regulatory removal to be $4,632.

D. Removal of Certain 2015 Edition Certification Criteria and Standards

1. Removal from the 2015 Base EHR Definition

ONC proposed to remove several certification criteria from the 2015 Edition that also are included currently in the 2015 Base EHR definition: Problem List, Medication List, Medication Allergy List, and Smoking Status. ONC noted that these criteria were no longer needed for CMS' Promoting Interoperability (PI) programs; would be captured in an interoperable form if the United States Core Data for Interoperability (USCDI) standard were adopted into the 2015 Edition as proposed (section IV.B.1 of the rule); and/or were EHR elements essential to patient care that still would be captured in the absence of associated certification requirements.

Problem List (§170.315(a)(6)). Commenters generally were supportive of removal but raised concerns that developer maintenance of this functionality would decrease in the absence of a certification requirement. ONC responds that this functionality is essential to clinical care and that IT users will demand its retention. ONC finalizes the removal of the Problem List criterion from the 2015 Base EHR definition and from the Program.
Medication List (§170.315(a)(7)). Commenter reactions to removal of this criterion were mixed. Concerns included potential impacts on drug costs and on efforts to combat the opioid epidemic. ONC believes that retention of a medication list functionality in EHRs will occur without a related certification criterion because the list is necessary for high quality patient care. ONC

[3] Accreditation could be obtained from any signatory to the Multilateral Recognition Arrangement with the International Accreditation Forum.

further notes that interoperable exchange of medication information would be facilitated by the adoption of the USCDI standard into the 2015 Edition (if finalized). ONC finalizes the removal of the Medication Problem List criterion from the 2015 Base EHR definition and from the Program.

Medication Allergy List (§170.315(a)(8)). Commenter reactions to removal of this criterion were mixed. Supporters noted that allergy information would be captured through the USCDI while opponents feared that developers would no longer be incented to maintain an allergy functionality. ONC concurs that USCDI adoption would foster interoperable exchange of allergy information and states that ONC will be vigilant in monitoring for safety consequences of removing the current criterion. ONC finalizes the removal of the Medication Allergy List criterion from the 2015 Base EHR definition and from the Program.

Smoking Status (§170.315(a)(11)). Commenters were divided on removing this criterion. Supporters observed that smoking status information would be captured through the USCDI while opponents cited the public health importance of smoking status information. ONC responds that the USCDI would ensure interoperable exchange of structured smoking status information while the current criterion does not. ONC also states that the utility and importance of smoking status in clinical care would incent developers to maintain functionality for capturing this information. ONC finalizes the removal of the Smoking Status criterion from the 2015 Base EHR definition and from the Program.

The now removed Smoking Status criterion referred to 8 smoking status SNOMED CT® codes that were required for reporting smoking status.[4] ONC proposed to remove this requirement in response to stakeholder feedback that the codes do not accurately capture all clinically relevant smoking statuses. Commenters were generally supportive; some suggested broadening the information captured to include smokeless tobacco use, secondhand smoke exposure, and e-cigarette (vaping) use. ONC finalizes removal of the eight-code value set (§170.207(h)). Finally, ONC states that changes to support broader data capture are outside the scope of this final rule, but also notes that USCDI references SNOMED CT®, U.S. Edition, as the standard for smoking status information.

2. Removal from the 2015 Edition

ONC proposed to remove the following 2015 Edition criteria that are not also part of the 2015 Base EHR definition: Drug Formulary and Preferred Drug Lists, Patient-Specific Education Resources, Common Clinical Data Set (CCDS) Summary Record (- Create and - Receive), and

[4] The Systematized Nomenclature of Medicine -- Clinical Terms (SNOMED CT®) is a comprehensive medical terminology for representing clinical content in EHRs, created by the College of American Pathologists, now owned by and maintained by a non-profit entity, the International Health Terminology Standards Development Organisation (IHTSDO®). The National Library of Medicine is a member of IHTSDO and is responsible for distributing the U.S. Edition. For more information, see https://www.nlm.nih.gov/healthit/snomedct/faq.html.

Secure Messaging.[5] ONC noted several reasons for removing these criteria, such as facilitating interoperability and removing constraints to innovation.

Drug Formulary and Preferred Drug List Checks (§170.315(a)(10)). Commenter reactions to removal of this criterion were mixed. Concerns included meeting certain Medicaid PI Program requirements. ONC responds that the current criterion does not require use of any specific interoperability standards and that the criterion will no longer be associated with any CMS PI program measures after 2021. However, to maintain alignment of the Program with CMS regulations, ONC does not finalize removal of this criterion. Instead ONC includes a provision in §170.550(m)(1) that allows ONC-ACBs to issue certificates for this criterion only until January 1, 2022, after which time the criterion will no longer be required for the Medicaid PI Program.

Patient-Specific Education Resources (§170.315(a)(13)). ONC states a belief that the ability to identify appropriate patient education materials is now widespread among health IT developers and their customers (e.g., health care providers). Commenters were concerned that criterion removal would impact their ability to meet certain Medicaid PI Program requirements. ONC responds that this narrowly-focused criterion no longer optimally encourages innovation in the use of health IT to support clinician-patient interactions. However, to maintain alignment of the Program with CMS regulations, ONC does not finalize removal of this criterion. Instead, ONC includes a provision in §170.550(m)(1) that allows ONC-ACBs to issue certificates for this criterion only until January 1, 2022.

Common Clinical Data Set (CCDS) Summary Record (Create and Receive) (§170.315(b)(4) and (5)). ONC proposed removal of these paired criteria since only 2 health IT products are certified only to them rather than including certification to the "transitions of care" criterion (§170.315 (b)(1)). Commenters supported the proposal and ONC finalizes removal of the paired CCDS criteria from the 2015 Edition and the Program.

Secure Messaging (§170.315(e)(2). ONC proposed removal of this criterion as no longer necessary to support sending and receiving secure messages between providers and patients in view of the rapidly evolving options for such data exchanges (e.g., portals and application programming interfaces (APIs)). Concern was expressed by commenters about meeting certain Medicaid PI Program requirements. However, to maintain alignment of the Program with CMS regulations, ONC does not finalize removal of this criterion. Instead ONC includes a provision in §170.550(m)(1) that allows ONC-ACBs to issue certificates for this criterion only until January 1, 2022.

ONC estimated that the two groups of changes above would produce cumulative cost savings of approximately $2.3 million for the period of August 2018 to August 2019, reflecting that some developers would still be newly certifying their products to these criteria in 2018 and 2019.

[5] The CCDS is a set of meaningful use data types, elements, and associated vocabulary standards applicable to multiple certification criteria, originally developed by ONC.

E. Removal of Program Disclosure Requirements (§170.523(k)(1)(iii)(B), §§170.523(k)(1)(iv)(B) and (iv)(C)); §170.523(k)(2))

Currently, ONC-ACBs must ensure that certified health IT includes full, detailed disclosures of any limitations that a user might encounter when implementing and using the IT; some of those limitations might be considered information blocking. However, because ONC addresses information blocking elsewhere in this rule, it removes §170.523(k)(1)(iii)(B), §§170.523(k)(1)(iv)(B) and /(iv)(C)) and the related Principle of Proper Conduct (PoPC) that currently requires developers to attest to their compliance with existing mandatory disclosure regulations (§170.523(k)(2)).

Commenters were supportive of these removals and ONC finalizes the changes as proposed. ONC emphasizes that the remaining transparency requirements addressing costs imposed on users at §170.523(k)(1)(iii)(A) and (iv)(A) remain in effect.

F. Recognition of Food and Drug Administration (FDA) Precertification Processes

In the proposed rule, ONC discussed a Food and Drug Administration (FDA) pilot precertification program for software-based medical devices and proposed a parallel process for health IT developers who are pre-certified under the FDA pilot program and that would initially be applicable only to the quality management systems and safety-enhanced design criteria.

Commenters expressed multiple concerns, mostly related to the limited experience thus far accrued with the FDA pilot program and whether that program's applicability to ONC's Program can yet be assessed. ONC does not finalize recognition of the FDA Software Precertification as applicable to health IT developers under ONC's Program though it anticipates revisiting this option in future rulemaking. ONC concludes by acknowledging the receipt of 21 comments to a request for information (RFI) contained in the proposed rule (84 FR 7439) about independent development by ONC of a developer precertification program.

III. Updating the 2015 Edition Certification Criteria

A. General Considerations

In the proposed rule (84 FR 7439-7454), ONC outlined an approach to updating the 2015 Edition by adopting a limited set of revised and new 2015 Edition certification criteria and related standards. While some commenters supported this approach, numerous others recommended that ONC instead put forth a new edition, citing the number and scope of 2015 Edition changes being proposed by ONC and the potential for confusion among providers who would have to purchase and use certified health IT modules spread across different products but available under the same label ("2015 Edition").

ONC discusses at length the considerations that led to the proposal to update the 2015 Edition rather than to create a new edition at this time. Highlights include:

- Only 2 new technical certification criteria were proposed for adoption (one of which is the Standardized API criterion, §170.315(g)(10)).
- Adoption of a new edition by ONC could trigger CMS to establish a new CEHRT definition to which participants in CMS programs (e.g., PI programs, QPP) would be required to update, imposing a considerable burden just as those participants have completed their full updates to 2015 CEHRT for use in reporting to CMS.
- Adoption of a new edition by ONC has historically led to the repackaging of new, revised, and unchanged criteria into new modules and new products by health IT developers whose timely rollout and implementation is burdensome and costly for developers and health care providers.
- ONC expresses a belief that an entirely new edition should only be established when the scope of the updates is significant enough to warrant the impacts of implementation, which ONC does not believe is true of the proposed updates to the 2015 Edition, if finalized.
- To mitigate potential confusion among providers, ONC plans to distinguish the 2015 Edition certification criteria from the new or revised criteria adopted in this final rule by referring to the new or revised criteria as the "2015 Edition Cures Update" on the CHPL. The CHPL will also differentiate to what standards the health IT product will be certified. ONC states that these additions to the CHPL will allow health care providers to identify if and when a specific Health IT Module has been updated to the criteria and standards finalized in this proposed rule.

ONC concludes the discussion about its approach to updating the Program by finalizing the decision not to create a new edition of certification criteria and associated standards.

B. Technical Standards and Implementation Specifications

To carry out policy objectives, ONC is required to use technical standards developed or adopted by voluntary consensus standards bodies whenever practical but has discretion to make exceptions, including the use of a government-unique standard.[6] ONC proposed to make four exceptions, listed below, and noted that compliance with the entire standard or implementation specification document would be required for each of the exceptions if finalized.

- Replacing the CCDS with a government-unique standard, the USCDI (§170.213);
- Replacing Health Level 7 (HL7) standards with government-unique (CMS) standards to support the use case for the criterion "reporting eCQM data to CMS" (§170.205(h)(3) and (k)(3));[7]

[6] The requirements are set out in the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 3701 et. seq.) and the Office of Management and Budget Circular A–119.

[7] The proposed and finalized standards for this criterion are the CMS Implementation Guide for Quality Reporting Document Architecture: Category I; Hospital Quality Reporting; Implementation Guide for 2019, and the CMS Implementation Guide for Quality Reporting Document Architecture: Category III; Eligible Clinicians and Eligible Professionals Programs; Implementation Guide for 2019.

- Adopting a government-unique implementation specification, the API Resource Collection in Health (ARCH) Version 1 (§170.215(a)(2)); and
- Adopting market-driven consortia standards - the Argonaut Implementation Guides - for APIs at §170.215(a)(3) through (a)(5).[8]

ONC notes that a few commenters voiced opposition to any use of standards other than voluntary consensus standards by federal programs. ONC responds that satisfactory alternatives to the USCDI and the CMS standards were not available for this final rule. ONC opts not to finalize ARCH adoption, but does opt to adopt the FHIR US Core Implementation Guide STU 3 Release 3.0.0 instead of the Argonaut Implementation Guides. The latter two decisions are discussed further in section VII.B.4 of the rule. Summaries and URLs for the adopted standards are provided in section XI of the final rule. Compliance with the entirety of each standard is required upon its incorporation by reference of the standard in the Federal Register.

C. Revised and New 2015 Edition Criteria

1. United States Core Data for Interoperability

a. General Considerations

In the early years of the Program, ONC created a single definition for all required data that could be referenced for all applicable certification criteria, termed the "Common MU Data Set". With the adoption of the 2015 Edition, the Program broadened its focus beyond supporting only CMS programs to fostering a nationwide interoperable health IT infrastructure, for which ONC developed a new data definition framework, termed the "Common Clinical Data Set" (CCDS). ONC noted that increasingly widespread CCDS use outside of the Program has exposed limitations imposed on health IT by the CCDS definitional framework.

More recently, ONC has partnered with stakeholders to create a new, hybrid framework that combines government unique policy considerations and voluntary consensus standards, the USCDI. This framework is a standardized set of health Data Classes and constituent Data Elements required to support nationwide electronic health information exchange (e.g., "patient name" is an element of the "patient demographics" data class). ONC has stated an intention to establish and follow a predictable, transparent, and collaborative process to expand the USCDI as needed (e.g., adding classes and elements), including opportunities for stakeholder input.

ONC proposed to replace the CCDS definition with the USCDI standard (§170.102) and to remove the CCDS definition and all its references from the 2015 Edition. Commenters were broadly supportive, and some identified health care settings for which additional data classes and elements are needed. ONC responds that the USCDI standard as used by the Program is not

[8] The Argonaut Project is a private sector initiative to advance industry adoption of modern, open interoperability standards that includes diverse for profit and not-for profit participants (e.g., Epic Systems, Mayo Clinic). See http://argonautwiki.hl7.org/index.php?title=Main_Page.

specific to any setting of care, nor is it specific to any content exchange standard (e.g., HL7 Fast Healthcare Interoperability Resources - FHIR). ONC goes on to finalize the adoption of the USCDI v1 in §170.213.

ONC estimates costs ranging from $214,000 to $492,000 for a health IT developer who develops support for the additional USCDI elements, and a total cost to all developers ranging from $116.6 million to $268.2 million.

b. USCDI 2015 Edition Certification Criteria

Updating CCDS-dependent criteria. ONC identified several certification criteria as being "CCDS-dependent" and proposed conforming changes to align them with the USCDI v1 standard once the latter was adopted:

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

Commenters generally were supportive, though a few questioned the potential impact on public health agency case reporting. ONC responds that more data might in fact become available to state agencies than currently. ONC finalizes the proposed revisions to the CCDS-dependent criteria. To mitigate commenter concerns about confusion when existing criteria are updated, ONC also finalizes regulatory text modifications for these criteria to clarify that either the CCDS or USCDI is applicable until 24 months after this final rule is published, after which only the USCDI remains applicable to their certification.

Included USCDI Data Classes. ONC received many suggestions from commenters for the addition of new USCDI Data Classes and Data Elements. ONC notes that it purposefully limited the classes and elements of USCDI to be adopted in this final rule to facilitate an orderly, timely transition from the CCDS to the USCDI. ONC, therefore, finalizes the adoption in this final rule of only the classes and elements that were addressed in the proposed rule. ONC also corrects an error in the Procedures Data Class: the American Dental Association's Code on Dental Procedures and Nomenclature (CDT) is to be used for Dental Procedures in the USCDI v1, not SNODENT as listed in the draft version of the USCDI.

Minimum standard code sets. ONC proposed that the newest versions of the minimum standard code sets included in the CCDS as of the time of this rule's publication would be incorporated into USCDI v1. Commenters were supportive and ONC finalizes the incorporation into USCDI. ONC notes that this proposal was not finalized for several criteria for which flexibility to use newer versions already exists: "family health history" (§170.315(a)(12)), "transmission to

immunization registries" (§170.315(f)(1)), and "transmission to public health agencies—syndromic surveillance" (§170.315(f)(2)).

Address and phone number. ONC proposed to add "address" and "phone number" as new USCDI v1 Data Elements to the Patient Demographics Data Class. These elements could facilitate patient matching during EHI exchange. Commenters were unanimously supportive and suggested additional similar elements. Many also recommended incorporating the U.S. Postal Service Postal Addressing Standards for all address data elements. ONC, however, declines to adopt the Postal Addressing Standards at this time as they allow multiple valid addresses under certain circumstances. ONC does stipulate standards for all phone number elements: ITU-T E.123 (02/2001) and ITU-T E. 164. ONC concludes by finalizing the following additions to the Patient Demographics class: "current address"; "previous address"; "phone number"; "phone number type"; and "email address".

Pediatric Vital Signs. These elements are optional in the CCDS. As part of USCDI v1 adoption, ONC proposed the required inclusion of the following elements: head occipital-frontal circumference percentile (Birth to 36 Months); weight-for-length percentile (Birth to 36 Months); body mass index (BMI) percentile (2-20 Years of Age); and the reference range/scale or growth curve, as appropriate. Most commenters were supportive, while a few wished to incorporate the elements as optional for use in USCDI v1. ONC declines to continue these elements as optional and finalizes their required inclusion in USCDI v1.

Clinical notes. ONC has heard from stakeholders that the free-text portion of a clinical note is information that they value highly yet most often find missing during EHI exchange; clinical notes also may have structured data fields. After reviewing public and private initiatives underway to facilitate clinical note exchange, ONC proposed to adopt for the USCDI v1 the 8 clinical note types identified by Argonaut Project participants: (1) Discharge Summary note; (2) History & Physical; (3) Progress Note; (4) Consultation Note; (5) Imaging Narrative; (6) Laboratory Report Narrative; (7) Pathology Report Narrative; and (8) Procedures Note. ONC invited comment on whether to include additional note types. Most commenters were supportive, particularly of the associated ability to capture free text. ONC finalizes the adoption of the proposed 8 types of clinical notes into USCDI v1. ONC closes by stating that the clinical note types as adopted are content exchange standard agnostic (not linked to similarly named Consolidated Clinical Architecture (C-CDA) Document Templates)[9] and must be represented in their plain-text form.

Provenance. Provenance describes metadata that could add to the trustworthiness and reliability of EHI data being exchanged (e.g., who created the data and when). Provenance may provide added-value when data exchange involves APIs that may lack the full clinical encounter context

[9] C-CDA is a document standard for transmitting structured summary data between providers, and between providers and patients; the data support care transitions, referrals and care coordination.

compared to exchange using the (typically larger) C-CDA documents. ONC proposed 3 data elements as part of the proposed new USCDI v1 Provenance class:

- Author – the person(s) responsible for the exchanged information;
- Author's Time Stamp – the time the information was recorded; and
- Author's Organization – the organization with whom the author was associated at the time the author interacted with the data.

The addition of Provenance as a USCDI v1 Data Class was strongly supported by commenters. Concerns were raised about the consistent interpretation of "author". ONC finalizes the addition of Provenance with the modification of including only two data elements: Author's time stamp and Author's Organization.

ONC also had proposed that Provenance would be included in the proposed ARCH Version 1 implementation specification but opted not to finalize ARCH adoption.

Medication Data Class. ONC proposed that the USCDI v1 Medication data class contain two data elements, "Medications" and "Medication Allergies". ONC also requested comment on an alternative approach to Medication Allergies that would: 1) remove the "Medication Allergies" element from the Medication data class; 2) create a new Substance Reactions data class having two elements within it – "Substance" and "Reaction"; 3) report medication allergies under Substance Reactions; and 4) include allergies to non-medication substances based on SNOMED CT®.

Commenters supported the creation of the Substance Reaction data class but recommended retaining the Medication Allergy element. They also recommended naming the new data class "Allergy/Intolerance" rather than "Substance Reaction" to better align with the HL7 FHIR resource of the same name. ONC finalizes creation of a new "Allergies and Intolerances" USCDI v1 Data Class having the following Data Elements: "Substance – (Medication)," "Substance – (Drug Class)," and "Reaction." RxNorm codes are required for representing "Substance – (Medication)" and SNOMED CT® codes are required for representing "Substance – (Drug Class)".

c. <u>USCDI, Content Exchange Standards, and Implementation Specifications</u>

ONC proposed that the USCDI v1 would be agnostic as to content exchange standard and any related implementation specifications (e.g., HL7 C-CDA Release 2.1). It believed that being agnostic to such standards could facilitate updates to newer standards versions. ONC states that all USCDI v1 Data Classes can be supported by commonly used content exchange standards. ONC received no comments and finalizes the proposal without modifications.

2. C-CDA Implementation Specification: Clinical Notes

Concomitant with USCDI v1, ONC proposed including the HL7 CDA® R2 IG: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 1 ("C-CDA Companion Guide") at §170.205(a)(5). The guide provides guidance for specifying data in the C-CDA Release 2.1, supporting Data Classes added by USCDI v1 (e.g., Clinical Notes). If finalized for incorporation, the Guide would impact the 2015 Edition certification criteria that reference C-CDA Release 2.1:

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

ONC received few comments and finalizes adoption of the C-CDA Companion Guide, modified to specify the most recently updated version in §170.205(a)(5). This version is incorporated by reference in §170.299. Further, ONC makes changes to align the criterion "clinical information reconciliation and incorporation" (§170.315(b)(2)) with the newly finalized "Allergies and Intolerances" data class and its constituent data elements. ONC concludes by finalizing timing of the C-CDA Companion Guide update: updates to previously certified IT for the 5 criteria referencing C-CDA Release 2.1 (listed above) must be in use no later than 24 months after the effective date of this final rule.

3. C-CDA Implementation Specification: Unique Device Identifier(s) for Implantable Device(s)

ONC sought comment through the proposed rule about the potential adoption into §170.299 of the HL7 CDA R2 Implementation Guide: C-CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1-US Realm (UDI IG Release 1). This Implementation Guide (IG) describes changes to improve UDI component data exchange (e.g., serial number, manufacturing date). Adoption was unanimously supported by commenters, but none responded to ONC's solicitation of estimates of the cost or burden of compliance. ONC finalizes the proposed UDI Data Class within the USCDI v1 and has adopted the UDI Organizer Template defined in the UDI IG Release 1.

4. Revising the Electronic Prescribing Certification Criterion

a. <u>General considerations</u>

ONC and CMS have historically aligned health IT certification criteria with Medicare Part D electronic prescribing (e-Rx) standards. CMS has finalized retiring National Council for Prescription Drugs Program (NCPDP) SCRIPT version 10.6, the current standard, and adopting NCPDP SCRIPT 2010771 as the new standard beginning January 1, 2020. To maintain

alignment with CMS, ONC had proposed adoption of NCPDP SCRIPT 2010771 by ONC as the standard for its "e-Rx" certification criterion and all transactions listed therein, along with those adopted by CMS for NCPDP SCRIPT 2010771 (42 CFR 423.160(b)(2)(iv)). Operationally, ONC proposed removing the current criterion (§170.315(b)(3)) referencing NCPDP SCRIPT version 10.6 and replacing it with the updated criterion that references NCPDP SCRIPT 2010771 (§170.315(b)(11)). ONC also proposed to permit continued use of the current criterion until required use of NCPDP SCRIPT 2010771 became effective for CMS programs.

The transactions for which ONC proposed NCPDP SCRIPT 2010771 would become applicable under the revised "e-Rx" criterion follow:

- Create new prescription,
- Change prescription,
- Cancel prescription,
- Renew prescription,
- Receive fill status notification,
- Request and receive medication history,
- Query the mailbox for transactions,
- Relay acceptance of a transaction back to sender,
- Report that there was a problem with the transaction,
- Confirm receipt of a transaction that requests return receipt,
- Request that additional supply of medication be sent,
- Communicate drug administration events,
- Transfer prescription(s),
- Recertify continued med administration order, and
- Complete RMS transactions.

Commenters were generally supportive, but raised concerns about certain specific transactions (discussed further below). An overarching concern was expressed about the lack of a certification program and associated standards for pharmacy information systems (PIS), and the inconsistency of technical capabilities within PIS users. ONC responds that PIS users for Part D transactions are required to comply with the NCPDP SCRIPT 2010771 as of January 1, 2020. ONC goes on to note that PIS are outside of the scope of the ONC HIT Certification Program. Commenters also worried about transition timeline and implementation challenges.

ONC finalizes the proposal to update the 2015 Edition e-Rx NCPDP SCRIPT standard to version 2010771. To facilitate the transition, ONC modifies its proposal to implement this update (and the associated "e-Rx" criterion), choosing to revise the current criterion at §170.315(b)(3) rather than removing and replacing it. ONC notes that related real-world testing provisions at §170.405(b)(5) allow a 24-month period for updating the "e-Rx" criterion by developers and dissemination of updated IT to customers.

b. Transaction-specific considerations

Some standardization concerns were raised for multiple transactions, citing, for example, limitations of the RxNorm standard when used for electronic prescribing (e.g., RxNorm does not require a single unique ID number for each branded drug). Others noted that NCPDP standards are not yet in an API-ready format. Other concerns voiced apply only to one or a small number of transactions; the ONC responses are available for each transaction in the preamble. (A table summarizing information from the rule about the finalized ONC transaction decision is provided below.)

c. Miscellaneous considerations

Electronic Prior Authorization (e-PA). ONC notes that NCPDP SCRIPT standard version 2010771 includes 8 transactions that would enable prescribers to initiate medication ePA requests at the time of the patient's visit: PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse. Commenter support for required use of the e-PA transactions was mixed, and ONC adopts these transactions as optional. Though optional, when used they are subject to the requirement of including a reason for the prescription (discussed below).

Reason for the Prescription. ONC notes that its requirement for Health IT modules seeking certification to the updated "e-Rx" criterion be capable of including the reason for the prescription, will be applicable to the following NCPDP SCRIPT standard version 2010771 transactions adopted by ONC in this final rule: NewRx, RxChangeRequest, RxChangeResponse, CancelRx, RxRenewalRequest, RxRenewalResponse, RxFill, RxHistoryResponse, Resupply, RxTransferRequest, RxTranferResponse, REMSInitiationRequest, REMSInitiationResponse, REMSRequest, REMSResponse, PAInitiationRequest, PAInitiationResponse, PARequest, PAResponse, PAAppealRequest, PAAppealResponse, PACancelRequest, and PACancelResponse.

Oral Liquid Medications. One commenter opposed continuation of the requirement for oral liquids to be prescribed using metric units (i.e., "mL" – milliliter). ONC responds that this requirement is not in the scope of this final rule but adds support for the continued requirement as an aid to improved patient safety compared to confusion and ambiguity of non-metric terms (e.g., teaspoon and tablespoon).

Signatura (Sig) Element. In response to a request that this element be required rather than optional, ONC retains the Sig element as optional given the paucity of interest expressed about it.

Real-Time Pharmacy Benefit (RTPB). ONC notes that in recent rulemaking,[10] CMS included a requirement for Part D plans to implement one or more electronic RTPB tools capable of integrating with at least one prescriber's electronic prescribing system or EHR no later than January 1, 2021.

Electronic Prescribing of Controlled Substances. Several commenters addressed topics related to the electronic prescribing of controlled substances and prescription drug monitoring programs. ONC notes that these topics are outside of scope for this final rule. ONC refers stakeholders to the discussion of these topics included in the RFI on opioid use disorder prevention and treatment in the proposed rule (84 FR 7461).

[10] On May 16, 2019, CMS issued the Modernizing Part D and Medicare Advantage to Lower Drug Prices and Reduce Out-of-Pocket Expenses final rule (see 84 FR 23832).

Table. ONC final actions by transaction included under the updated (NCPDP SCRIPT 2010771) "e-Rx" certification criterion			
Transaction Purpose	**Transaction Terms**	**ONC Final Action**	**Need Rx Reason?**
Create new prescription	NewRx NewRxRequest NewRxResponseDenied	Required Optional Optional	Yes Yes
Change prescription	RxChangeRequest RxChangeResponse	Required Required	No Yes
Cancel prescription	CancelRx CancelRxResponse	Required Required	Yes No
Renew prescription	RxRenewalRequest RxRenewalResponse	Required[a] Required[a]	Yes Yes
Receive fill status notification	RxFill RxFillIndicatorChange	Required Optional	Yes No
Request and receive medication history	RxHistoryRequest RxHistoryResponse	Required Required	No Yes
Query the mailbox for transactions	GetMessage	Optional	No
Relay acceptance of a transaction back to sender	Status	Required	No
Report that there was a problem with the transaction	Error	Required	No
Confirm receipt of a transaction that requests return receipt	Verify	Required	No
Request that additional supply of medication be sent	Resupply	Optional[b]	Yes
Communicate drug administration events	DrugAdministration	Optional[b]	No
Transfer prescription(s) alignment	RxTransferRequest RxTransferResponse RxTransferConfirm	Optional Optional Optional	Yes Yes No
Recertify continued med administration order	Recertification	Optional[b]	No
Complete REMS transactions	REMSInitiationRequest REMSInitiationResponse REMSRequest REMSResponse	Optional[c] Optional[c] Optional[c] Optional[c]	Yes Yes No No

[a] All requirements of §170.315(b)(3) must be met
[b] Supports use in the long-term post-acute care setting
[c] System readiness for use of this transaction varies widely

5. Clinical Quality Measures – Report

ONC details the history of its endeavors to support electronic reporting of clinical quality measures (CQMs) by providers to CMS programs (e.g., end-to-end reporting). These have entailed adoption of the Category I and Category III Quality Reporting Document Architecture (QRDA) standards along with their related HL 7 and CMS IGs. Stakeholder feedback has been mixed and suggests that health IT modules certified to the "CQM–report" criterion are used virtually exclusively for reporting to CMS programs. ONC proposed to reduce the burden of multiple standards for developers and providers by removing the HL7 QRDA standards from the 2015 Edition CQM-report criterion (§170.315(c)(3)), while also requiring certified modules to support the most recent available CMS QRDA I (for hospital reporting) and QRDA III (for eligible providers) IGs.

Most but not all commenters were supportive of the proposed changes. Some sought retention of the standards as optional for use by non-CMS programs in which HL7 QRDA standards are also used, such as those of The Joint Commission. Commenters also suggested that developers be allowed to comply with either or both of the QRDA I and QRDA 3 standards according to the settings in which their health IT would be used. ONC finalizes the changes as proposed and adopts the latest standards versions available at the time of publication of this final rule. ONC concludes by agreeing with many commenters that quality reporting in general is not yet ready for transition to FHIR within the ONC certification program.

6. Electronic Health Information Export

a. Addition of "EHI Export" criterion

ONC proposed to add a new certification criterion for "EHI export" (§170.315(b)(10)) to the 2015 Edition and to the 2015 Edition Base EHR definition. The new criterion was designed to support exporting in two contexts: 1) exporting a single patient's EHI when requested by a patient or on their behalf (single patient export), and 2) exporting all EHI of multiple patients when a health care provider is switching from one health IT system to another (patient population export). The proposed definition of the EHI to be exported was all of the protected health information (PHI) that a certified health IT product produces and electronically manages. Additionally, ONC proposed that all formatting necessary to support both export contexts would be made available via publicly accessible hyperlink and that the hyperlinked format file would be kept current by the developer. Commenters supported the goal of adding "EHI Export": advancing the access, exchange, and use of EHI consistent with the provisions of the Cures Act. However, commenters also raised multiple implementation concerns, especially regarding the extent of EHI for which export would be required.

ONC finalizes adding to the 2015 Edition a revised version of the proposed criterion that includes defining EHI as that which can be stored by a health IT product certified to the EHI export criterion at the time of certification. ONC paraphrases this definition as "the same ePHI that a patient would have the right to request a copy of pursuant to the HIPAA Privacy Rule" (see §171.102 for the complete definition). ONC clarifies that the definition of data to be exported would apply to all stored EHI, including data from third parties, whether the data are

stored in conjunction with a product's certified modules or stored using "non-certified capabilities" of the product. ONC acknowledges that the amount of EHI exported and the format in which it is represented will vary across developers and their products. Of note, ONC rejected the recommendation to define EHI as only the data represented by the USCDI, made by multiple commenters, as too limiting to advancing the policy interests of the Program. Given the many operational questions raised, ONC does not finalize adding "EHI Export" to the 2015 Base EHR definition.

ONC states that the total cost to developers for EHI export criterion product development is estimated to range from $18.7 million to $151.6 million. Approximately one-half of this cost would be one-time rather than perpetual. Estimated total costs for hospitals and clinical practices to implement and support the EHI export range from $351.7 million to $703.3 million, along with an estimated cost savings ranging from $256.8 million to $2.6 billion.

b. Single Patient EHI Export

ONC proposed that certification to the "EHI Export" criterion would require enabling a user of certified health IT to timely create one or more export file having all the EHI the health IT product produces and electronically manages on a single patient. ONC also proposed to require that a user would be able to execute the export at any time of the user's choice and without the necessity for assistance from the developer. ONC further proposed to require that certified modules would enable restricting the users who could create the export file. Restriction would be required to take the form of a specific set of identified users and/or a system administrative function; other restrictions could also be added. Finally, ONC proposed to require that the export file(s) created must be electronic, in a computable format, and be accompanied by the file format, including its structure and syntax, along with a publicly accessible hyperlink.to the formatting.

Commenters supported the proposal; a few suggested file formats and standards. ONC finalizes the single patient export functionality for the EHI Export criterion with some modifications. The revised definition of EHI (see above) will be applied to single patient export and user restriction will be implemented as proposed. ONC also finalizes that the export file be electronic and in a computable format. The formatting hyperlink must be accessible to the file's user but will not be required to accompany the export file; the developer is responsible for ensuring that the formatting hyperlink is kept up to date. ONC states that the EHI export criterion is subject to real world testing. (See section VI.B.5 below.)

c. Patient Population EHI Export

ONC proposed that certification to the "EHI Export" criterion would require a developer to enable a complete export of all EHI that is produced or electronically managed by the developer's health IT modules whenever a user requests that records for a patient population be migrated to another health IT system. Many commenters supported the proposal; a few raised concerns (e.g., handling patient consent).

ONC finalizes the patient population export functionality for the EHI Export criterion with some modifications. The revised definition of EHI (see above) will be applied to patient population

export. ONC also finalizes that the export file be electronic and in a computable format. The formatting hyperlink must be accessible to the file's user but is not required to accompany the export file; the developer is responsible for ensuring that the formatting hyperlink is kept up to date. ONC acknowledges that, given the potential size and complexity of a patient population EHI export file, the developer's assistance might be needed by the user to execute EHI migration. ONC states that the EHI export criterion is subject to real world testing, summarized in section VI.B.5 below. Reasonable cooperation must be provided by the developer consistent with the Assurances Condition. (See section VI.B.2 below.)

d. Scope of Exported Data

In General. ONC proposed that the definition of EHI to be exported using a certified health IT product would include all the PHI that a certified health IT product produces and electronically manages. There were numerous commenters, the majority of whom regarded the proposed definition as ambiguous, too broad, and open to inconsistent interpretation. After an extended discussion of commenter concerns, ONC finalizes the scope of the EHI to be exported as that which can be stored by a health IT product certified to the EHI export criterion at the time of certification.

Additionally, ONC reiterates that "stored" EHI includes data from third parties and that the definition includes both data stored in conjunction with a product's certified modules or stored using "non-certified capabilities" of the product. ONC clarifies that any new EHI stored by the product as a result of storage enhancements would not need to be included with exported EHI until a new version of the product with the new EHI storage capabilities is presented for certification and listing on the CHPL. ONC points out that scope of EHI for export would include data stored within the product itself and at other data storage locations. Finally, developers could choose to support EHI export beyond the scope of the finalized definition, but data disclosures would be subject to all applicable laws and regulations.

Image, Imaging Information, and Image Element Export. In the proposed rule, ONC sought input as to the feasibility, practicality, and necessity of exporting images and/or imaging information, as well as what image elements, at a minimum, should be shared (e.g., image type). However, ONC did not make any proposals. Most commenters supported exporting images but stated concerns about added burden, efficiently handling very large data files, and collating files from disparate health IT systems. Comments on the extent of minimum image elements to be shared varied widely.

ONC reminds stakeholders that all stored imaging data that meets the finalized EHI definition must be included as part of single patient and patient population export files. It notes that if only the hyperlinks through which users can access imaging data are stored within the health IT (and not the images) then only the hyperlinks would be required for inclusion in the EHI export files.

Attestation of Inability to Export. In the proposed rule, ONC invited input about whether health IT developers should be required to attest to or publish types of EHI that they cannot support for export. ONC did not make any specific proposals. Most commenters were supportive of

documenting this information. However, ONC decided that the revised definition of EHI for export is sufficiently clear, and that additional requirements for such attestation are not needed.

e. Accessing Exported EHI

File Formatting. ONC did not propose a content standard for the exported EHI, but it did propose to require developers to document that their health IT includes the formatting necessary for users to access and process the EHI. ONC also proposed to require that the export format be made publicly available and by hyperlink; developers would be required to keep the formatting current and the hyperlink active. Commenters were supportive. ONC finalizes the proposals with modification for clarity. The documentation for the export format must provide information on the structure and syntax for how the product will be exported (e.g., C-CDA document, .csv files) but not the actual EHI. The export format could differ from that used internally by the sending health IT system. Formatting must be updated, for example when a developer changes specified standards from to FHIR from C-CDA and ceases to support the C-CDA format. ONC clarifies that the hyperlink must be readily accessible: the export support file must be available to any user through the hyperlink without preconditions or additional steps

Real-time Access. In the proposed rule ONC stated for clarity that discrete data export rather than "persistent" or "continuous" access would suffice as the minimum to achieve "EHI Export" certification. However, ONC made no specific proposals. Multiple commenters raised definition and operational questions about the terms "persistent" or "continuous". ONC responds that the revised scope of EHI defined in this final rule provides context for the meaning of "persistent" or "continuous" and again notes the absence of any requirement that incorporates those terms.

Time limitation of EHI export data. In the proposed rule, ONC asked if the Export criterion should be capable of allowing health care providers to set timeframes for the data to be exported (e.g., "past month"). Most commenters opposed requiring this capability, citing technical complexity and the potential for information blocking. ONC decides not to require the ability for time-limited export.

7. Data Export Criterion Removal (§170.315(b)(6))

ONC proposed that if the new EHI criterion were to be finalized, the existing data export criterion would be removed from the 2015 Edition upon the effective date of the final rule, and an implementation period provided for the new criterion of 24 months from that same date. Most commenters were concerned about a potential temporary gap in functionality. ONC responds by maintaining availability of certification to the data export criterion by ONC-ACBs until 36 months after this final rule's publication date. ONC finalizes the removal of "data export" from the 2015 Edition Base EHR on the effective date of the rule. The existing criterion will not be updated to the USCDI. ONC concludes by responding to commenters that the data export criterion is not required for compliance with the CMS QPP measure entitled "Provide Patients Electronic Access to their Health Information", and notes that technology certified to the "View, Download and Transmit to 3rd party" criterion (§170.315(e)(1)) is required by CMS to meet this measure.

8. Standardized API for Patient and Population Services

As part of Cures Act implementation, ONC proposed to adopt a new "Standardized API for Patient and Population Services" certification criterion (§170.315(g)(10)) to replace the current "application-access–data category request" criterion" (§170.315(g)(8)). The new API criterion also would be added to the 2015 Edition Base EHR definition. Commenters were supportive.

ONC finalizes the addition of "Standardized API for Patient and Population Services" to the 2015 Edition and to the 2015 Base EHR definition. Features of the finalized criterion include required use of the HL7 Version 4.0.1 Fast Healthcare Interoperability Resources (FHIR) Release 4 standards, adoption of several implementation specifications, and the provision of support for the two "EHI export" criterion use cases (i.e., single patient access and patient population EHI export). Additional aspects of the API criterion are discussed in section VI.4 of this summary.

ONC provides an estimate of average cost per developer to develop and maintain a product to the new API criterion ranging from $0.75 million to $1.64 million. Total estimated costs to developers are $297.3 million to $644.8 million; of the total costs, $110.9 million to $272.3 million are one-time costs and not perpetual. ONC also estimates total cost to hospitals and clinical practices to acquire and use software applications that engage with certified API technology would range from $140.6 million to $929.3 million. Additionally, ONC calculates an estimated total annual benefit of APIs, ranging on average from $0.34 billion to $1.43 billion, spread across patients and providers.

9. Privacy and Security Attestations and Framework Updates

a. General Considerations

Criteria Additions and Attestations. The privacy and security (P&S) framework applicable to the 2015 Edition is codified at §170.550(h). Following direction from the Secretary, ONC proposed adding two new "authentication" certification criteria to the framework: "encrypt authentication credentials" (§170.315(d)(12)) and "multi-factor authentication" (§170.315(d)(13)).[11] For both criteria, ONC proposed to require health IT developer attestations (yes/no) as to whether their modules have either or both authentication capabilities. Reporting by developers of results of actual module testing to either or both criteria would not be required, but modules certified to the new criteria would be subject to ONC-ACB surveillance. (Testing requirements are detailed in the finalized P&S framework, provided as Table 2 of the final rule and reproduced below).

The two proposed authentication certification criteria, and their associated yes/no attestation format, were supported by the vast majority of commenters. ONC clarifies that the new criteria do not require certified health IT to have these capabilities or require developers to include these capabilities for specific use cases. Further, ONC notes that these criteria would not require IT users (e.g., health care providers) to implement the associated authentication capabilities. ONC

[11] Both new authentication criteria were recommended by the HIT Standards Committee and endorsed by the National Coordinator.

finalizes adoption of the "encrypt authentication credentials" and "multi-factor authentication" criteria into the 2015 Edition and its P&S framework.

Scope and Timeline. ONC proposed that each of the new criteria would be applicable to all modules that are required to meet the "authentication, access control, and authorization" certification criterion (§170.315(d)(1)).[12] ONC further proposed that the new criteria would apply both to currently certified health IT modules and to modules being presented for certification. For health IT certified prior to this final rule's effective date, certification (by attestation) to the new criteria would be required within six months after the rule's effective date. Health IT presented for certification for the first time after this final rule's effective date would be required to meet the new criteria (by attestation) at the time of certification.

Although some come commenters advocated requiring multi-factor authentication (MFA) for all health IT, ONC disagrees. Numerous commenters recommended that the timeline for compliance be adjusted or that the new criteria be applied only to new certification requests and not to previously certified health IT. ONC agrees and modifies its proposal, finalizing that certification to the new authentication criteria under the updated 2015 Edition P&S framework will be required only for Health IT Modules presented for first-time certification after the effective date of this final rule. Similarly, a previously certified but newly revised P&S framework module presenting for certification after the effective date of this final rule will be required to satisfy the new criteria at the time of presentation.

Posting Health IT Developer Attestations. ONC further proposed that the "yes" and "no" attestations made by health IT developers would be publicly posted on the CHPL. An attestation response of "yes" to either of the authentication criteria would indicate that the Health IT Module(s) to be certified to that criterion can support either Approach 1 (technically demonstrate) or Approach 2 (system documentation) of the 2015 Edition P&S certification framework. Guidance for using the two Approaches is provided within the finalized P&S framework (Table 2 of the final rule, reproduced below). In response to queries from commenters, ONC notes that attesting "no" could indicate inability to support both Approaches but also might have other explanations, discussed separately below for the two criteria. ONC finalizes that health IT developers' attestations for the new authentication criteria will be posted on the CHPL.

b. Specific considerations

Encrypt authentication credentials. While the 2015 Edition has required encryption of EHI saved on end-user devices (§170.315(d)(1)) and specifies an encryption standard (§170.210(a)(2)),[13] encryption has not been explicitly required for the credentials used to access the EHI. This gap is addressed by modules for which developers attest "yes" for the newly finalized "encrypt authentication credentials" criterion. ONC notes that encryption could include password

[12] This criterion describes the capability of a module to verify through the use of a unique identifier(s), such as user name or number, that a user seeking access to EHI is in fact the one claimed.
[13] The adopted standard is Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

encryption, cryptographic hashing, or any other method included in the encryption standard. In response to commenters, when finalizing the "encrypt authentication credentials" criterion, ONC added the ability for developers who attest "no" to explain their answers; the answers would appear along with the "no" attestation on the CHPL. For example, a developer might indicate that a module is not designed to store authentication credentials and therefore the ability to encrypt such credentials is unnecessary.

Multi-factor authentication (MFA). ONC notes that single-factor authentication is particularly prone to cyber-attack. Modules certified to the newly finalized MFA criterion are able to support authentication of user identity through multiple elements to industry recognized standards.[14] Responding to commenters, when finalizing the MFA criterion ONC added a requirement that developers who attest "yes" during module certification must also describe the use cases supported by their modules. For example, a developer could indicate that a module supports MFA for remote access by clinical users and report this explanation on the CHPL. Developers who attest "no" would be permitted but not required to report a reason for their "no" attestations. For example, a developer could explain that a module does not support MFA because the module is used only in system public health reporting for which MFA is not applicable.

P&S Framework Revision. ONC also proposed to revise the 2015 Edition P&S Framework (Table 1 of the proposed rule, 84 FR 7455). The revisions would reflect that many 2015 Edition certification criteria would be subject to the two proposed (now finalized) authentication criteria. No comments specific to the framework revision were received. ONC finalizes the proposed framework with minor modifications to incorporate all actions taken throughout the final rule that are relevant to the P&S framework. The finalized P&S framework is provided in Table 2 of the final rule and reproduced below.

Table 2: 2015 Edition Privacy and Security Certification Framework

If the Health IT Module includes capabilities for certification listed under:	It will need to be certified to Approach 1 or Approach 2 for each of the P&S certification criteria listed in the "Approach 1" column	
	Approach 1	Approach 2
§170.315(a)(1) through (3), (5), (12), (14), and (15)	§170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (auditreports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6) (emergency access), (d)(7) (end-user device encryption), (d)(12) (encrypt authentication credentials), (d)(13) (multi-factor authentication)	For each applicable P&S certification criterion not certified using Approach 1, the health IT developer submits system documentation that is

[14] For example, National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Authentication Guidelines; see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

Table 2: 2015 Edition Privacy and Security Certification Framework		
If the Health IT Module includes capabilities for certification listed under:	It will need to be certified to Approach 1 or Approach 2 for each of the P&S certification criteria listed in the "Approach 1" column	
	Approach 1	Approach 2
§170.315(a)(4), (9), (10), and (13)	§ 170.315(d)(1) through (d)(3), (d)(5) through (d)(7), (d)(12), and (d)(13)	sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable P&S certification criterion that enable the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion
§ 170.315(b)(1) through (3) and (6) through (9)	§ 170.315(d)(1) through (d)(3), (d)(5) through (d)(8) (integrity), (d)(12), and (d)(13)	
§170.315(c)	§ 170.315(d)(1) through (d)(3) and (d)(5), (d)(12), and (d)(13)*	
§170.315(e)(1)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(7), (d)(9) (trusted connection), (d)(12), and (d)(13)	
§170.315(e)(2) and (3)	§ 170.315(d)(1) through (d)(3), (d)(5), (d)(9), (d)(12), and (d)(13)*	
§170.315(f)	§ 170.315(d)(1) through (d)(3), (d)(7), (d)(12), and (d)(13)	
§170.315(g)(7) through (g)(10)	§ 170.315(d)(1) and (d)(9); (d)(2) or (d)(10) (auditing actions on health information), (d)(12), and (d)(13)	
§170.315(h)	§ 170.315(d)(1) through (d)(3), (d)(12), and (d)(13)*	

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

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

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

10. Security Tags and Consent Management Criteria

Security tagging enables recognition of and limiting access to sensitive data elements (e.g., HIV status) while supporting interoperable EHI exchange in accordance with applicable laws, policies, and patient preferences. The 2015 Edition currently includes two certification criteria: "DS4P-send" and "DS4P-receive" (§170.315(b)(7) and (b)(8)) that incorporate the Data Segmentation for Privacy (D4SP) standard and HL7 Healthcare Classification System (HCS) specifications. The current criteria allow security tagging at the document level of documents formatted to the C-CDA 2.1 standard. ONC has expressed an intent to move the Program along a glide path towards using technical standards to ensure interoperable sharing of sensitive EHI, which would support security tagging at the section and entry levels as well as the document level. More granular tagging potentially allows support of sensitive EHI exchange for more complex use cases (e.g., behavioral health).

a. Changes to "DS4P-send" and "DS4P-receive" (§170.315(b)(7) and (b)(8))

ONC proposed to remove the current "DS4P-send" and "DS4P-receive" criteria as of the effective date of this final rule, replacing them with new criteria "DS4P-send" and "DS4P-receive" (§170.315(b)(12) and (b)(13)) that would call attention to their full tagging capabilities (document, section, and entry). No standards revisions would be required. ONC received numerous supportive and opposing comments, and categorized them into 9 topic areas: provider and developer burden; readiness of the standard and C-CDA exchange; information blocking and EHI; future multidisciplinary activities (such as workgroups) and creating a vision for segmentation using health IT; safety; privacy policy conformity; suggested use cases; cost; and requests for specific clarifications. Highlights from the ONC responses include:

- These criteria would remain voluntary and not required under the definition of CEHRT or to participate in any HHS program.
- The substantial burden described by stakeholders (e.g., manual redaction workarounds) is primarily created by the complexity of the privacy law landscape rather than by the D4SP criteria and standards.
- Segmented records are inherently incomplete and could create patient safety issues, but the excluded data are identified by the patient, not mandated by the DS4P standard.
- Data segmentation is necessary for implementation of full EHI export, and factors into the application of information blocking regulations.[15]
- ONC disagrees that experience with the current DS4P criteria and standard is insufficient, citing description of the standard as "normative" by HL7.
- ONC acknowledges the lack of conformity of state and federal privacy laws but such issues are beyond the scope and abilities of ONC to address.
- Commenters and ONC cite ongoing and pending activities to advance D4SP adoption.

ONC finalizes changes to the current DS4P criteria as revisions to §170.315(b)(7) and (b)(8) rather than adopting their removal and replacement as proposed. ONC also modifies the

[15] Inability to unambiguously segment requested EHI from remaining EHI may invoke the Infeasibility Exception to the information blocking definition.

proposed effective date (effective date of this final rule) to allow for document-level (only) tagging for up to 24 months after final rule publication. As a result of the final actions:[16]

- The prior criterion "DS4P-send" with document-level tagging (§170.315(b)(7)) is revised to "Security tags – Summary of Care (send)" with document, section, and entry-level tagging but remains at §170.315(b)(7)).
- The prior criterion "DS4P-receive" with document-level tagging (§170.315(b)(8)) is revised to "Security tags – Summary of Care (receive)" with document, section, and entry-level tagging but remains at §170.315(b)(8)).
- Both "DS4P-send" and "DS4P-receive" allow for continuation of document-level tagging (only) for up to 24 months after final rule publication and for document, section, and entry-level tagging beginning with this final rule's effective date and subsequent years.

b. Electronic consent for exchange of security-tagged data via API (Consent2Share)

As development of APIs for health IT use accelerates, ONC noted in the proposed rule that API infrastructure could be leveraged by developers for secure, scalable sharing of segmented data. ONC reprised prior work with the Substance Abuse and Mental Health Services Administration (SAMHSA) in developing the Consent2Share application. This open source application for data segmentation and consent management is designed to integrate with existing FHIR systems to enable privacy protections for substance abuse disorder treatment data. ONC proposed a new certification criterion "consent management for APIs" (§170.315(g)(11)) for support of data segmentation and consent management through an API and linked to the FHIR-based Consent Implementation Guide (Consent IG) developed by SAMHSA.[17] Certification to this criterion would be discretionary for developers but would indicate a system's capability to use an API with standards-based security labeling.

Commenters supported the proposed criterion conceptually but raised numerous concerns about its implementation, including that the Consent IG is not yet adapted for FHIR Release 4. Having just finalized the use of FHIR Release 4 under the "Standardized API for Patient and Population Services" criterion §170.315(g)(10)), ONC does not finalize its proposal to add the "consent management for APIs" criterion.

11. Auditable events and tamper-resistance, Audit Reports, and Auditing Actions on Health Information, Audit Reports

ONC notes that the ASTM E2147 standard for the "Auditable events and tamper-resistance" (§170.315(d)(2)), "Audit Reports" (§170.315(d)(3)), and "Auditing Actions" (§170.315(d)(10)) criteria has been replaced by a newer version. ONC describes changes that have been made to align the existing criteria with the latest version, ASTM E2147-18. ONC asserts that the changes to the standard are not substantial and the criteria updates are largely technical or for clarity. Developers of modules certified to these criteria must update their modules within 24 months of

[16] The 24-month timeline is further discussed under real world testing, §170.405(b)(6), summarized in section VI.B.5,

[17] Consent2Share Consent Profile Design, accessible under STU3 Implementation Guide at https://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseBrowse&frs_package_id=303.

the publication date of this final rule, and must provide updated health IT to their customers no later than 24 months from the publication date of this final rule.

D. Program Reference Alignment for Otherwise Unchanged Criteria

Reflecting the renaming by CMS of its EHR Incentive programs to Promoting Interoperability programs, ONC proposed to update two otherwise unchanged criteria that reference those programs: "automated numerator recording" (§170.315(g)(1)) and "automated measure calculation" (§170.315(g)(2)). ONC received no comments and finalizes the updated criteria.

E. Summary of Changes to 2015 Edition Certification Criteria

In Table 1 of this final rule, ONC provides a complete list of all certification criteria changes, reproduced below with minor modifications.

Summary 2015 Edition Cures Update (modified from Table 1 of the final rule)				
Certification Criterion	**Reference**	**Change Type**	**Change Timing**	**Impact CMS PI Programs**
Problem List	§170.315(a)(6)	Removed	Final rule effective date	Removed from 2015 Edition Base EHR
Medication List	§170.315(a)(7)	Removed	Final rule effective date	Removed from 2015 Edition Base EHR
Medication Allergy List	§170.315(a)(8)	Removed	Final rule effective date	Removed from 2015 Edition Base EHR
Drug Formulary and Preferred Drug List Checks	(§170.315(a)(10)	Time-limited	ONC-ACBs may certify until 1/1/2022	e-Rx and PDMP Query measures operational for Medicaid until 1/1/2022
Smoking status	§170.315(a)(11)	Removed	Final rule effective date	Removed from 2015 Edition Base HER
Patient-specific Education Resource	§170.315(a)(13)	Time-limited	ONC-ACBs may certify until 1/1/2022	Operational for Medicaid until January 1, 2022 Supports Patient Electronic Access to Health Information Objective Measure
Transitions of Care	§170.315(b)(1)	Revised	Update to USCDI or C-CDA companion IG w/in 24 mo rule publication	PI Measures: -Support Electronic Referral Loops Send -Support Electronic Referral Loops Receive and Incorporate
Clinical information reconciliation and incorporation	§170.315(b)(2)	Revised	Update to USCDI or C-CDA companion IG w/in 24 mo of final rule publication	PI Measures: Support Electronic Referral Loops by Receiving and Incorporating Health Information
Electronic prescribing	(§170.315(b)(3)	Revised	Update standard w/in 24 mo final rule publication	PI measure e-Prescribing
CCDS summary – create	§170.315(b)(4)	Removed	Final rule effective date	No impact described by ONC
CCDS summary – receive	§170.315(b)(5)	Removed	Final rule effective date	No impact described by ONC
Data Export	§170.315(b)(6)	Time-limited	ONC-ACBs may certify for 36 mo once rule published	Removed from 2015 Edition Base EHR definition final rule effective date
Security tags – summary of care—send	§170.315(b)(7)	Revised	Document level until 24 mo after rule publication/ Document, section, entry level effective date rule	No impact described by ONC

Summary 2015 Edition Cures Update (modified from Table 1 of the final rule)				
Certification Criterion	**Reference**	**Change Type**	**Change Timing**	**Impact CMS PI Programs**
Security tags – summary of care—receive	§170.315(b)(8)	Revised	Document level until 24 mo after rule publication/ Document, section, entry level effective date rule	No impact described by ONC
Care plan	§170.315(b)(9)	Revised	Update to C-CDA companion IG w/in 24 mo rule publication	No impact described by ONC
EHI export	§170.315(b)(10)	New	Update within 36 months of final rule publication	No impact described by ONC
CQMs – Report	§170.315(c)(3)	Revised	Final rule effective date	PI Programs
Auditable events and tamper- resistance	§170.315(d)(2)	Revised	Update to new ASTM standard w/in 24 mo of final rule publication	No impact described by ONC
Audit report(s)	§170.315(d)(3)	Revised	Update to new ASTM standard w/in 24 mo of final rule publication	No impact described by ONC
Auditing actions on health Information	§170.315(d)(10)	Revised	Update to new ASTM standard w/in 24 mo of final rule publication	No impact described by ONC
Encrypt authentication credentials	§170.315(d)(12)	New	Final rule effective date (New and updated certifications only)	No impact described by ONC
MFA	§170.315(d)(13)	New	Final rule effective date (New and updated certifications only)	No impact described by ONC
View, Download, and Transmit to 3rd Party	§170.315(e)(1)	Revised	Update to USCDI/C-CDA companion IG w/in 24 months after rule published	Used with PI measure: Provide Patients Electronic Access to Their Health Information
Secure Messaging	§170.315(e)(2)	Time-limited	ONC-ACBs may certify until 1/1/2022	Operational for Medicaid until January 1, 2022; Supports Coordination of Care through Patient Engagement Objective

Summary 2015 Edition Cures Update (modified from Table 1 of the final rule)				
Certification Criterion	**Reference**	**Change Type**	**Change Timing**	**Impact CMS PI Programs**
Transmission to public health agencies electronic case reporting	§170.315(f)(5)	Revised	Update to USCDI/C-CDA companion IG w/in 24 months after rule published	PI Measure: Electronic Case Reporting
CCDA creation performance	§170.315(g)(6)	Revised	Update to USCDI/C-CDA companion IG w/in 24 months after rule published	No impact described by ONC
Application Access – Data Category Request	§170.315(g)(8)	Time-limited	Available for 24 months after final rule publication	PI Measure: Provide Patients Electronic Access to Their Health Information
Application Access - All Data Request	§170.315(g)(9)	Revised	Update to USCDI/C-CDA companion IG w/in 24 months after rule published	PI Measure: Provide Patients Electronic Access to Their Health Information
Standardized API for patient and population services	§170.315(g)(10)	New	Update w/in 24 mo of final rule publication	Added to the 2015 Edition Base EHR definition
Note: The CHPL will be updated to indicate the standards utilized for new or revised certification criteria, as well as denote criteria removed from the Program				

IV. Modifications to the ONC Health IT Certification Program

A. Corrections and Other Updates

ONC proposed several clarifications, corrections, and codification of previously issued guidance:

- Codifying guidance about exemptions from the "end-user device encryption" criterion applicable to the "auditable events and tamper resistance" criterion (§170.55(h)(3);
  - The change would permit certification for an audit log process to proceed without the associated health IT module demonstrating the ability to record an encryption status;
- Codifying guidance that stops the erroneous application of the "amendments" criterion to clinical category criteria that lack patient data for which an amendments request would be relevant (e.g., patient specific education) (§170.315(h); and
- Removing a cross-reference (§170.315(e)(1)(ii)(B)) that references testing that is no longer a part of certifying to the "view, download, and transmit to 3rd party" criterion.

No comments specific to these changes were received and they are finalized as proposed. ONC also proposed to revise the 2015 Edition P&S Certification Framework, primarily to reflect that nearly all certification criteria would be subject to the two new proposed criteria "encrypt authentication credentials" and "multi-factor authentication", as shown in Table 1 of the proposed rule (84 FR 7455). No comments specific to this proposal were received. ONC finalizes the proposed changes with minor modifications that reflect the final actions taken throughout the final rule relevant to the various P&S framework criteria. The finalized framework is provided in Table 2 of the final rule and reproduced below.

B. Principles of Proper Conduct (PoPC)

1. ONC-Authorized Certifying Bodies

Records retention (§170.523(g)). ONC proposed to revise for increased clarity the records retention requirement for ONC-ACBs. ONC-ACBs would be required to retain their records for the "life of the edition" and for at least 3 years thereafter. The life of the edition would begin with the codification of an edition of certification criteria in the CFR and would extend through a minimum of 3 years from the effective date of the final rule removing that edition from the CFR. Similarly, ONC-ACBs also would be required to make records available to HHS upon request during the entire retention period (life of the edition plus 3 years). Commenters were supportive and ONC finalizes the changes as proposed.

Conformance methods (§170.523(h)). The existing PoPC specifies that ONC-ACBs may certify only health IT first tested by ONC-ATLs whose tools and test procedures have been approved by the National Coordinator. ONC proposed to revise the PoPC to reflect the following changes:

1) Permit the ONC-ACBs to evaluate and certify health IT modules that have not first passed through an ONC-ATL for conformance with certification criteria; and

2) Methods to determine conformity would require advance approval by the National Coordinator and range from testing with an ONC-ATL to developer self-declaration.

Commenters were mostly supportive of the flexibility offered to ONC-ACBs and of the requirement for advance approval of conformance testing methods, and ONC finalizes these proposals. ONC states that the process now used for alternative test methods will be applied to all future non-governmental-developed conformance methods that are submitted to the National Coordinator for approval, referencing the process published at 76 FR 1280. Approved conformance methods will be added to the ONC web site after notices of their availability are published in the Federal Register. ONC states a belief that all certification criteria will continue to have some method of holding their developers responsible for ensuring conformity.

In the proposed rule, ONC noted that certification of "Complete EHRs" would no longer be possible if the proposed removal of the 2014 Edition from the CFR was finalized. As noted in section II.B of this summary, ONC is finalizing the 2014 Edition removal, thereby eliminating complete EHR certification (§170.523(k)). ONC also had proposed to delete the gap certification provision that allowed for the certification of health IT previously certified to an edition if the certification criterion (or criteria) to which the Health IT Module(s) was previously certified had not undergone interval change(s). As all of the 2015 Edition criteria have undergone changes since their initial certifications, this provision is no longer functional, and thus ONC finalizes deleting the gap provision. ONC notes that ONC-ACBs do have discretion and processes to evaluate updates made to previously certified health IT and to allow for conforming updates to be made without additional testing. Finally, ONC notes that test results from testing laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) can no longer be used by ONC-ACBs for determining conformance, since the regulatory transition period from NVLAP-accredited labs to ONC-ATLs has expired.

Acceptable Test Results. ONC proposed to require ONC-ACBs to accept results of testing from any ONC-ATL in good standing and compliant with International Standards Organization (ISO) standard 17025 requirements[18] because all ONC-ATLs are held to a single set of standards. Further, ONC-ACBs can share any concerns about a specific ONC-ATL's results with ONC and a final determination about acceptability of the results would be rendered by ONC for each case. Having received supportive comments, ONC finalizes this PoPC proposal at §170.523(r).

Mandatory Disclosures and Certifications. ONC proposed to revise the PoPC to include a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities, whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification (§170.523(k)). Commenters strongly supported this proposal, though one concern was raised about unintended effects on market pricing. ONC finalizes the proposal, noting that the disclosure applies to types of costs or fees rather than amounts. ONC also proposed removing a provision addressing

[18]This is the primary ISO standard used by testing and calibration laboratories in most countries and is available for purchase from the ISO.

certification of pre-coordinated, integrated health IT module bundles; such bundles are no longer certifiable under the Program. Absent comments, ONC finalizes the change (§170.523(k)(3)). (ONC-ACB PoPCs for real world testing are addressed in section VII.B.5.l of the rule.)

2. ONC-Authorized Testing Laboratories

ONC proposed changes to the records retention requirements for ONC-ATLs that parallel those proposed for ONC-ACBs (i.e., related to "life of the edition" plus 3 years, discussed above. Absent comments, ONC finalizes the changes as proposed (§170.524(f)).

V. Health IT for the Care Continuum

A. Health IT for the Pediatric Setting

Section 4001 (b)(iii) of the Cures Act directed the Secretary to make recommendations and adopt certification criteria in support of the voluntary certification of health IT for the care of children. ONC proposed to fulfill the statutory mandate by addressing pediatric HIT in the context of ONC's overall health IT certification program (the Program) rather than as a separate but parallel voluntary HIT framework or as a specified "track" or "pathway" within the Program. After reviewing available resources (e.g., the Children's Model EHR Format [19]) and conferring with stakeholders (e.g., American Academy of Pediatrics), ONC proposed 10 recommendations for the structure and content of a voluntary certification program embedded within ONC's Program. Additionally, ONC identified multiple existing and proposed 2015 Edition certification criteria potentially applicable to pediatric health IT. Finally, ONC solicited structured input, using technical worksheets linking the recommendations to the certification criteria,[20] as well as unstructured comments about whether the recommendations, criteria, and ONC's overall strategic approach would provide an appropriate framework for voluntary pediatric health IT development and certification.

1. Recommendations for the Voluntary Certification of Pediatric Health IT

Most commenters were supportive of the 10 recommendations, regarding them as an initial step along a path to fully interoperable health IT that facilitates the care of children. Questions were raised and suggestions made about various aspects of implementing the recommendations. ONC responds that it is exploring options for non-regulatory informational resources on effective pediatric health IT implementation and directs stakeholders to ONC's pediatrics health IT webpage (www.healthIT.gov/pediatrics) for information on future activities. In response to a query, ONC specifically states that adding a separate tag functionality on the CHPL to identify a product as supporting pediatric care is not planned. ONC also agrees with a commenter that pediatric-focused testing of health IT modules by developers would be valuable, support patient

[19] Portions of the Children's Format are available at https://ushik.ahrq.gov/mdr/portals/cehrf?system=cehrf.
[20] The technical worksheets were provided as an Appendix to the proposed rule.

safety, and be consistent with the real world testing condition of certification and maintenance requirements (section VII.B.5 of the rule).

ONC finalizes the 10 recommendations for voluntary certification of health IT for pediatric care as proposed, shown below.

1) Use biometric-specific norms for growth curves and support growth charts for children;
2) Compute weight-based drug dosage;
3) Ability to document all guardians and caregivers;
4) Segmented access to information;
5) Synchronize immunization histories with registries;
6) Age- and weight- specific single-dose range checking;
7) Transferrable access authority;
8) Associate maternal health information and demographics with newborn;
9) Track incomplete preventative care opportunities; and
10) Flag special health care needs.

2. Certification Criteria and Standards for Pediatric Health IT

ONC identified multiple 2015 Edition certification criteria potentially applicable to the IT needs of pediatric health care providers and their patients and families (84 FR 7459-7461). One concern raised by commenters is a requirement in the NCPDP SCRIPT Standard Version 2017071 Implementation Guide for including the most recent patient height, weight, and the date of measurement when submitting all new and renewal prescriptions for patients 18 years of age or younger. Although the requirement is intended to improve accurate dosing and pediatric patient safety, there are circumstances in which the measurements are not necessary for appropriate dosing. ONC states that this requirement needs refinement, and until such occurs, ONC instead recommends that vital signs be included in all electronic prescriptions for all patient populations when available and where applicable.

The final list of certification criteria and standards that support health IT for the care of children is shown below and reflects criteria as they have been finalized in section IV of the rule. (The full discussion of comments and ONC responses specific to each new and revised criterion for use with patients of any age can also be found in Section IV of the rule.)

<u>New criteria as finalized</u>

1) "Standardized API for patient and population services" (§170.315(g)(10)
   Provides for the use of application programing interfaces (API) to facilitate access, exchange, and use of EHI "without special effort" as required by the Cures Act
2) USCDI standard (§170.213)
   Replaces the prior CCDS standard under which pediatric vital signs were optional. Under the USCDI standard, the following Data Elements are included in the Vital Signs Data Class: head occipital-frontal circumference percentile (Birth to 36 Months); weight-for-length percentile (Birth to 36 Months); body mass index (BMI) percentile (2-20 Years of

Age); and the reference range/scale or growth curve, as appropriate. The USCDI represents the *minimum* data set for which interoperable exchange is required.

3) "Electronic Prescribing" §170.315(b)(3))
   New standard implemented. The NCPDP SCRIPT 10.6 standard is replaced by the NCPDP 2010771 standard; the latter is more readily configured for pediatric dosing.

Revised criteria as finalized

4) "Security tags – Summary of Care (send)" and Security tags -Summary of Care (receive)" (§170.315(b)(7) and (b)(8))
   Formerly specified as "DS4P-send" and "DS4P-receive". Support security tagging at the document, section, and entry level rather than only at the document level, potentially allowing more granular electronic segmentation of sensitive information items such as adoption or child abuse history. (A related proposal for a new criterion Consent management for APIs" (§170.315(g)(11)) based upon SAMHSA's "Consent2Share" application was not finalized.)
5) "Transitions of care" (§170.315(b)(1))
   Revised to reference the USCDI standard
6) "View, download, and transmit to 3rd party" (VDT) (§170.315(e)(1))
   Transferrable access authority allows data access by patient representatives (e.g. parents)
   Technical revision to delete an obsolete cross reference (§170.315(e)(1)(ii)(B))

Existing criteria unchanged by the final rule

7) "Care plan" (§170.315(b)(9)
8) "Clinical decision support" (CDS) (§170.315(a)(9))
9) "Demographics" (§170.315(a)(5))
10) "Family health history" (§170.315(a)(12))
11) "Patient health information capture" (§170.315(e)(3))
    Facilitates documentation of decision-making authority of patient representative(s) e.g., guardian)
12) "Social, psychological, and behavioral data" (§170.315(a)(15))
13) "Transmission to immunization registries" (§170.315(f)(1))
    Links immunization data with registries, facilitating discussions about upcoming immunizations that are based on evidence-based national guidelines

B. Health IT for Opioid Use Disorder (OUD) Prevention and Treatment – Request for Information

Through a request for information in the proposed rule (84 FR 7461-7465), ONC sought input as to how health IT might contribute across the healthcare continuum to the national effort to combat the opioid epidemic. ONC acknowledges receiving over 100 comments and input from the Health Information Technology Advisory Committee (HITAC) and states that the feedback will be shared with other appropriate HHS Department partners.

VI. Conditions and Maintenance of Certification

Under section 3001(c)(5)(d) of the Public Health Service Act, as added by 4002 of the Cures Act, the Secretary must establish Conditions and Maintenance of Certification requirements for health IT developers participating in the ONC Health IT Certification Program. ONC finalizes new requirements in this section of the rule; they involve information blocking; appropriate exchange, access, and use of EHI; communications regarding health IT; APIs; real world testing for interoperability; attestations regarding certain requirements and submission of reporting criteria under the EHR reporting program.

A. Implementation

ONC finalizes its proposal to implement this Cures Act requirement using an approach under which the Conditions and Maintenance of Certification expresses both initial and ongoing requirements for health IT developers and their certified health IT Modules under the Program. Maintenance of Certification requirements for each Condition of Certification are finalized as standalone requirements. ONC believes that this approach establishes clear baseline technical and behavior conditions with evidence that the conditions are continually being met through the maintenance requirements.

Under the final rule, if these requirements are not met, the health IT developer may no longer participate in the Program and/or its certification may be terminated.

ONC clarifies that, except for the information blocking requirements and assurances, the requirements finalized in this section and discussed below apply only to actions and behaviors of HIT developers with respect to certified health IT; for information blocking requirements and assurances, the developer is responsible for ensuring that all of its health IT and related actions and behavior do not constitute information blocking (section VII below).

B. Provisions

The Conditions and Maintenance of Certification requirements finalized in this rule are set forth in regulatory text in 45 CFR Part 170 in a new Subpart D, including sections 170.400 through 170.406.

1. Information Blocking (§170.401)

(a) *Condition of Certification*. A health IT developer must not take any action that constitutes information blocking as defined in section 3022(a) of the PHS Act. Section VII below summarizes the final requirements for implementing the information blocking provisions of the Cures Act. ONC notes that the HHS Office of the Inspector General (OIG) has investigatory and enforcement authority over information blocking. Enforcement is discussed in section VI.D below.

(b) *Maintenance of Certification*. No Maintenance of Certification requirements are adopted for this condition.

This requirement is effective 6 months after publication of this final rule.

2. Assurances (§170.402)

(a) *Condition of Certification*. (1) A health IT developer must satisfy the Secretary that it will not take any action that constitutes information blocking unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information. Legitimate purposes specified by the Secretary are the exceptions to the information blocking definition as discussed in section VII.

(2) A health IT developer must ensure that its health IT certified under the Program conforms to the full scope of the certification criteria. Recognizing that this has always been its expectation as well as a Program requirement, ONC believes that incorporating this into the certification conditions will result in assurances and documentation that IT developers understand their responsibilities under the Program.

(3) A health IT developer would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. Again, while these actions are already prohibited ONC believes including this as a condition would ensure that health IT developers attest to them on a regular basis. (See section VI.B.6 below for a discussion of the attestation requirements.) ONC offers examples of actions that would violate the condition including failing to fully deploy or enable certified capabilities; imposing limits on the use of certified capabilities; requiring subsequent developer assistance to enable the use of certified capabilities contrary to their intended uses; refusal by a developer to provide documentation, support or other reasonable assistance; or imposing additional types of costs, especially if not disclosed at purchase of the certified health IT.

(4) A health IT developer that manages electronic health information must certify health IT criterion in §170.315(b)(10) regarding electronic health information export. (This EHI export criterion is discussed in section III.C.6 above.) For the maintenance of certification requirements, a health IT developer must provide all its customers of certified health IT with IT certified to the EHI export criterion within 36 months of the final rule's effective date. ONC modified the time frame from the proposed rule, which was generally 24 months, but provided for a timeframe of 12 months after initial certification to the 2015 Edition if longer. ONC believes the 36-month timeframe is enough and that new IT developers will understand the requirements in this final rule. Finally, under §170.550(g) an ONC-ACB must certify health IT to the 2015 Edition EHI export criterion when a developer presents for certification a Health IT Module that can store EHI.

(b) *Maintenance of certification.* In addition to the maintenance requirement pertaining to the EHI export described immediately above, another finalized maintenance of certification requirement pertains to record retention. Specifically, a health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the Program for a period of 10 years beginning from the date of initial certification under the Program. This applies separately to each unique Health IT Module (or Complete EHR) certified under the Program. ONC believes that 10 years is an appropriate period because it aligns with various CMS programs that many users of certified health IT participate in. (Section VI.D below includes more discussion of records access.) The final rule provides that if applicable certification criteria are removed from the CFR before the 10 years have expired, records only have to be kept for 3 years from the date of removal, unless the timeframe would exceed the overall 10-year retention period. This provision aligns with other records retention requirements for ONC-ACBs and ONC-ATLs under the Program.

Request for Comment on the Trusted Exchange Framework and Common Agreement (TEFCA)

The proposed rule include a request for comment on whether certain health IT developers should be required to participate in the TEFCA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. ONC received 40 comments and will take these into consideration for future rulemaking.

3. Communication (§170.403)

In this section ONC adopts a condition of certification to implement Cures Act requirements barring a health IT developer from prohibiting or restricting certain protected communications. ONC finalizes a broad general rule with specific narrow exceptions. Some changes, as noted, are made from the proposed rule. One is the addition of a definition for the term communication as "any communication, irrespective of the form or medium and includes visual communications, such as screenshots and video." As noted earlier, the communications protections apply only to actions and behaviors of HIT developers with respect to certified health IT.

ONC's aim with these provisions is to significantly improve transparency about the functioning of health IT in the field. It reviews the history of concerns about industry practices that limit consumer knowledge about the functionality of health IT due to contract language regarding nondisclosure, confidentiality, intellectual property protection and other provisions. Among concerns are inhibition of communication of information on errors and adverse events and other information relevant to safety and interoperability.

This Condition of Certification is not limited to formal prohibitions or restrictions (i.e., contracts or agreements) but also encompasses any conduct by a developer that is likely to restrict a communication protected by the condition. ONC notes that contracts do not have to expressly prohibit a protected communication in order to have the effect of prohibiting or restricting a protected communication. Non-disclosure agreements and restrictions that "flow down" to a

customer's employees or others that work with the developers IT would not comply with the condition. Conduct by the IT developer that has the effect of restricting protected communication is subject to the condition if there is a nexus between the conduct and the making of (or attempt at making) of protected communication.

Examples of the types of protected communications that were described in the preamble of the proposed rule include: a post made to an online forum; the sharing of screenshots, subject to certain proposed restrictions on their general publication; an unattributed written review by a health IT user; a quote given by a health care executive to a journalist; a presentation given at a trade show; a social media post; a product review posted on a video-sharing service such as YouTube; statements and conclusions made in a peer-reviewed journal; and private communications made between health IT customers about the health IT.

The specific requirements for the condition and maintenance of certification are described in items (a) and (b) respectively.

(a) *Condition of Certification*. (1) A health IT developer may not prohibit or restrict the communication regarding—

- The usability of its health IT

ONC notes that 'usability' is not defined in statute but discusses external definitions and identifies a series of usability factors that could be the subject of protected communication including the user interface; ease of use; how the technology supports user workflows; the organization of information; cognitive burden; cognitive support; error tolerance; clinical decision support; alerts; error handling; customizability; use of templates; mandatory data elements; the use of text fields; and customer support.

- The interoperability of its health IT

This protects communications about whether a health IT product and developer's business practices meet the PHS Act definition of interoperability, including communications about IT capabilities and developer practices that may inhibit the access, exchange or use of EHI, including information blocking.

- The security of its health IT

Health security is broadly construed to include any safeguards employed by a developer, whether or not required by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, to ensure the confidentiality, integrity and security of EHI as well as the developer's performance regarding security. ONC says that under the final rule a developer may not prohibit or restrict communication about the approach to security adopted for the health IT; the resilience of the health IT; identified security flaws; or the developer's response to cyber threats or security breaches. Responding to a comment, ONC notes that developers may use appropriate legal remedies to address communications of concern.

- Relevant information regarding users' experiences when using its health IT

ONC adopts an ordinary meaning of the term "user experience" as an experience had by a user of health IT.

- The business practices of developers of health IT related to exchanging electronic health information

For this provision, protected communications include the costs charged by a developer for products or services that support the exchange of EHI, (such as interface costs, API licensing fees and royalties, subscription and maintenance fees, or transaction-based costs for information exchange); timeframes and terms on which developers will (or not) enable connections (or not) and facilitate exchange; the developer's approach to participation in health information exchanges or networks; the developer's licensing practices related to making APIs and other aspects of its technology enabling interoperability available; and the developer's approach to creating interfaces with third-party products or services.

- The manner in which a user of the health IT has used such technology

This includes information about work-arounds; customizations; constraints imposed on IT functionality due to implementation decisions; and information about the ways in which health IT could not be used or did not function as represented by the developer.

Unqualified protection for certain communications. The final rule provides that a health IT developer *may not* prohibit or restrict communication of any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters identified in (a)(1) above and it is made for any of the following purposes—

- Making a disclosure required by law;
- Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;
- Communicating information about cybersecurity threats and incidents to government agencies;
- Communicating about information blocking and other unlawful practices to government agencies; or
- Communicating information about a health IT developer's failure to comply with a condition of certification or another requirement to ONC or an ONC-ACB.

ONC clarifies that known vulnerabilities and IT defects would likely be considered types of events and conditions to which this protection would apply; however, vulnerabilities and defects that are not already public knowledge would be a non-user-facing aspect of IT for which developers may restrict communication as discussed below. ONC expects IT developers to share information about vulnerabilities with health care providers and other users as soon as feasible.

Permitted prohibitions and restrictions. For communications about one or more of the subject matters enumerated in (a)(1) above that are not entitled to unqualified protection, a health IT developer may prohibit or restrict communications only as expressly permitted in the list below. Any prohibition or restriction not expressly permitted violates the condition of certification. A developer choosing to avail itself of a permitted type of communication prohibition or restriction must ensure that potential communicators are notified about what

information can and cannot be communicated. ONC admonishes that associated contract language should be precise and specific.

Under the final rule a health IT developer *may* prohibit or restrict the following communications:

- Communications of its employees or contractors, except that a health IT developer may not prohibit or restrict communications of users of their health IT that are also employees or contractors.

ONC modified this provision from the proposed rule to clarify that a self-developer of certified health IT may not prohibit communications of users who are also employees. For example, a health system with a self-developed EHR may not restrict providers who are users and also employees of the system from communicating about the EHR as a user.

- Communications that disclose information about non-user-facing aspects of the developer's health IT.

Non-user facing aspects of health IT include source and object code, software documentation, design specifications, flowcharts, and file and data formats. ONC clarifies that it also includes underlying software that is utilized by the health IT in the background and not directly by a user of the health IT, algorithms that are not readily apparent to persons using health IT, and documentation for back-end components.

- Communications that infringe on the intellectual property rights of the developer's health IT (including third-party rights), provided that any prohibition or restriction imposed by a developer must be no broader than necessary to protect the developer's legitimate intellectual property interests and consistent with all other requirements for permitted prohibitions and restrictions on communication. A restriction or prohibition is deemed broader than necessary and inconsistent with the permitted prohibitions and restrictions if it would restrict or preclude a public display of a portion of a work subject to copyright protection (without regard to whether the copyright is registered) that would reasonably constitute a "fair use" of that work.

This language is changed from the proposed rule in response to commenters seeking clarification.

- Communications that are screenshots or videos may be restricted so that the IT developer may require the communicator to (1) not alter them except to resize or annotate; (2) limit the share of screenshots to the relevant number needed to communicate about the health IT regarding one or more of the six subjects enumerated in the statute and in (a)(1) above.

This language is changed from the proposed rule to include videos as well as screenshots, to permit developers to limit the sharing of screenshots and video to a number or length needed to communicate and clarify that the subject of the communication must be one of those enumerated in the condition of certification. In addition, to be protected videos must convey matters that cannot be communicated through screenshots or other means. ONC intends to balance protections for developer IP with the need to allow communication about health IT issues within the six subject areas. ONC does not finalize proposed language that would have allowed IT developers to restrict communications or screenshots that contain personal health information because it believes that most of those communicating the screenshots would be bound by HIPAA and state privacy laws.

- Communications that disclose information or knowledge acquired only through participation in developer-led product development and testing. This permission does not apply to communications about the released version if it otherwise meets the requirements under this condition of certification and the information communicated could be discovered by any ordinary user of the health IT.

(b) The maintenance of certification requirements are as follows:

- Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene this condition of certification stating that any communication or contract provision that contravenes this condition will not be enforced by the developer. The notice must be provided annually beginning in 2020 and until the developer has amended the contract to remove or void the offending language.
- The developer may not establish, renew or enforce any contract or agreement that contravenes this condition, and any contract in existence as of 60 days after publication of this final rule must be amended to remove or void the language whenever the contract is next modified for other reasons or renewed. ONC clarifies that in the case of a contract that auto-renews, the developer is still prohibited from enforcing any contravening provisions and is responsible for sending annual notices until the provisions are modified.

The timeframes for the notice and amendments to the contracts are modified from the proposed rule. ONC believes the final language simplified the compliance for health IT developers while providing adequate notice. ONC emphasizes that effective with publication of the final rule contravening provisions of contracts and agreements cannot be enforced without the IT developer risking loss of certification for the health IT or a certification ban for the developer under the Program. This is the case whether or not the notification requirement is met.

4. Conditions and Maintenance of Certification: Application Programming Interfaces (§170.404)

By ONC's description, APIs can be thought of as a set of commands, functions, protocols, or tools published by one software developer ("A") that enables other software developers to create programs and applications that interact with A's software without needing to know the internal workings of A's software. ONC previously adopted three 2015 Edition certification criteria that specify API capabilities for Health IT Modules (45 CFR 170.315(g)(7), (g)(8), and (g)(9)).

In this rule, ONC finalizes technical standards and implementation specifications along with a new API certification criterion to implement the requirements associated with the Cures Act's API Condition of Certification.

<u>New Standards and Implementation Specifications for APIs</u>

As a Condition of Certification (and Maintenance thereof) under the Program, the Cures Act requires health IT developers to publish APIs that allow "health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law." In addition, a

developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws." The term "without special effort" is interpreted by ONC to mean standardized, transparent, and pro-competitive.

New API standards at 45 CFR 170.215

ONC finalizes addition of a new 45 CFR 170.215 with the following technical standards and associated implementation specifications for APIs. Throughout the preamble ONC discusses and responds to comments on technical issues pertaining to these standards that are not included in this summary.

Adoption of FHIR Standard. ONC adopts at 170.215(a)(1) the HL7® Fast Healthcare Interoperability Resources (FHIR®) Release 4.0.1 as the foundational standard. Developers seeking certification must build, test, and certify systems solely to FHIR Release 4.0.1 and its associated implementation specifications. This is the most recent release available at the time the final rule was issued. ONC had proposed adoption of FHIR Release 2 but sought comment on adoption of FHIR Release 4 because it is the most advanced and will allow the industry to coalesce around a single baseline standard rather than accommodating multiple releases while ultimately moving to Release 4.

ONC does not finalize its proposal to adopt API Resource Collection in Health (ARCH) Version 1. Most commenters opposed this proposal in favor of other standards, and ONC ultimately determined that having an implementation specification to map USCDI to HL7 FHIR could create more restrictions than it intended. It further determined the linkage of the USCDI Data Elements to FHIR Resources can be accomplished without the ARCH.

In finalizing adoption of FHIR Release 4.0.1, ONC also modifies related provisions from the proposed rule and adopts implementation specifications and FHIR profiles that support USCDI) data access. (FHIR profiles are additional rules about which elements must be used and which have been added that are not part of the base FHIR resource,) Specifically, ONC adopts the following implementation specifications:

- HL7 FHIR US Core Implementation Guide STU 3.1.0 (US Core IG), the latest version at the time of the final rule publication. The US Core IG defines the minimum conformance requirements for accessing patient data using FHIR Release 4, including profiled resources, operations, and search parameters for the USCDI Data Elements.
- HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for "SMART on FHIR Core Capabilities,[21]" which ONC specifies as mandatory because these capabilities are indicated as optional in the implementation specification. As mandatory elements, The SMART on FHIR Core Capabilities are subject to testing and certification. ONC notes that Health IT Modules

[21] The final regulatory text at 170.215(a)(3) references "SMART Core Capabilities" but the preamble clearly discusses "SMART on FHIR Core Capabilities" as the policy adopted.

presented for testing and certification must include the ability for patients to authorize access to their EHI at the individual FHIR resource level, giving patients increased control over how much EHI they authorize applications of their choice to receive. For example, if a patient downloaded a medication management application, they would be able to use these authorization scopes to limit the EHI accessible by the application to only information contained in FHIR "MedicationRequest" and "Medication" profile. HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0 is a profile of the OAuth 2.0 specification, and ONC responds to comments regarding security threats such as cross-site request forgery (CSRF) by encouraging implementers to adhere to best practices to mitigate these threats.

- HL7 FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1) implementation specification (Bulk IG), which includes the "Backend Services Authorization Guide" in § 170.215(a)(4) for backend services authorization.
- Open ID Connect Core 1.0 including errata set 1. ONC clarifies that only the relevant parts of the OpenID Connect Core 1.0 including errata set 1 adopted in §170.215(b) that are also included in the implementation specification adopted in §170.215(a)(3) will be in-scope for testing and certification.

New API Certification Criteria at 45 CFR 170.315(g)(10)

ONC adopts new API certification criterion at §170.315(g)(10) to replace the existing criterion set forth at §170.315(g)(8), and the definition of the 2015 Based Edition is modified to reflect this change. Current requirements at (g)(7) and (g)(9) remain unchanged because they do not prescribe specific technical approaches that need to be replaced. The new criterion at (g)(10) will be required beginning 24 months after publication of the final rule. Until then, (g)(8) will continue to be applicable during the transition period for 24 months after publication of the final rule.

Under the Standardized API for patient and population services Condition of Certification criterion proposed at §170.315(g)(10), API technology must meet the following technical outcomes and conditions for certification.

Data response. The technology must be able to respond to requests for data on a single patient and for multiple patients (in accordance with the new standards at 170.215 described above) for each of the data elements included in the USCDI. This new API certification criterion requires Health IT Modules to support API-enabled "read" services for single and multiple patients. "Write" services are specifically excluded; ONC believes that write services have not reached a level of maturity to warrant addition to the regulatory requirements for certification. ONC clarifies that "read" services for multiple patients are not intended for individual patient end users. ONC also notes that the standards of API-related Health IT Modules presented for certification themselves do not compel health care providers to implement these features, although other CMS programs may do so. Readers are referred to the information blocking section below for further clarification.

Search support. The technology must be able to respond to search requests for a single patient's data consistent with the search criteria included in the HL7 US Core IG implementation specification at 170.215(a)(2), specifically the mandatory capabilities described in "US Core Server Capability Statement," and for search requests for data on multiple patients consistent with the search criteria included in the Bulk IG implementation specification adopted in §170.215(a)(4).

App registration. The technology must be capable of enabling apps to register with the technology's "authorization server." The Certified API Developer must demonstrate its registration process, but ONC does not require that it be done according to a specific standard because it believes that Certified API Developers and Information Sources are best poised to innovate and execute various methods for app registration within a clinical environment.

Secure connection. The technology must demonstrate capability to establish a secure and trusted connection with an application that requests data in accordance with the HL7 US Core IG implementation specification at 170.215(a)(2) for a single patient and with the SMART Backend Services Authorization Guide and other specifications at §170.215(a)(4) for multiple patients.

Authentication and app authorization. Requirements for authentication and authorization, which were proposed separately, are combined into new 170.315(g)(10)(v). For patients and users, the first time an application connects to request data, the user authentication and authorization must occur during the process granting access to patient data under the relevant implementation specifications (i.e., the HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0) and the OpenID Connect 1.0 standard. An application capable of storing a client secret must be issued a refresh token valid for at least three months. For subsequent connections, access must be granted without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application, and a new refresh token issued for a new period of at least three months.

Requirements for authentication and authorization for "system scopes" (accessing data on multiple patients) authentication and authorization must occur during the process of granting an application access to patient data in accordance with the "SMART Backend Services: Authorization Guide" section of the implementation specification and the application must be issued a valid access token. ONC notes that for system scopes, applications will likely be authorized via a prior authorization negotiation and agreement between applications and Health IT Modules.

A Health IT Module's authorization server must be able to receive and validate tokens it has issued. No specific standard is finalized with respect to receiving and authorizing tokens. However, the industry is encouraged to coalesce around using specific standard for this purpose, such as OAuth 2.0 Token Introspection. Implementers are expected to have the capability of revoking refresh tokens when appropriate, and they are not prohibited from changing the length of refresh tokens for users, keeping in mind the information blocking provisions.

Finally, a Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction. This will enable patients to definitively revoke an application's authorization to receive their EHI until reauthorized, if ever, by the patient.

Technical documentation. In new §170.315(g)(10)(viii) an API must include complete accompanying documentation including at a minimum:

- API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
- The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
- All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

ONC also modifies existing documentation requirements at §170.315(g)(7) through (g)(9) and to focus the documentation solely on the technical documentation associated with the API technology, removing provisions associated with "terms of use" which are reflective of business practice.

ONC recognizes that adopting the HL7 FHIR standard will be consistent across Health IT modules and there may be little technical documentation needed beyond what is already documented in adopted standards and implementation specifications. However, any additional documentation that is required must be accessible to the public via a publicly accessible hyperlink without any additional access requirements. Prohibited for example would be requirements for registration, account creation, click-through agreements, or requirements for contact information or other information.

<u>API Condition of Certification Requirements (§170.404)</u>

To implement the Cures Act, ONC adopts API Condition of Certification to complement the technical capabilities set forth above and address the broader technology and business context within which the API will be used. They apply to developers of Health IT Modules certified to any of the criteria under current and proposed §170.315(g)(7) through (10). ONC notes that the policies do not apply to a health IT developer's practices associated with criteria that are not one of the API-focused criteria but says that developers should be mindful that other provisions of the final rule, such as information blocking, could still apply to the non-API-focused certification criteria.

Under definitions finalized at §170.404, an API User creates or uses software applications that interact with certified API technology (i.e., health IT Modules certified to any of the criteria in §§170.315(g)(7) through (10)) created by Certified API Developer (proposed as a API Techno1logy Supplier), and an API Information Source (proposed as the API Data Provider) is the organization that deploys the certified API technology (e.g., a health care provider). ONC

clarifies that an API User may interact with certified API technology directly (to develop third-party apps or services) or indirectly (as a user of a third-party app or service), and includes software developers, patients, health care providers, and payers. A person or entity can serve more than one role, and the role that applies is based on the context in which they are acting.

Condition of Certification. A Certified API Developer must publish APIs and allow health information from APIs to be accessed, exchanged, and used without special effort using APIs or successor technology or standards, as provided under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws. ONC clarifies that for this purpose it assumes that both USCDI and the FHIR implementation specification are included in its interpretation of "all data elements."

Transparency conditions. ONC finalizes that the business and technical documentation published by a Certified API Developer must be complete and published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. The published documentation must include all terms and conditions for the API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

- Develop software applications to interact with the certified API technology;
- Distribute, deploy, and enable the use of software applications in production environments that use the certified API technology;
- Use software applications, including to access, exchange, and use electronic health information by means of the certified API technology;
- Use any electronic health information obtained by means of the certified API technology;
- Verify the authenticity of API Users; and
- Register software applications.

All fees charged by a Certified API Developer for the use of its API technology would have to be described in detailed, plain language. The description of the fees must include all material information, including the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variables and methodologies used to calculate the fee.

ONC expects suppliers to make clear to the public the timing of their disclosures in order to prevent discrepancies between information in its public documentation and what it may be communicating directly to customers. Elsewhere in the final regulations ONC requires Certified API Developers to provide notice and a reasonable opportunity for API Information Sources and API Users to update their applications to preserve compatibility with certified API technology and to comply with applicable terms and conditions. ONC states that notice could include a public notice made available on a website, but also encourages developers to contact customers and registered users directly prior to updating business and technical documentation.

Fees conditions. In general, a Certified API Developer is prohibited from imposing any fees other than certain permitted fees detailed below. The permitted fees may result in a reasonable profit margin consistent with the information blocking costs exception described in §171.302 and discussed in section VII below. ONC states that any fees not meeting that exception would be suspect under the information blocking provision and equally not permitted under this condition of certification requirement.

For any permitted fee, several general requirements apply. First, a Certified API Developer must ensure that the fee was based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of API Information Sources and API Users. Second, the fees imposed on Information Sources need to be reasonably related to the developer's costs of supplying and supporting API technology to the Information Source being charged. Third, the costs of supplying and supporting the API technology upon which the fee is based would have to be reasonably allocated among all the similarly situated information sources. Finally, fees may not be based in any part on whether the Information Source or User is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the Certified API Developer.

Prohibited Fees. Fees are specifically prohibited for costs associated with intangible assets other than for the actual development or acquisition costs of such assets, and opportunity costs unrelated to the access, exchange or use of electronic health information. Further, the permitted fees described below cannot include any costs that led to the creation of intellectual property if the actor charged a royalty for that intellectual property pursuant to the information blocking licensing exception at §171.303 (discussed in section VII below) and that royalty included the development costs for the creation of the intellectual property. This provision was added in response to commenters recommending that developers should not be able to charge an additional license fee for what is an inherent part of the software.

ONC identifies the following examples of prohibited fees:

- Any fee for access to the documentation that a Certified API Developer is required to publish or make available under the Condition of Certification.
- Any fee for access to other types of documentation or information that a software developer may reasonably require to make effective use of API technology for any legally permissible purpose.
- Any fee in connection with any services that would be essential to a developer or other person's ability to develop and commercially distribute production-ready applications that use API technology. These services could include, for example, access to "test environments" and other resources that an app developer would need to efficiently design and develop apps or access to distribution channels necessary to deploy production-ready software and to production resources, such as the information needed to connect to FHIR servers (endpoints) or the ability to dynamically register with an authorization server.

The general prohibition on fees is meant to ensure that API developers do not engage in pricing practices that create barriers to entry and competition for apps that health care providers seek to

use, while the permitted fees are intended to recognize that suppliers need to recover costs and earn a reasonable return for providing certified API technology. ONC discusses practices that it believes close off the market to innovation apps and services that could be beneficial to consumers and providers. For example, some API developers engage in discriminatory pricing with competitors or condition access to technical documentation on revenue sharing or royalty agreements that are unrelated to the costs of providing or enabling use of the API technology.

ONC notes that the certification conditions do not address who may pay a permitted fee charged by a Certified API Developer. For example, an API User or other party may offer to pay a fee owed to a Certified API Developer by the API Information Source. ONC cautions stakeholders to be mindful of other federal and state laws and regulations that could prohibit or limit certain types of relationships involving remuneration.

The following permitted fees are finalized. In addition to satisfying one of the proposed permitted fees, the general conditions described above would apply.

Permitted fee – Development, deployment, and upgrades. A Certified API Developer may charge fees to an API Information Source to recover the costs reasonably incurred by the Certified API Developer to develop, deploy, and upgrade API technology.
ONC states that fees for developing certified API technology may not include the supplier's costs of updating non-API related capabilities, including its databases, because this would be inconsistent with the Cures Act requirement that API technology be deployed "without special effort." Fees for "deploying" API technology comprise supplier's costs of operationalizing API technology in a production environment and include standing up hosting infrastructure, software installation and configuration, and the creation and maintenance of API Information Source administrative functions. These fees would not include the costs associated with managing the traffic of API calls that access the API technology, which a supplier can only recover under the permitted fee for usage support costs described immediately below. For the purpose of this Condition of Certification, ONC considers API technology to be "deployed" by the customer—the API Information Source—that purchased or licensed it. Fees for "upgrading" API technology comprise the supplier's costs of supplying a provider with an updated version of API technology, such as the costs required to bring API technology into conformity with new program requirements, upgrades to implement general software updates (not otherwise covered by development fees or under warranty), or developing and releasing newer versions of the API technology at the request of an API Information Source. Any fees under this category of permitted fees could be charged only to the Information Source(s) for whom the capabilities are deployed. It expects the fees would be negotiated between these parties.

Responding to comments from developers, ONC states that it would be inappropriate for developers to go around the customer (the Information Source) to also charge the user. This would be seen as creating a special effort on users just to be able to connect to the information source's API technology. ONC notes that the value-added services permitted fee allows developers a wide range of options for making additional revenue from their certified API technology.

Permitted fee – recovering API usage costs. A Certified API Developer may charge usage-based fees to an API Information Source to recover the incremental costs reasonably incurred by the developer when hosting API technology on behalf of the Information Source.

While ONC had proposed to exclude from this fee any costs incurred by the Certified API Developer to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information, the final rule does not include that exclusion. ONC determined that these fees are needed for developers to recover the incremental costs reasonably incurred by the developer when hosting API technology on behalf of the Information Source.

In the proposed rule, ONC indicated its expectation that usage support fees would only come into play when the supplier acts on behalf of the provider to deploy the technology. The fees would include incremental costs attributable to supporting API interactions at increasing volumes and scale. ONC expects that suppliers would offer a certain number of "free" API calls and impose the usage-based fee after that threshold was exceeded, on the basis that a certain number of calls would be assumed in the costs recovered for deployment services. Suppliers might charge on a fee-per-call pricing structure, but in this case ONC cautions that the fees paid by the provider would need to be reasonably related to the supplier's costs of proving the technology. Similarly, a flat fee pricing structure would be permitted provided that the fee was reasonably related to the cost of services (i.e., a realistic estimate of the volume of calls). The usage fees could not include any costs associated with preparing to get the technology up and ready for use. A fee to cover these costs would be permitted under the development, deployment, and upgrades fee described immediately above.

Responding to commenters asking ONC to cap usage fees, it declines stating that its focus is to permit this type of fee and not to dictate a specific fee model or interfere with developers' ability to innovate new fee models.

ONC reiterates the general prohibition on fees associated with the access, exchange, and use of EHI by patients. This prohibition is based on the view that fees between a supplier and provider would likely be passed on directly to patients, creating a significant impediment to their ability to access, exchange, and use their EHI, without special effort, through applications and technologies of their choice. ONC also believes that patients have effectively paid for most of the information contained in a patient's electronic record because either directly or through employers, health plans and other third-party payers. ONC notes that any unreasonable fees associated with a patient's access to their EHI may be suspect under the information blocking provision discussed in section VII below, and inconsistent with an individual's right of access to their PHI under the HIPAA Privacy Rule.

In addition, ONC notes that through tax preferences, Medicare and Medicaid programs and other public funds, the development of EHI has been federally subsidized, yet it is not readily available where needed. For this reason, ONC believes that the benefits of publishing certified APIs that

permit access, exchange and use of EHI without special effort outweigh any burdens on API Developers and Information Sources.

Permitted fee – Value-added services. A Certified API Developer may charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.

These value-added services would need to be provided in connection with and supplemental to the development, testing, and deployment of software applications that interact with certified API technology. A fee would only be permitted if it relates to a service that a software developer can elect to purchase but is not required to purchase in order to develop and deploy the software. ONC cautions that the condition of certification would not apply to practices that do not pertain to certified API technology, and developers should be mindful that information blocking rules may apply to app store practices depending on facts and circumstances.

Permitted Fees Record-keeping Requirements. A Certified API Developer would be required to keep for inspection detailed records of any fees charged with respect to the API technology, the methodologies used to calculate such fees, and the specific costs to which such fees are attributed. Responding to comments about the burden of this requirement, ONC says it is difficult to believe that developers are not already keeping these financial records and that the provision would be a substantial new burden. ONC emphasizes the value of transparency and accountability in the Program and the need to mitigate unfair pricing practices.

(4) *Openness and pro-competitive conditions*. *General condition.* A Certified API Developer must grant an API Information Source the independent ability to permit API Users to interact with the API technology deployed by the Information Source.

Responding to a query from commenters on whether an API Information Source can vet third party applications, ONC covers when a HIPAA business associate relationship is required; if an app is developed to create, receive, maintain or electronically transmit PHI on behalf of the Information Source (i.e., a HIPAA covered entity) a business associate agreement is required, and in those cases the Information Source has the ability to conduct whatever vetting it deemed necessary before granting access and use of EHI under the HIPAA Security Rule. However, a business associate relationship is not required for third party applications chosen by an individual to facilitate their access to EHI. Readers are referred to the Information Blocking section for more information regarding the difference between interference and patient education.

- Non-discrimination. A Certified API Developer must provide API technology to API Information Sources on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship. The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. Different terms of service may not be offered based on whether a competitive

relationship exists or would be created or based on the revenue or other value that another party may receive from using the API technology.

- Rights to access and use API technology. A Certified API Developer must have and grant upon request to API Information Sources and their API Users all rights that may be reasonably necessary to (1) access and use API technology in a production environment; (2) develop products and services designed to interreact with the developer's certified API technology; and (3) market, offer and distribute products and services associated with it.
- The Certified API Developer may not condition the rights described above on any of the following:
    - Receiving a license fee, royalty, revenue-sharing arrangement or other fee;
    - Agreeing not to compete with the Certified API Developer on any product service or market;
    - Agreeing to deal exclusively with the Certified API Developer in any product, service, or market;
    - Obtaining additional licenses, products, or services that are unrelated to or can be unbundled from the API technology;
    - Licensing, granting, assigning, or transferring any intellectual property to the Certified API Developer;
    - Meeting additional developer-specific testing or certification requirements; and
    - Providing the Certified API Developer or its technology with reciprocal access to application data.
- Service and support obligations. A Certified API Developer must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of certified API technology by API Information Sources and their API Users in production environments. The following obligations are specified:
    - Changes and updates to certified API technology: A supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of certified API technology in production environments.
    - Changes to terms and conditions: Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions, a supplier must provide notice and a reasonable opportunity for its Information Sources and API Users (its customers) to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

Maintenance of Certification. (1) *Authenticity verification and registration for production use.* A Certified API Developer with health IT Module certified under 170.315(g)(10) may institute a process to verify the authenticity of API Users so long as the process is objective and the same for all users and completed within ten business days after an API User requests to register their software application for use with the developer's (g)(10)-certified health IT module.

A Certified API Developer must register and enable all applications for production use within 5 business days of completing its verification of an application developer's authenticity (as described in the application developer verification provision above). The timeframe is changed from 1 day in the proposed rule.

ONC notes that an Information Source would not be prohibited from showing a warning to patients as part of the patient authorization for an application to receive their EHI from the Information Source. This could include a warning that the application attempting to access the data is untrusted. Warnings to patients are discussed further in the Information Blocking section.

(2) *Service Base URL publication*. A Certified API Developer must publish the service base URLs for all Health IT Modules certified to §170.315(g)(10) that can be used by patients to access their EHI. The service base URLs must be publicly published for all its customers, regardless of whether the modules are centrally managed by the developer or locally deployed by an API Information Source and must be published in a machine-readable format at no charge.

ONC agreed with commenters about the need for a single or multiple publicly available repositories that maintain provider service-base URLs, and it encourages the industry to coalesce around development of such a public resource. ONC notes that in the final rule it narrowed this requirement to (g)(10) certified APIs that can be used by patients to access their EHI,

(3) *Rollout of (g)(10)-Certified APIs.* A Certified API Developer with API technology previously certified to the criterion in §170.315(g)(8) must provide all API Information Sources that have deployed that API technology with API technology certified to the (g)(10) criterion within 24 months after publication of the final rule. In addition, by 6 months after publication a Certified API Developer with modules certified to §170.315(g)(7),(8), or (9) must comply with the condition of certification requirements at §170.404(a), including revisions to their business and technical API documentation, and must make the documentation available via publicly accessible hyperlink that allows a person to access the information without preconditions or additional steps.

ONC responds to commenters seeking a longer roll out time frame by saying that the 24-month timeframe will end about 5 years after enactment of the Cures Act (December 2016); it believes implementation should not be delayed further. Regarding the 6-months deadline for APIs certified to the other criteria to meet the documentation requirement, ONC notes that previously certified modules will have 24 months to transition to (g)(10) certification, so this provides API Information Sources with modules certified to earlier versions with 18 months of updated documentation for these versions. Therefore, ONC believes providing more time for updating documentation for the previous versions would diminish the benefits of the provision.

5. Real World Testing (§170.405)

Condition of Certification

The Cures Act requires health IT developers with modules certified to any one or more of certain 2015 Edition certification criteria (limited to those in §170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10)), and (h) must successfully test the real world use of the modules for interoperability in the type of setting in which that technology is marketed; this requirement is imposed as a Condition and Maintenance of Certification. As a related matter, ONC codifies the Cures Act definition of interoperability.[22]

Maintenance of Certification

The final rule provides for real world testing for maintenance of certification only; it does not mandate testing the real world use of a Health IT Model in actual production environments before it is certified.

For purposes of the Maintenance of Certification, a developer must submit to its ONC-ACB an annual real world testing plan by a date determined by the ONC-ACB that allows it to make publicly available a hyperlink to the plan in the Certified Health IT Product List (CHPL) no later than December 15 each year. The plan must be approved by a representative of the developer, whose contact information is provided, who is authorized to bind the developer to execution of the plan. The plan must include all IT subject to this requirement that is certified by August 31 of the year of plan submission and must address the real world testing plan for the coming calendar year.

For each certification criterion, a testing plan must address each of the following:

- The testing method that would be used to demonstrate real world interoperability and conformance to the certification criteria's requirements, including scenario and use case-focused testing.
- The care setting(s) that will be tested for real world interoperability and an explanation for the developer's choice of care setting(s) to test.
- The timeline and plans for any voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.
- A schedule of key real world testing milestones.
- A description of the expected outcomes of real world testing.

[22] Section 3000(10) of the PHS Act, as added by section 4003(a) of the Cures Act, defines interoperability, with respect to health IT, as health IT that enables the secure exchange of EHI with, and use of EHI from, other health IT without special effort on the part of the user; allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; **and** does not constitute information blocking.

- At least one measurement or metric associated with the real world testing.
- A justification for the developer's real world testing approach.

The developer must report any non-conformities identified during the conduct of real world testing to the ONC-ACB within 30 days. A report on real world testing must be provided by a date determined by the ONC-ACB that enables it to publish a report on CHPL no later than March 15 each calendar year. ONC notes that the ONC-ACB will assess whether the plans and reports meet the requirements of the certification criteria, but otherwise is not formally evaluating the testing approach for its quality. However, testing results and reports of nonconformities may be used by the ONC-ACB as part of its ongoing surveillance of certified health IT. ONC does not finalize its proposal to allow a developer to have its ONC-ARB oversee the execution of its real world testing plan because it does not believe this is the most effective or least burdensome approach and may slow development of more innovative approaches.

ONC clarifies the timeline for the first effective year. It had proposed that 2020 be a pilot testing year but given the timing of the publication of the final rule it does not believe a pilot year is needed. The initial real world testing plans for 2021 will be published via publicly accessible hyperlink on CHPL by December 15, 2020. These plans will be executed in 2021 and the report on testing results will be published in the CHPL by March 15, 2022. ONC further notes that while it does not specify a deadline for ONC-ACBs to require submission of the testing result for the March 15th publication, it suggests that ONC-ACBs consider the merits of allowing at least one calendar month between submission and publication.

The final rule does not finalize language from the proposed rule requiring that the initial submission of the plan to the ONC-ACB be done via a publicly accessible hyperlink; while this may be the most efficient method, ONC does not want to unnecessarily limit the manner of submission. Further, the plan will be publicly posted by the ONC-ACB by December 15th each year.

The ONC finalizes that a test server may be used for real world testing; synthetic data may also be used in lieu of or in addition to real patient data. However, the testing plan must include an explanation justifying how the testing plan is appropriate to meet real world environments. ONC believes that it has provided flexibility to developers in designing real world testing approaches that minimize burden and optimize the value of testing to current and prospective customers. Developers are encouraged to innovate to these ends. ONC notes that nothing in this certification criteria would prohibit a developer from compensating customers for participating in real world testing, although it reminds readers that there may be other laws and regulations that apply. Readers are referred to the HHS Office of Inspector General advisory opinion process as a source of meaningful advice about the applicability of the anti-kickback statute or other statutes to specific facts.

In the annual testing report, the developer must provide the following information for each certification criterion:

- The method used to demonstrate real world interoperability.
- The care setting that was tested for real world interoperability.
- The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.
- A list of the key milestones met during real world testing.
- The outcomes of real world testing, including a description of any challenges encountered during real world testing.
- At least one measurement or metric associated with the testing.

ONC clarifies that even if a developer does not have customers or has not deployed its certified Health IT Module at the time the real world testing plan is due, the developer would still need to submit a plan that addresses its prospective testing for the coming year for any health IT certified prior to August 31 of the preceding calendar year.

In addition, ONC clarifies that a developer with multiple products listed in the CHPL that include one or more modules certified to the interoperability criteria affected by this provision need only submit one real world testing plan and one results report. However, the plan and results report must address each of the developer's products listed in the CHPL.

Responding to comments, ONC declines to provide specific "one size fits all" testing tools, and notes that the ONC-ACBs will be assessing the real world testing plans for completeness and not assessing the testing methods. ONC says it is aware that developers are being asked to apply innovation and problem solving skills to their real world testing. It believes that the alternative of developing a catalog of detailed specifications and checklists would be undesirably complex, less supportive of ongoing innovation in the market, and ultimately not less burdensome for developers or their customers.

Standards Version Advancement Process

In order to avoid slowing the pace of standards development and deployment in the market, ONC finalizes a more flexible process to make newer versions of standards voluntarily available to developers, which it calls the Standards Version Advancement Process (SVAP). Under this option, developers with health IT certified to a criterion specified for interoperability and data exchange may use a more advanced version of adopted standards or implementation specifications approved by the National Coordinator. Developers could use the SVAP either (i) to update their health IT to a more advanced version of a standard or implementation specification included in the criteria or (ii) to initially certify a Health IT Module. ONC-ACBs will offer certification to newer versions of all standards approved by the National Coordinator to which real world testing requirements apply.

Developers using the SVAP must indicate planned and actual timelines for implementation and rollout of standards updates in their annual real world testing plans and real world testing results submissions. Developers with existing certifications must notify both their ONC-ACB and their affected customers of (i) their intention and plans to update their certified health IT and (ii) its anticipated impact on their existing certified health IT and customers (i.e., how it will affect the interoperability of the Health IT Module in the real world). Mandatory disclosures required of developers also include use of an SVAP standard or specification. ONC also notes that all Conditions of Certification and Maintenance of Certification requirements will apply, meaning, for example, that real world testing plans and results must include the newer standards versions under the SVAP and that developers must maintain their Health IT Modules consistent with the requirements of those newer SVAP standards. If a nonconformity with a newer standard is discovered, it must be addressed in the same manner as a nonconformity with a standard specified in regulation; in other words, surveillance and enforcement under the Program will apply to Health IT Modules certified or updated under the SVAP.

Developers updating their Health IT Modules under the SVAP must provide notice of its anticipated impact which includes whether, and if so for how long, the developer intends to continue to support the certificate for the health IT certified to the prior version of the standard. The notice must be provided sufficiently in advance of the developer establishing its planned timeframe for implementation of the upgrade to afford customers reasonable opportunity to ask questions and plan for the update. ONC-ACBs must attribute updated information to product listings on the CHPL for the Health IT Module involved.

Developers presenting a new Health IT Module for certification using an updated standard under the SVAP could use any (or all) of the newer versions of standards adopted under the SVAP. ONC will implement this new flexibility by allowing ONC-ACBs to accept developer self-declaration of conformity as to the use, implementation, and conformance to a newer version of a standard as sufficient demonstration of conformance in situations where the ONC has approved a version update of a standard but no testing tool is yet available.

Principle of Proper Conduct for ONC-ACB for all Real World Testing Proposals

To enforce new duties on ONC-ACBs related to real world testing and the SVAP, ONC proposes to require them to review and confirm that applicable developers submit real world testing plans and real world testing results. (The principles of proper conduct of ONC-ACBs appear in §170.523.) ONC-ACBs would have to submit testing plans to ONC by December 15 and testing results by March 15. They would also have to make plans and results available through the CHPL and continue to conduct in-the-field surveillance. At least once a quarter, ONC-ACBs would collect all updates successfully made to standards in certified health IT pursuant to developers using the SVAP under the real world testing Condition of Certification. Additionally, ONC-ACBs would have to ensure that developers using the SVAP comply with the applicable requirements.

6. Attestations (§170.406)

The Cures Act requires that a developer, as a Condition and Maintenance of Certification under the Program, must attest to the Secretary that it meets all the Conditions of Certification specified in the Cures Act (other than the "EHR reporting criteria submission" Condition of Certification). In new §170.406, ONC requires developers to attest to compliance with those Conditions and Maintenance of Certification requirements every 6 months. ONC finalizes a 30-day attestation period that would occur twice a year, instead of 14 day windows as proposed. The first window will begin on April 1, 2021 and cover the period from publication of the final rule through March 31, 2021. The next period will begin October 1, 2021 covering the previous 6 months and a semiannual schedule will continue thereafter. Developers presenting health IT for certification for the first time will attest at the time of certification and then be expected to comply with the semiannual attestation requirements. ONC plans to provide notice and reminders to developers to complete their attestations.

ONC also finalizes that it will provide a method for developers to indicate their compliance, non-compliance with, or the inapplicability of each Condition and Maintenance of Certification requirement as it applies to all of their health IT certified under the Program for each attestation period. Developers will have the flexibility to specify non-compliance per certified Health IT Module, if necessary.

Developers must submit their attestations to ONC-ACBs. ONC-ACBs will review and submit the attestations to ONC. ONC will then make the attestations publicly available through the CHPL. Before issuing certifications, ONC-ACBs must ensure that the developer of the Health IT Module met its responsibilities for the Conditions and Maintenance of Certification requirements as solely evidenced by its attestation. ONC provides the following example: where a developer with an active certification under the Program indicated non-compliant designations in its attestation but is already participating in a corrective action plan under ONC direct review to resolve the non-compliance, certification may proceed while the issue is being resolved.

7. EHR Reporting Criteria Submission

The Cures Act requires developers to submit reporting criteria on certified health IT in accordance with the EHR reporting program established under section 3009A of the PHSA, as added by the Cures Act. ONC has not yet established the EHR reporting program and in the final rule no timeline is offered.

C. Compliance

ONC notes that its proposals for Maintenance of Certification requirements do not necessarily define all the outcomes necessary to meet the Conditions of Certification. Instead, they constitute preliminary or baseline evidence used to measure whether a condition is being met. Thus, ONC notes it could determine that a Condition of Certification is not being met through reasons other than the Maintenance of Certification requirements. ONC clarifies that, for compliance and

surveillance purposes, ONC and the ONC-ACBs will examine whether the certified health IT meets the full scope of the certification criteria rather than the subset of functions against which it was tested.

D. Enforcement

Section 4002 of the Cures Act adds Program requirements focused on developers' actions and business practices through the Conditions and Maintenance of Certification requirements; these requirements expand the current focus of the Program beyond the certified health IT itself. The Cures Act also permits the Secretary to encourage compliance with the Conditions and Maintenance of Certification requirements and to take action to discourage noncompliance.

Accordingly, ONC finalizes a general enforcement approach outlining a corrective action process for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement has not been or is not being met by a developer under the Program. Essentially, for the certification criteria at §§170.401 through 170.406, developers may undertake a corrective action plan to correct a nonconformity with a condition of certification; failure to do so may result in a ban of all of the developer's certified Health IT Modules or a termination of a Module's certificate.

Use of Existing Direct Review Enforcement Process. ONC finalizes its proposal to use (with minor changes) the processes previously established for ONC direct review of certified health IT and codified in §§170.580 and 170.581 for the enforcement of the Conditions and Maintenance of Certification requirements. ONC emphasizes that its priority will be to work with the developer to remedy the matter through a corrective action process. By direct review, ONC says that it will be the sole party responsible for enforcing compliance; ONC-ACBs will not be involved in enforcement though their surveillance activities would continue and could supplement ONC enforcement efforts. In essence, the final rule expands the reasons for which ONC may conduct direct review to include these non-conformities.

ONC may initiate direct review if it has a reasonable belief that a developer has not complied with a Condition of Certification. ONC will issue a notice to the developer of a potential or actual non-conformity; the developer may provide a response. ONC notes its preference that customers and end-users first work with developers to resolve an issue and if that does not resolve the issue that they contact the ONC-ACB.

Records Access. ONC gives itself access to developers' records and technology related to the development, testing, certification, implementation, maintenance, and use of the certified health IT as well as any complaint records (including issue logs and help desk tickets). This requirement also extends to records related to marketing and distribution, communications, contracts, and any other information relevant to compliance with any of the requirements. ONC says it would include appropriate safeguards for proprietary business information or trade secrets.

Bans and Terminations. ONC may issue a certificate ban or termination for a certified Health IT Module if it determines that a developer is not cooperating with the fact-finding process, not working with ONC to develop a corrective action plan or not carrying out the plan. The ban would apply to the developer, its subsidiaries and successors and would prohibit future certification of the developer's health IT. ONC notes that this does not mean an existing certification would be withdrawn, but it does mean the developer could not make updates to the certified products.

In addition, ONC may terminate the certification if the IT developer fails to work with ONC or is otherwise noncompliant with the corrective action process. ONC will evaluate on a case-by-case basis whether termination is appropriate, taking into account factors such as whether the developer was previously noncompliant with Program requirements, the severity and pervasiveness of the noncompliance (including the effect of the noncompliance on widespread interoperability and health information exchange), the extent of the developer's cooperation with ONC, the extent of potential negative impact on providers, and whether termination or a certification ban is required for the integrity of the certification process. Notice of termination will include information for the developer on appeals as well as instructions for requesting reinstatement using current procedures.

ONC would work with HHS, CMS and other partners to make appropriate remedies available for users of health IT that has been banned or terminated, such as hardship exceptions for the Promoting Interoperability Programs.

ONC does not include in its enforcement policy two aspects of its current enforcement authority under §170.580. First, it does not believe its suspension authority for serious risks to public health or safety applies in this context. Second, ONC does not wish to be bound by its "proposed termination" procedure under §170.580(e), which it describes as an intermediate step between a developer's failure to take appropriate and timely corrective action and ONC termination of the certificate; ONC prefers to be able to move directly to termination if the developer does not take appropriate and timely corrective action.

Public Availability. ONC will publicly list on its website developers and certified Health IT Modules that are subject to a certification ban or that have been terminated. ONC-ACBs must promptly report to ONC information that could inform whether ONC should exercise direct review for noncompliance with a Condition of Certification or any other matter within ONC direct review.

Relationship to OIG. Noting that the HHS Office of Inspector General is also authorized to investigate claims of information blocking or false attestations, ONC clarifies that the two agencies operate independently and may both exercise those authorities at any time. ONC believes the agencies will cooperate and coordinate enforcement activities, such as sharing information about possible information blocking or false attestations.

Self-developers. Finally, noting that self-developers differ from other health IT developers in that their products are not made commercially available and they do not have customers, ONC nonetheless finalizes that all general Conditions and Maintenance of Certification requirements apply to such developers.

VII. Information Blocking

Section 4004 of the Cures Act added section 3022 of the Public Health Service Act (PHSA) to define and prohibit information blocking by health care providers, IT developers of certified health IT, health information exchanges (HIEs), and heath information networks (HINs). While section 3022 defines information blocking in very broad terms, it also directs the Secretary to identify reasonable and necessary activities and practices that do not constitute information blocking.

ONC identifies eight types of activities that do not constitute information blocking, and it refers to these activities as exceptions. The exceptions apply to certain activities that do in fact interfere with the access, exchange, or use of electronic health information (EHI) but that may be reasonable and necessary to further the goals of section 3022 if certain conditions are met.

The preamble to the final rule reiterates the legislative background and purpose of the information blocking rule. ONC adds a new part 171 to title 45 of the Code of Federal Regulations to implement the information blocking rules of section 3022. ONC sought comment on all aspects of its proposals to implement the information blocking rule.

While many commenters supported the policy goals in the proposed rule, many were concerned by the breadth of the proposed definitions, the ambiguity of expectations, and the narrowness of the exceptions. Still other comments observed that the exceptions were too vague and did not specify how exceptions would be arbitrated. ONC states that the final rule focuses the scope of some of its defined terms (e.g., the definitions of EHI and HIN); adds a new exception called the Content and Manner Exception at §171.301; and provides clarification and additional examples.

Many commenters were concerned by the proposed effective date; they also requested a non-enforcement policy for periods ranging from 18 months to 5 years. ONC finalizes a general effective date for the information blocking regulations at 45 CFR part 171 of 6 months after the date of publication of the final rule in the *Federal Register* (referred to as the compliance date). Additionally, ONC notes that the definition of EHI is more limited in scope for the first 18 months after the compliance date and expands thereafter. Thus, compliance during those first 18 months applies only to the EHI identified by the data elements represented in the USCDI. The new Content and Manner Exception provides time for actors to adjust to the new information blocking paradigm.

With respect to enforcement, ONC and OIG are coordinating the timing; first OIG must establish policies for information blocking civil money penalties (CMPs) through rulemaking. ONC notes

that no enforcement will apply before the compliance date and the precise date for the beginning of enforcement will depend on the OIG's final rule.

Commenters also suggested that the agency develop education and training materials; ONC states that it will undertake multiple education efforts, including infographics, fact sheets, and webinars.

A. Definitions

1. Information Blocking (§171.103)

ONC finalizes its proposal to codify the definition of information blocking contained in section 3022(a)(1) of the PHSA with some language modifications and a new temporary policy for EHI. Specifically, for the 24-month period beginning on the date of publication of the final rule, the scope of EHI subject to the information blocking rules is limited to EHI identified by the data elements represented in the USCDI standard. ONC believes this new policy responds to concerns about the breadth of information covered by the rule and about the pace at which the rule impacts stakeholders. The definition reads as follows:

> *Information blocking*. (a) Information blocking means a practice that—
> (1) Except as required by law or covered by an exception set forth in subpart B or subpart C of this part, is likely to interfere with access, exchange, or use of electronic health information; and
> (2) If conducted by a health information technology developer, health information network or health information exchange, such developer, network, or exchange knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or
> (3) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.
> (b) Until [Insert date 24 months after the publication date of the final rule], electronic health information for purposes of paragraph (a) of this section is limited to the electronic health information identified by the data elements represented in the USCDI standard adopted in §170.213.

ONC clarifies that "required by law" specifically refers to any interference with access, exchange, or use of EHI that is explicitly required by state or federal law. ONC notes that the reference to state or federal law includes statutes, regulations, court orders, and binding administrative decisions or settlements, and also includes tribal laws.

2. Other Definitions (§171.102)

ONC establishes definitions for a number of additional terms, some of which are described below:

a. Actor. The term actor refers to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks. ONC distinguishes among the types of actors in the rule when necessary.

b. Health care provider. ONC finalizes its proposal to use the very broad definition of health care provider established under the HITECH ACT under section 3000(3) of the PHSA which includes, but is not limited to, all individuals and entities covered by the HIPAA definition.[23] ONC will consider whether to expand the definition of health care provider in the future. The agency notes that a health care provider could also be operating as a different type of actor (e.g., a health information network) under certain circumstances. Many commenters requested a narrower definition; they also requested a phased-in approach. ONC believes that a broader definition is preferable; it claims the 24-month limited EHI policy addresses any need for a phased-in approach to its definition of health care provider. ONC also notes that medical device manufacturers and community-based organizations are not considered health care providers unless they are also a type of individual or entity identified in the definition.

c. Health Information Network (HIN) or Health Information Exchange (HIE). ONC had proposed separate definitions for health information network and health information exchange; many commenters suggested combining them to avoid confusion. The agency concurs and creates a single definition for both terms as follows:

> *Health information network or health information exchange* means an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information:
> (1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and
> (2) That is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164.

For the final rule, the language of the definition is narrowed. First, the types of actions (e.g., manages or facilitates) that were covered by the definition have been reduced; for example, the final definition omits "substantially influences" as an element of the definition. Second, the

[23] The term health care provider is defined to include a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician, a practitioner (as described in section 1842(b)(18)(C) of the SSA), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization, a rural health clinic, a 340B covered entity, a physical or occupational therapist or a qualified speech-language pathologist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.

definition clarifies that there must be exchange between two or more unaffiliated individuals besides the HIN/HIE that are enabled to exchange with each other. Finally, the definition is focused on three types of activities: treatment, payment, or health care operations (as defined under the HIPAA Rules.

ONC clarifies that the reference to the three types of activities does not limit the application of the definition to HIPAA covered entities or business associates. It also notes that if an individual or entity meets any of the three types of activities, it will be considered an HIN/HIE for any practice they conduct while functioning as a HIN/HIE. ONC reiterates that the HIN/HIE definition applies only to claims of information blocking; an HIN/HIE's business associate agreement with participating covered entities may also contain conditions relating to how information may be accessed or to whom to provide access.

Commenters suggested excluding certain entities (e.g., health plans and other payors, providers, ACOs, etc.); the final definition does not expressly exclude any type of entity. ONC notes that the revised, more narrow definition in the final rule clearly excludes entities such as social networks, internet service providers, and technology that only facilitates information exchange among patients and family members.

d. Health IT developer of certified health IT. ONC defines the term to mean an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health IT certified under the ONC Health IT Certification Program (Program), and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a certification program kept or recognized by ONC.

ONC underscores that the definition applies to individuals or entities that develop *or offer* certified health IT; this includes the individuals' or entities' subsidiaries and successors. ONC also notes that the information blocking rule is not limited to practices related only to certified health IT; it applies to any practice by an individual or entity that develops or offers certified health IT that is likely to interfere with access, exchange, or use of EHI, including practices associated with any of the developer's or offeror's health IT products that have not been certified under the Program.

The definition also encompasses claims of information blocking against a developer whose certification is terminated or withdrawn for practices that occurred during the period of the health IT's certification. ONC believes the text of its regulation makes it clear that an information blocking claim does not have to be brought while the developer still has certified health IT. In response to a query, ONC states that the vast majority of public health agencies would not be included in this definition; the public health certification criteria within the Program apply to health IT that health care providers use to exchange information with the public health information infrastructure. The criteria do not apply to public health reporting or the exchange infrastructure itself.

ONC considered additional approaches to ensure developers and offerors are subject to the information blocking rule for an appropriate period of time after leaving the Program. However, the agency does not extend the definition beyond the date the developer or offeror no longer has any health IT certified under the Program.

Self-developers of certified health IT (as understood under the Program) are treated as health care providers. However, ONC notes that self-developers of Health IT Modules are subject to certain Condition and Maintenance Certification requirements under subpart D of part 170 which include assurances and attestations that the Modules do not engage in information blocking. ONC further clarifies that the health care provider is responsible for the certification status of the Health IT Module and is the primary user of that Module; it also means that the provider does not offer the health IT to other entities on a commercial basis.

e. Electronic health information (EHI). ONC had proposed a very expansive definition of EHI which included but was not limited to electronic protected health information (ePHI) and which would have encompassed health information that is created or received by health care providers and those operating on their behalf; health plans; health care clearinghouses; public health authorities; employers; life insurers; schools; or universities. Some commenters objected to the proposal noting its breadth and concern over their ability to discern what health information they would have to make available; others noted a heavy compliance burden if they were required to separate EHI from ePHI to comply with both HIPAA and the information blocking rules.

CMS finalizes the following revised definition:

> *Electronic health information (EHI)* means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include:
> (1) Psychotherapy notes as defined in 45 CFR 164.501; or
> (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

ONC focuses the definition on ePHI (as defined in the HIPAA Rules) and limits it to the extent that ePHI is included in a designated record set. The reference to the HIPAA ePHI definition also incorporates related HIPAA definitions for protected health information and electronic media. The final definition omits any reference to observational health mentioned in the proposed rule in part because of an absence of a concrete definition of that term. ONC felt that limiting the scope of EHI to data identified in the USCDI standard would be too narrow, especially over time. The final definition specifically excludes psychotherapy notes[24] as well as information for civil, criminal or administrative actions.

[24] Psychotherapy notes are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session that are maintained separate from the rest of the patient's medical record (see 45 CFR 164.524(a)(1)).

ONC sought comment on whether to include price information in the definition of EHI; it does not finalize this policy. However, ONC states that the definition does not specifically include or exclude price information and notes that to the extent ePHI includes price information and is included in a designated record set, that price information will be considered EHI. ONC says that same analysis applies to algorithms or processes that create EHI; if they are ePHI included in a designated record set, they are EHI for purposes of the information blocking rule.

f. Access, exchange and use. Because the information blocking rules promote the ability to access, exchange and use EHI, ONC proposed definitions for these terms that reflected the agency's understanding of the meanings ascribed to those terms by the healthcare industry. Commenters observed that each of the proposed definitions was overly broad and in need of clarification. ONC finalizes revisions to each of the definitions though it notes that the revisions do not narrow the scope of the definitions with respect to the intended interpretation and purpose of supporting interoperability.

> *Access* means the ability or means necessary to make EHI available for exchange or use.

The changes are intended to clarify that access applies with respect to exchange, use or both. ONC notes that access is not limited to direct interfaces.

> *Exchange* means the ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks.

ONC emphasizes that transmission in the definition is not limited to one-way transmission. ONC also makes editorial changes and removes what it describes as extraneous language (e.g., the phrase "securely and efficiently" to describe how EHI is transmitted has been omitted).

> *Use* means the ability for EHI, once accessed or exchanged, to be understood and acted upon.

ONC notes that "understood" encompasses the ability to comprehend various features, such as structure, content and meaning of the information; however, understood is not intended to convey the ability to understand the clinical significance or relevance of the EHI. The agency also clarifies that use is bidirectional. It also removes language from the proposed definition that the term use required that the action must accomplish a desired outcome or achieve a desired purpose. ONC considered adopting the HIPAA Privacy Rule definition of use but rejected it in favor of its own approach which it believes is more suitable for the information blocking rules.

g. Interoperability element. ONC modifies the language of its definition of interoperability element though it states the term is defined to be very broad.

> *Interoperability element* means hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that:
> (1) May be necessary to access, exchange, or use electronic health information; and
> (2) Is controlled by the actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of electronic health information.

While the revised definition is still intended to be broad in scope, it is nonetheless constrained by the more focused final definitions of "EHI," "access," "exchange," and "use" described above. These changes result in a smaller scope of interoperability elements with respect to which access, exchange or use of EHI must be enabled. ONC notes that it leverages the definition of health information technology from section 3000(5) of the PHSA which includes a reference to intellectual property as well as to integrated technologies and upgrades to eliminate any ambiguity as to whether these elements are included.

The definition also clarifies that control by the actor is a necessary component of an interoperability element. ONC believes this addition addresses concerns that its rule could require or encourage actors to infringe on the intellectual property (IP) rights of others; where an actor cannot control the ability to confer rights to use the element, the actor does not have the requisite control over the interoperability element.

ONC believes most certified Health IT Modules and proprietary APIs would be considered interoperability elements; it also clarifies that the underlying substantive content or health facts are not considered interoperability elements. For this definition, a determination of whether a functionality is an interoperability element is determined without regard to whether it is protected under copyright or patent law.

3. Practices that May Implicate the Information Blocking Provision: Likelihood of Interference

ONC states that the information blocking rule is preventive in nature. The final rule prohibits practices that are likely to interfere with, prevent or materially discourage (hereafter generally referred to as interfere or interfering) access, exchange, or use of EHI. Thus, where there is a reasonably foreseeable risk that a practice will interfere with access, exchange, or use of EHI, that practice may violate the information blocking rule even if harm does not actually materialize. The agency emphasizes that analysis of information blocking requires careful consideration of the facts and circumstance, including whether the practice is required by law, whether the actor had the requisite knowledge and whether an exception applies.

In the proposed rule, ONC described a number of different practices that always will, almost always will, or are likely to implicate the information blocking rule. ONC says commenters supported the categories of practices the agency identified in the proposed rule as well as the examples. For the final rule, ONC reiterates the categories of practices and examples from the proposed rule; adds additional examples; and makes changes to some of the relevant terms.

a. Prevention, Material Discouragement, and Other Interference. ONC believes that these terms are not mutually exclusive; prevention and material discouragement are types of interference and when ONC uses the term interfere with or interference, it necessarily includes prevention and material discouragement. As finalized, the term "interfere with" means to prevent, materially discourage, or otherwise inhibit.

b. Likelihood of Interference. The information blocking rules prohibit practices that are likely to interfere with access, exchange or use of EHI. As noted above, a practice implicates the information blocking rules if, under the circumstances, there is a reasonably foreseeable risk that the practice will interfere with access, exchange or use of EHI.

c. Purposes for Which Information May Be Needed. ONC believes that a practice that interferes with access, exchange, or use of EHI under any of the following circumstances, and does not satisfy the conditions of an exception, will almost always implicate the information blocking rule.

- Providing patients access to their EHI and the ability to exchange and use it without special effort.
- Ensuring health care professionals, care givers, and other authorized persons have the EHI they need, when and where they need it, to make treatment decisions and effectively coordinate and manage patient care, and can use the EHI they may receive from other sources.
- Ensuring that payers and other entities that purchase health care services can obtain the information they need to effectively assess clinical value and promote transparency concerning the quality and costs of health care services.
- Ensuring that health care providers can access, exchange, and use EHI for quality improvement and population health management activities.
- Supporting access, exchange, and use of EHI for patient safety and public health purposes.

Thus, practices that increase the cost, difficulty, or other burden of accessing, exchanging, or using EHI for these purposes will almost always implicate the information blocking rule. ONC views fees charged by actors to access, exchange or use their EHI as inherently suspect.

d. Control over essential interoperability elements. ONC states that where an actor has substantial control over one or more interoperability elements that provide the only reasonable means of accessing, exchanging, or using EHI for a particular purpose, any practice by the actor that could impede the use of the interoperability element(s)—or that could unnecessarily increase the cost or other burden of using the element(s)—will almost always implicate the information blocking provision. ONC also cites examples of technological dependence, such as contractual and intellectual property obligations, a reluctance to switch to other technologies due to costs and workflow disruptions, and network effects of health IT adoption (where providers rely on

technologies adopted by other parties with whom they must exchange EHI). ONC provides specific examples of this dependence.

ONC cautions that actors with control over interoperability elements must be careful not to exclude appropriate persons from use of those elements or to create artificial costs or other impediments to that use. ONC says it "looks at accountability through the lens of whether the actor is the individual or entity engaging in the practice."

e. Practices likely to interfere. ONC believes the following practices described in the proposed rule are likely to implicate the information blocking provision by restricting access, exchange, or use of EHI.

- Formal restrictions, such as license or contract terms, sharing policies, intellectual property or other rights, etc., as well as informal restrictions, such as when an actor refuses to exchange or facilitate access or use of EHI. ONC provides several examples of each.
- Limiting or restricting the interoperability of health IT, such as disabling or restricting use of a capability that permits users to share EHI with other systems or configuring technology so that the types of data that may be exported or used is limited.
- Impeding innovation and advancement, such as exclusionary, discriminatory, or other practices that impede development, dissemination or use of interoperable technologies and services that enhance access, exchange, or use of EHI. ONC provides several examples.
- Opportunistic pricing practices, such as "rent-seeking" and other practices that artificially increase the cost and expense to access, exchange, or use EHI. ONC provides several examples.
- Non-standard implementation policies of health IT that increase the complexity or burden of accessing, exchanging, or using EHI. This occurs where an actor chose not to adopt, or to materially deviate from, relevant IT standards, implementation specification, and certification criteria established by ONC or by the relevant segment of the IT industry.

Commenters sought clarity on the type of contract and agreement terms that could implicate the information blocking rules. ONC responds that contracts and agreements can interfere with access, exchange, or use of EHI through terms besides those dictating unreasonable fees or commercially unreasonable licensing requirements. It notes that unconscionable terms for access, exchange, or use of EHI or for licensing an interoperability element are problematic; for example, it would be an unconscionable term to require a software company that produced a patient access application to relinquish all IP rights to the actor. However, ONC clarifies that an actor may refuse a request to license an interoperability element where the entity requesting the license or the use of the interoperability element does not seek to use the element with either the actor or the actor's customers for EHI to be accessed, exchanged, or used.

ONC notes it designed the proposed and final rules to be consistent with the HIPAA Privacy Rule; it does not require disclosure of EHI in any way that would not be permitted under that

Privacy Rule. However, if an actor is permitted under the Privacy Rule (or under any other law) to provide access, exchange, or use of EHI, it may be required to do so under the information blocking rules.

ONC provides additional examples of practices that limit or restrict interoperability of health IT. One is that an actor may not withhold a FHIR service base URL; these URLs are necessary to enable the access, exchange, or use of EHI (for example for patients to access their EHI). ONC notes that it is not requiring that all FHIR service base URLs must be made publicly available; the agency is focused on patient access to their EHI. Similarly, an actor's refusal to register a software application to enable patient access to their EHI limits or otherwise restricts interoperability. ONC adds definitions for the terms "API Information Source," "API User," Certified API Developer," and "certified API technology" using the same definitions that apply for certification requirements of API under §170.404.

ONC clarifies that slowing or delaying access, exchange, or use of EHI could constitute interference depending on the circumstances.

Commenters expressed concerns that application (app) developers not covered by the HIPAA rules often do not give patients clear terms of how their EHI will subsequently be used (e.g., sold) once the patient authorizes the app to receive their EHI. ONC states that the final rule supports an individual's choice of third-party app developer and app; it will be necessary for the individual to agree to what ONC describes as clear and public terms of use on how engagement with the developer and app occurs. ONC rejects calls to require app developers to use its Model Privacy Notice; it believes any privacy notice that adheres to the following practices and policies should suffice. The privacy policy is (i) publicly accessible at all times; (ii) shared with all individuals that use the technology before EHI from an actor is received by the technology; (iii) written in plain language; (iv) describes whether and how EHI may be accessed, exchanged or used by any entity (including sale of EHI); and (v) requires the express consent from the individual. ONC provides examples. ONC says it will monitor how individuals are educated about potential privacy and security risks of third-party aps.

Clarity was also sought by actors about the extent to which they could vet third-party apps. ONC responds that for certified API technology there should be few, if any, security concerns about risks posed by patient-facing apps to the disclosing actor's health IT system. ONC notes that health care providers may conduct such vetting as they deem appropriate of their business associates before granting access and use of EHI to those entities.

4. Applicability of Exceptions

Section 3022(a) of the PHSA requires the Secretary to identify reasonable and necessary activities that do not constitute information blocking. ONC distinguishes between practices and activities as follows: a practice is conduct that implicates the information blocking rule and that does not fall into one of the exceptions whereas an activity is conduct that implicates the information blocking rule but falls within an exception and meets all terms and conditions for the

exception to apply. ONC finalizes a shorter definition of practice: a practice is an act or omission by an actor. The change is intended to clarify that a single act or omission may constitute a practice. ONC also finalizes its approach that "when identifying exceptions, [it] describes *practices* that, if all applicable conditions are met, are reasonable and necessary and not information blocking."

5. Price Information Not Defined

ONC did not propose a definition of the term price information; however, in the proposed rule ONC claimed it "has a unique role" in possibly establishing a framework to prevent the blocking of price information. It sought comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care. ONC says it received more than 1,000 comments on challenges with respect to price transparency in the context of the information blocking rule; it has shared the feedback with the relevant agencies.

B. Exceptions to the Information Blocking Definition

Consistent with PHSA section 3022, ONC proposed seven exceptions that would apply to certain activities that do in fact interfere with the access, exchange, or use of EHI (i.e., constitute information blocking) but that are reasonable and necessary if certain conditions are met. ONC finalizes those exceptions, with some modifications and often significant restructuring, and the final rule adds an eighth exception called the Content and Manner Exception which is described below.

The final rule divides the exceptions into two categories: (i) exceptions that involve not fulfilling requests to access, exchange, or use EHI (finalized in §§171.201-205); and (2) exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI (finalized in §§171.301-303). ONC uses the term "fulfill" throughout the exceptions; fulfill refers to making the EHI available for the requested access, exchange or use—it goes beyond simply responding to a request.

Pursuant to §§171.200 and 171.300, for any of the exceptions to the information blocking rule to apply, an actor must comply with all applicable terms and conditions of the exception(s) at all relevant times. The actor has the burden of proof to demonstrate that compliance. ONC finalizes its proposal to apply the exceptions to all actors; depending on the exception, the agency creates special conditions to apply to subsets of actors.

1. Preventing Harm Exception (§171.201)

ONC finalizes its proposal, with modifications, for an exception for reasonable and necessary practices to prevent harm to a patient or another person, subject to certain conditions. The major modifications include better aligning the exception with the HIPAA Privacy Rule and substantial restructuring of regulation text of the exception.

To qualify for the exception—

(i) the actor must have a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another person that would otherwise arise from the access, exchange, or use of EHI affected by the practice;

(ii) the practice must be no broader than necessary to substantially reduce the risk of harm; and

(iii) the practice must satisfy at least one element from each of the following three conditions:

(I) the practice is based on a type of risk;

(II) the practice protects against a type of harm; and

(III) the practice is implemented based on an organizational policy or a determination specific to the facts and circumstances.

Additionally, ONC specifies in regulations that a patient, and under certain circumstances a patient's representative, may have rights under the Privacy Rule, or any federal, state, or tribal law, to have a determination to restrict access, exchange of use of EHI under this exception reviewed and potentially reversed.

Commenters observed that the proposed standard that a practice must be no broader than necessary to "directly and substantially reduce" the risk of harm was more stringent than necessary to accomplish the goals of the exception; the agency agrees and modifies the language in §171.201(b) (described in clause (ii) immediately above) to omit the requirement for a direct reduction of harm and instead require only a substantial reduction in the risk of harm.

a. Types of risk

The risk of harm must either (i) be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient; or (ii) arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

The condition as finalized does not require actors to evaluate whether they agreed with individualized determinations of risk made by a licensed health care professional to comply with the exception. ONC also clarifies that actors relying on an individualized determination made by a licensed health care professional are not required to review or confirm the health care professional's judgment.

The final rule specifically requires the licensed health care professional to have a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination. ONC emphasizes that an individualized determination by a licensed health care professional in the exercise of professional judgment must be that a risk of harm cognizable under this exception is associated with particular access, exchange, or use of the patient's EHI. However, a risk that is

less individualized (because it arises from data issues) may be identified by a clinician or other persons with relevant expertise without regard to any clinician-patient relationship.

ONC clarifies that the exception applies to practices that interfere with access, exchange and use of EHI for individuals that the actor determines not to treat as a personal representative of the patient which is consistent with the HIPAA Privacy Rule at 164.502(g)(5). This would include permitting an actor to rely on another licensed health care professional (or other type of covered entity) to not treat the individual as a patient's personal representative. The exception also applies to circumstances that the professional determines that the risk of abuse of the patient by the personal representative is beginning as well as where prior or ongoing abuse is known or suspected. ONC does not impose any specific documentation requirements for this condition. The agency notes that the information blocking rules do not require actors to disclose to the patient representative their awareness or suspicion of patient abuse by the representative. ONC observes that limiting access, exchange of use of EHI to the patient under these circumstances may be a permissible practice if the actor knows or suspects the person suspected of abusing the patient is looking over the patient's shoulder when the patient is reviewing their EHI.

b. Types of risks of patient harm

The types of harm for this exception are focused on the types of harm under the HIPAA Privacy Rule for which a covered entity could deny access to an individual's protected health information; these are described in the table below. The types of risk of patient harm in the proposed rule are maintained and expanded upon as follows, and include the relevant HIPAA standards:

Type of Harm Exception Requirements	HIPAA Standards
§171.201(d)(1): The practice interferes with access, exchange, or use of the patient's EHI by their legal representative, and the practice is implemented pursuant to an individualized determination of risk of harm made by a licensed health care professional in the exercise of professional judgment (§171.201(c)(1))	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(iii), which is substantial harm to the individual or another person.
§171.201(d)(2): The practice interferes with the patient's or their legal representative's access to, use or exchange of information that references another natural person, and the practice is implemented pursuant to an individualized determination of risk of harm made by a licensed health care professional in the exercise of professional judgment (§171.201(c)(1))	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(ii), which is substantial harm to such other person.
§171.201(d)(3): The practice interferes with the patient's access, exchange, or use of their own EHI, regardless of whether the risk the practice is implemented to substantially reduce is determined	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(i), which is a harm to the life or

Type of Harm Exception Requirements	HIPAA Standards
on an individualized basis by a licensed health care professional in the exercise of professional judgment (§171.201(c)(1)) or arises from data that is known or reasonably suspected to be corrupt due to technical failure, erroneous for another reason, or misidentified or mismatched (§171.201(c)(2))	physical safety of the individual or another person.
§171.201(d)(4): The practice interferes with the patient's legal representative's otherwise legally permissible access, exchange, or use of the patient's EHI and the practice is implemented to reduce a risk arising from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (§ 171.201(c)(2))	The harm of which the actor reasonably believes the practice will substantially reduce a risk must be the type of harm described in 45 CFR 164.524(a)(3)(i), which is a harm to life or physical safety of the individual or another person.

For the types of circumstances where the Preventing Harm Exception is used to permit denial of access under the information blocking rules and the HIPAA Privacy Rule permits denial of access to PHI, ONC believes the application of the HIPAA standard under both provisions is appropriate. Where circumstances would only apply under the Preventing Harm Exception, ONC believes applying the HIPAA standard under the information blocking rules provides consistency. It set the standards to ensure that a higher standard would not apply for the Preventing Harm Exception as applies under the HIPAA Privacy Rule. ONC provides some examples of when access, exchange, or use of EHI with which the practice interferes is not related to the right of access under the HIPAA Privacy Rule: when access, exchange, or use of the patient's EHI is by the patient's health care providers or when the risk of harm arises from data issues rather than having been determined on an individualized basis by a licensed health care professional.

Commenters sought expansion of the exception's types of harm to include psychological and other types of non-physical harm. ONC could not develop what it refers to as an appropriate and unique standard for non-physical harm; the final rule limits the scope of harm under the exception to life or physical safety of the individual (or another person).

With respect to documentation, ONC does not finalize its proposal to require that health care professionals use any particular format to document the individualized risk of harm determinations. However, it confirms that use of EHRs to document risk determinations is appropriate; further, it does not intend to duplicate or require different documentation of information that may already be captured in reliable business records under the HIPAA Privacy Rule and applicable state laws.

In response to comment, ONC clarifies that delaying fulfillment of an otherwise feasible and legally permissible request for exchange, access, or use of EHI that is finalized and available simply because the actor knows that more EHI for the patient will become available at

some later date does not qualify for the exception. It does not consider mere incompleteness of a patient record as making the rest of the information in the record inaccurate. Additionally, if an actor cannot effectively sequester non-final EHI where use of that EHI would not be appropriate, the actor may have to rely on the new Content and Manner Exception. ONC also observes that where a health care provider believes EHI in the patient's records is safe enough for their use, it may not deny a patient request to access, exchange or use that EHI simply because the patient might find an error.

Regular and systematic interference from a particular source based on considerations other than the risk profile of data quality issues (e.g., where data comes from a competitor) would not meet the conditions for the exception. ONC clarifies that the exception applies to practices likely to interfere with access, exchange, or use of EHI that the actor knows includes mismatched or misattributed data or reasonably suspects includes such errors. Similarly, the exception does not apply to an actor's refusal to allow access, exchange, or use of EHI because the actor may not know, or may not be satisfied with, the matching methods to be used by the recipient; this concern may be addressed by the Security Exception.

The agency does not require an actor to meet a patient-matching threshold or to use particular methods for patient identification and matching. ONC does not believe its final rule imposes obligations on actors to ensure they do not release information that could include latent errors. It also notes that an actor who receives EHI in error is not required, for purposes of this exception, to identify the correct recipient or to forward the mis-directed EHI to the proper recipient.

c. Practice based on organizational policies or a determination specific to the facts and circumstances

ONC finalizes these two alternative conditions for a practice to satisfy the exception. If the practice implements an organizational policy, the practice must:

- Be in writing;
- Be based on relevant clinical, technical, and other appropriate expertise;
- Be implemented in a consistent and non-discriminatory manner; and
- Satisfy the other conditions of the exception.

The final rule omits references to particular or unique documentation forms, methods, or content. In response to comment about practices that routinely delay release of certain results (e.g., laboratory results), ONC does not believe that the routine delay of the availability of broad classes of EHI should qualify for the exception. The agency's position is that where applicable law does not prohibit making particular information available to a patient electronically before it has been conveyed in another way, deference should generally be afforded to patients' right to choose whether to access their data as soon as it is available or wait for the provider to contact them to discuss their results. However, a health care professional may make an individualized determination of risk of harm in the exercise of their professional judgment, and that practice may be protected whether the professional was acting directly on their own

determination or on another actor implementing the delay in reliance on that determination. To be protected under the exception, the professional would have to demonstrate a reasonable belief that delaying availability of the information until delivery can be made in conjunction with counseling and context substantially reduces the risk of harm to the life or physical safety of the patient.

If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm. A determination must be based on:

- Facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and
- Expertise relevant to implementing the practice consistent with the other conditions of the exception that apply to the practice and its use in particular circumstances.

A health care professional's independent and individualized judgment about the safety of the actor's patients or other persons will be entitled to substantial deference, taking into account all relevant facts under the particular circumstances.

d. Rights of Review

ONC finalizes a condition permitting patients to exercise their rights to review a determination to interfere with access, exchange or use of their EHI; these are rights established under any federal, state or tribal law or regulation which may apply. The right of review applies to the patient whose EHI is at issue but may be exercised by the patient's representative. While any such review is pending, if the practice otherwise complies with all the conditions of the exception, the practice may continue. If the determination is reversed on review, the practice does not meet the conditions of the exception and is considered information blocking.

2. Privacy Exception (§171.202)

ONC finalizes its proposal to establish an exception to protect the privacy of an individual's EHI, with minor modifications and clarifications. Under this exception, ONC identifies four methods, each with its own terms and conditions, by which the practice of an actor may qualify for protection from the information blocking rules to protect the privacy of an individual's EHI. ONC refers to these four methods as "sub-exceptions;" as is the case for each exception under the rule, the terms and conditions of each sub-exception must be met at all relevant times. ONC reiterates that any privacy protection practice must be consistent with applicable laws related to health information privacy, such as the HIPAA Privacy Rule, the HITECH Act, 42 CFR Part 2, and state privacy laws.

ONC believes that the Privacy Exception operates consistently with the HIPAA Privacy Rule framework and that it promotes patient privacy rights. However, as it does elsewhere in the rule, ONC acknowledges that the information blocking rules may require actors to provide access,

exchange, or use of EHI in situations where HIPAA does not. HIPAA permits covered entities to use and disclose ePHI; the information blocking rule requires actors to provide access, to exchange, or to use EHI unless they are prohibited from doing so under federal or state law or are covered by one of the exceptions.

a. Definitions

ONC adds a definition of the HIPAA Privacy Rule to its defined terms for the Privacy Exception (defined as 45 CFR Parts 160 and 164) to support alignment of the exception with the HIPAA Privacy Rule.

ONC also finalizes, with minor clarifications, its proposal to define "individual" in a more expansive manner than the term is defined under the HIPAA Privacy Rule or in section 3022 of the PHS Act. This definition of individuals applies only with respect to this exception and its four sub-exceptions. The term individual means one or more of the following:

(1) An individual (as defined under§160.103 of the HIPAA Privacy Rule).
(2) Any other natural person who is the subject of the EHI being accessed, exchanged, or used.
(3) In relation to an individual described in (1) or (2) above:
    (i) A person who legally acts on behalf of such person in making decisions related to health care as a personal representative, in accordance with 45 CFR 164.502(g);
    (ii) A person who is a legal representative of and can make health care decisions on behalf of such person; or
    (iii) An executor, administrator or other person having authority to act on behalf of a deceased person or the individual's estate under state or other law.

ONC clarifies that the reason to include "any other natural person who is the subject of the EHI being accessed, exchanged, or used" in paragraph (2) above is to include EHI that would be accessed, exchanged, or used by entities that are not subject to HIPAA (i.e., entities that are not covered entities or business associates). ONC seeks to protect information about all individuals, not just individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates.

b. Sub-exception: Precondition imposed by law not satisfied

Because state and federal privacy laws may impose conditions before disclosure of PHI is permitted, this sub-exception protects actors who do not provide access, exchange or use of EHI because a necessary precondition imposed under law for that disclosure has not been met. An actor in this situation may elect not to provide access, exchange, or use of such EHI if the precondition under law has not been satisfied, subject to a number of conditions. However, ONC is concerned that actors may use protection of an individual's privacy as a pretext for information blocking; the agency repeats its concerns in the final rule.

To qualify for this sub-exception, an actor must have documented written organizational policies that specify the criteria it will use, and the steps the it will take, to satisfy the legal precondition.

This may include taking reasonable steps to ensure that the actor's workforce and its agents understand and consistently apply and actually follow the policies and procedures.

With respect to actors operating in multiple states, ONC explains in the final rule that they may either (i) satisfy this condition by adopting and implementing uniform policies and procedures required by the most protective state than would otherwise be required by federal law or the laws of any of the other states in which it operates. Alternatively, the actor may comply with the preconditions of each state in which it operates. ONC says the uniform policies and procedures approach must assure alignment with the HIPAA Privacy Rule individual access implementation specifications and help assure that the broader policy goals for individual access to information are met. ONC warns against actors using state or federal laws to shield against disclosing information. The agency also clarifies that not only must policies and procedures meet these requirements, but actions undertaken pursuant to those policies and procedures must meet the conditions of the sub-exception. It also notes that this condition applies only after insufficient consent or authorization is received; ONC states that if no consent or authorization is received, the actor is not required to communicate to the entity requesting the EHI that the actor does not have the individual's consent or authorization.

Alternatively, an actor could document, on a case-by-case basis, the objective criteria it uses to determine when the legal precondition is satisfied, any criteria that were not met, and the reason why the criteria were not met. The documentation must identify the specific circumstances of the practice, the criteria the actor uses to determine that the precondition was satisfied, and the objective criteria the actor applied that are directly relevant to meeting the precondition.

Additionally, if the legal precondition relies on consent or authorization from an individual, the actor must use reasonable efforts within its control to provide the individual with a meaningful opportunity to provide the consent or authorization. ONC had proposed a higher standard where the actor would have had to do "all things reasonably necessary" within its control; the change to requiring reasonable efforts was made to clarify that the actor does not need to chase the patient to get consent or authorization or take other extraordinary measures. ONC notes reasonable efforts could include a legally compliant consent form, and it says that a best practice would include informing the individual of the right to revoke consent. ONC cautions that an actor may not improperly encourage the individual to refuse to provide the consent or authorization. ONC notes in response to comment that an HIN is not excused from meeting the conditions of this sub-exception; even actors that do not have a direct relationship with the patient should use reasonable efforts within their control to obtain consent or authorization.

Under the final rule, the actor's practice must be tailored to the applicable legal requirement as well as the specific privacy risk or interest being. The actor must carefully evaluate the privacy requirements imposed on the actor (including pursuant to federal or state law) and the privacy interests to be managed by the actor, and must develop a considered response tailored to protecting and promoting the privacy of EHI.

Finally, the actor's practice must be implemented in a consistent and non-discriminatory manner; this means that the actor's privacy-protective practices must be based on objective criteria that apply uniformly for all substantially similar privacy risks. ONC clarifies that "consistent and non-discriminatory" means that similarly situated actors whose interactions pose the same level of privacy risk should be treated consistently with one another under the actor's privacy practices; inconsistent treatment across similarly situated actors whose interactions pose the same level of privacy risk based on extraneous factors are not appropriate.

c. Sub-exception: Health IT developer of certified health IT not covered by HIPAA

Noting that the vast majority of developers of certified health IT are regulated by the HIPAA Privacy Rule because they operate as business associates to health care providers or plans and thus may use the first sub-exception described above, ONC says that some direct-to-consumer products and services would not benefit from that sub-exception.

ONC establishes this sub-exception for developers of certified health IT who are not required to comply with the HIPAA Privacy Rule (referred to by ONC in this sub-exception as non-covered actors). Non-covered actors who engage in a practice that promotes the privacy interests of an individual may choose not to provide access, exchange, or use EHI according to a process described in their organizational privacy policies if the practice meets all the following conditions:

- The actor's organizational privacy policies must have been disclosed to the individuals and entities that use the actor's product or service before they agree to use them.
- The actor implements the practice according to a process described in the organizational privacy policies.
- The practice complies with applicable state or federal privacy laws.
- The practice is tailored to the specific privacy risk or interest being addressed.
- The practice is implemented in a consistent and non-discriminatory manner.

d. Sub-exception: Denial of an individual's request for their ePHI in the circumstances provided in 45 CFR 164.524(a)(1) and (2)

Under the HIPAA Privacy Rule, covered entities (and in some instances business associates) may deny an individual access to PHI. The Privacy Rule establishes grounds for denial of access to PHI that are reviewable and other grounds for denial that are unreviewable. As finalized, the sub-exception applies only to unreviewable grounds of denials of access. (ONC notes it moved the reviewable grounds for denial to the Protecting Harm Exception discussed above because they are directly linked to likelihood of harm to a patient or other individual.)

The unreviewable grounds for denial for individuals include situations involving the following:

- Certain requests made by inmates of correctional institutions.
- Information created or obtained during research that includes treatment, if certain conditions are met.

- Denials permitted by the Privacy Act.
- Information obtained from non-health care providers pursuant to promises of confidentiality.

Additionally, two categories of information are expressly excluded from the individual right of access: psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

In restricting this privacy sub-exception to only unreviewable grounds (i.e., those described in 45 CFR 164.524(a)(1) and (2)), ONC clarifies the regulation text to specify that actors who are covered entities, and in some instances business associates, may deny an individual access to EHI and such denials do not provide an opportunity for review if the denial complies with HIPAA Privacy Rule requirements.

ONC notes that the unreviewable ground for information created or obtained during research described above applies to PHI that is in a designated record set that is part of the research that is still in progress if the individual consented to the temporary access suspension. However, ONC says that access to the individual's PHI may be reinstated upon completion of the research study.

e. Sub-exception: Respecting an individual's request not to share information

ONC finalizes a sub-exception to ensure actors are confident that they may respect an individual's privacy choices when the individual specifically asks an actor not to provide access, exchange, or use of EHI. Thus, unless otherwise required by law, an actor may choose not to provide that access, exchange, or use if all of the following conditions are met:

- The individual asks the actor not to provide such access, exchange, or use.
- The individual initiates the request without any improper encouragement or inducement by the actor.
- The actor documents the request within a reasonable time period.
- The actor's practice is implemented in a consistent and non-discriminatory manner.

ONC notes that once a proper request is made, there is no need for the individual to reiterate that request or for the actor to repeatedly reconfirm or re-document the request. ONC clarifies that individuals have the right to revoke a request not to share information.

ONC declined to specify what constituted a reasonable time period for documentation of the request noting that the Privacy Rule affords covered entities the discretion to determine the exact timing of the documentation.

To further align the sub-exception with the HIPAA Privacy Rule, ONC adds provisions relating to termination of a restriction to deny access, exchange, or use of the individual's EHI that the individual requested. Specifically, an actor may terminate an individual's request for a restriction only if one of the three following conditions is met:

- The individual requests, or agrees to, the termination in writing;
- The individual orally agrees to the termination which the actor documents; or
- The actor informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual's EHI, except that the termination is:
    - Not effective to the extent prohibited by applicable federal or state law; and
    - Only applicable to EHI created or received after the actor informed the individual of the termination.

3. Security Exception (§171.203)

Noting that actors may be reluctant to implement security measures or otherwise safeguard the confidentiality, integrity and availability of EHI without an exception to the information blocking rule, ONC proposed an exception to permit actors to engage in reasonable and necessary practices to promote the security of EHI. ONC is concerned that the information blocking rule could discourage best practice security protocols and diminish the reliability of the health IT ecosystem. However, ONC is also concerned about practices purporting to promote the security of EHI but that may be unreasonably broad, onerous on those seeking access to the EHI, not applied consistently across/within an organization, or otherwise unreasonably interfere with access, exchange, or use of EHI. ONC also notes that a practice that complies with the HIPAA Security Rule might not necessarily qualify for this exception. ONC finalizes the exception without substantive modifications; as it does for all the exceptions, it revises the introductory text for readability.

ONC says the overall goal of the Security Exception is to provide flexibility for reasonable and necessary security practices while screening out practices that purport to promote the security of EHI but that otherwise unreasonably and/or unnecessarily interfere with access, exchange, and use of EHI.

a. <u>Conditions</u>

To qualify for this exception, each practice by an actor must meet all the following conditions:

- The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI. ONC will examine whether the practice directly addresses specific security risks (and whether it served other purposes) to determine the necessity of the practice and its direct relation to safeguarding EHI.
- The practice must be tailored to the specific security risk being addressed. ONC expects actors to have carefully evaluated the security risk and developed a considered response tailored to mitigating the specific vulnerability.
- The practice must be implemented in a consistent and non-discriminatory manner. ONC believes consistent and non-discriminatory means that similarly situated actors whose interactions pose the same level of security risk should be treated consistently with one another under the actor's security practices.

Actors may satisfy the requirements for this exception through practices that implement either organizational security policies and practices developed by the actor or through case-by-case determinations.

b. Organizational security policies

If the practice implements an organizational security policy, the policy must—

- Be in writing;
- Have been prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the actor;
- Align with one or more applicable consensus-based standards or best practice guidance; and
- Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

To support a presumption that an actor's security policy is reasonable, ONC believes the policy must be informed by an assessment of the security risk (e.g., threat and vulnerability analysis, data collection, security measures, etc.); must align with one or more applicable consensus-based standards; and must provide objective timeframes and common terminology to identify, respond to, and address security incidents. ONC notes that compliance with the HIPAA Security Rule is relevant but not dispositive to the issue of whether the policy is objectively reasonable. ONC believes documented policies should include specific references to consensus-based standards and best practice guidance.

c. Case-by-case determinations

While ONC expects most security practices will implement organizational security policies, there may be occasions when novel and unexpected threats require action to mitigate a security risk. Thus, where a practice does not implement an organizational security policy, to qualify for this exception an actor must determine in each case, based on the particularized facts and circumstances, that—

- The practice is necessary to mitigate the security risk to EHI; and
- There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.

ONC notes that what constitutes reasonable and appropriate alternatives will depend on the urgency and nature of the specific security threat.

4. Infeasibility Exception (§171.204)

As noted earlier, the information blocking rule would be implicated if an actor refuses to facilitate access, exchange, or use of EHI, either as a general practice or in isolated instances.

However, ONC notes that in certain circumstances there are legitimate practical challenges beyond an actor's control which limit its ability to comply with requests for that access, exchange, or use either because the actor may not have (or may be unable to obtain) the necessary technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, exchange, or use or because the actor would incur costs or other burdens that are clearly unreasonable under the circumstances. ONC proposed an exception that would permit an actor to decline a request when carrying out the request would be infeasible or impossible and when the actor otherwise did all that it reasonably could under the circumstances to facilitate other means of accessing, exchanging, and using the EHI. ONC proposed using a structured, fact-based approach for determining whether a request was infeasible, focusing on the immediate and direct financial and operational challenges of facilitating access, exchange, or use rather than remote, indirect, or speculative types of harm.

ONC finalizes its proposal to add an Infeasibility Exception with substantial changes in response to concerns from commenters. Under the new framework, to be covered under the exception an actor must meet one of three conditions, and comply with a requirement to respond to requests.

a. Uncontrollable events

The actor cannot fulfill a request because of a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority. All that the actor must show is that one of these events occurred and interfered with its ability to fulfill a request.

b. Segmentation

The actor cannot fulfill the request because it cannot unambiguously segment the requested EHI from EHI that:

- Cannot be made available due to an individual's preference or because the EHI cannot be made available by law; or
- May be withheld under the Preventing Harm Exception (under §171.201 described above).

ONC explains that this condition would apply where the actor cannot unambiguously segment the requested EHI from patient records protected under 42 CFR Part 2 for substance use disorder treatment or from records the patient has expressed a preference not to disclose.

c. Infeasible under the circumstances

The actor demonstrates, before providing notice and explanation of infeasibility in its response to the requester, through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

- The type of EHI and the purposes for which it may be needed;

- The cost to the actor of complying with the request in the manner requested;
- The financial, technical, and other resources available to the actor;
- Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use to companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged; and
- Why the actor was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception (under §171.301).

ONC indicates that the following circumstances do not constitute a burden to the actor for purposes of this exception and the agency will not consider them in determining whether a request is infeasible: the manner of the requested access, exchange, or use either would have (i) facilitated competition with the actor or (ii) prevented the actor from charging a fee or resulted in a reduced fee. ONC emphasizes that the exception is intended to help actors who face legitimate practical challenges beyond their control.

In the final rule, ONC does not specify the amount of detail required in the written record or other documentation; it does require that the documentation be contemporaneous to prevent actors from post hoc rationalizations for claims of infeasibility.

ONC declines to adopt a suggestion to permit entities who have joined the Trusted Exchange Framework and Common Agreement (TEFCA) to use the Infeasibility Exception if a requestor or third party refused to join TEFCA. While it may consider this policy at a later date, ONC notes that not joining TEFCA is not de facto proof of infeasibility.

c. Responding to requests

In response to concerns about additional burden on health care providers, ONC modifies its requirements for actors to respond to requests under this exception in a timely manner and the information that must be provided in writing. When the actor does not fulfill a request under this exception, within ten business days of receipt of the request it must provide to the requestor in writing the reason(s) why the request is infeasible. The 10-business day deadline is substituted for the more general "timely" requirement in the proposed rule; ONC also decides not to specify any level of detail or specific type of information that must be included in the written response.

The proposed rule had included a requirement that the actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI. ONC substitutes its new Content and Manner Exception for the reasonable alternative policy under this exception; it believes the new exception clarifies actors' obligations to provide access, exchange or use of EHI in all situations and creates actionable technical procedures. It also believes the new exception will reduce burden on providers.

5. Health IT Performance Exception (§171.205)

Noting that health IT needs to be maintained and occasionally improved, and that performing maintenance or improvement requires the health IT to be temporarily taken offline, ONC proposed an exception to the information blocking rule for practices that are reasonable and necessary to maintain and improve the overall performance of health IT, subject to certain conditions, and applied to both planned and unplanned maintenance and improvement. ONC finalizes its proposal with some changes.

ONC notes that the exception applies to a variety of specific practices that make health IT unavailable; it is not limited to downtime or performance degradation of an actor's entire health IT system. An actor who takes down one means of EHI access to conduct health IT maintenance or improvement may (but is not required to) provide alternative access to EHI during the downtime, in circumstances where this may be practical, and remain in compliance with the exception.

a. Maintenance and improvements to health IT

An actor may make health IT under its control temporarily unavailable, or may temporarily degrade the performance of health IT, to perform maintenance or improvements to the health IT if the actor's practice is—

- Implemented for a period of time no longer than necessary to complete the maintenance or improvements;
- Implemented in a consistent and non-discriminatory manner; and
- If the unavailability or degradation is initiated by an actor that is a health IT developer of certified health IT, a HIE, or a HIN—
    - In the case of planned maintenance or improvement, the practice is consistent with existing service level agreements between the individual or entity to whom such actor supplied the health IT; and
    - In the case of unplanned maintenance or improvement, the practice—
        - is consistent with existing service level agreements between the individual or entity; or
        - is agreed to by the individual or entity to whom such actor supplied the health IT.

ONC modified its proposed text by adding references to temporary performance degradation to clarify that the exception does not only apply to complete unavailability of health IT.

Some commenters complained that the phrase "no longer than necessary" should be defined; ONC responds that it would be impractical to establish specific timeframes applicable to various maintenance and improvement purposes due to wide variation in system architectures and operational contexts. It believes this standard provides adequate flexibility to consider particular circumstances of each case and a variety of factors, including service level agreements in place

for the specific health IT at issue, the type of maintenance or improvements, the technical resources available to the actor, or best practices or other relevant industry benchmarks. In response to comment, ONC clarifies that it does not interpret this condition as requiring immediate full restarts of any or every system.

With respect to agreements with recipients of health IT, ONC notes that availability of health IT is typically addressed in contracts or other agreements which puts recipients on notice about the level of unavailability (both planned and unplanned) that may be expected. For situations where health IT must be taken offline on an urgent basis that is not expressly permitted in a contract, ONC notes the actor could still satisfy this condition by providing oral notice to the recipient. ONC declines to specify specific contract terms dictating timeframes, scheduling or other scope of planned downtime expectations.

When a recipient or customer (as opposed to the supplier of health IT) initiates unavailability, no agreement is necessary for the customer (e.g., a health care provider) to benefit from this exception. However, unavailability initiated by a recipient or customer would still need to satisfy the other conditions of this exception.

b. Assured level of performance

An actor may take action against a third-party application that
is negatively impacting the health IT's performance, provided the practice is—

- For a period of time no longer than necessary to resolve any negative impacts;
- Implemented in a consistent and non-discriminatory manner; and
- Consistent with existing service level agreements, where applicable.

In the final rule, the agency adds this provision to its exception to include a broader class of practices that are the subject of reasonable commercial agreements that may be considered information blocking absent an exception, such as "throttling" or "metering" availability of health IT, to limit the negative impact that may result from third party applications.

ONC confirms that time to complete a maintenance or improvement purpose, objective, or activity includes reasonable and necessary practices such as confirmatory testing and phased restart protocols to ensure that newly deployed or newly updated application functions in a particular production environment as intended and do not adversely affect system stability or the performance of critical functions or components of that system.

d. Practices that prevent harm

If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor is not required to satisfy the requirements of this exception; however, the actor must comply with all the requirements for the Preventing Harm Exception (at §171.201) at all relevant times to qualify for an exception.

e. Security-related practices

Similarly, if the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to EHI, the actor is not required to satisfy the requirements of this exception; however, the actor must comply with all requirements for the Security Exception (at §171.203) at all relevant times to qualify for an exception.

6. Content and Manner Exception (§171.301)

ONC includes a new exception in its final regulation to protect practices that limit the content of an actor's response to a request, or the manner in which the actor fulfills a request, to access, exchange, or use EHI. To qualify for the exception, a practice must meet conditions related to both content and manner. The exception addresses concerns related to the breadth of the EHI definition as well as comments seeking clarification of the proposed reasonable alternative policy under the Infeasibility Exception. ONC moves the reasonable alternative policy from the Infeasibility Exception to the new exception which describes both the requisite content and two ways an actor may fulfill a request for access, exchange or use of EHI (i.e., the manner condition).

a. EHI Content

To mirror the phased-in approach for the scope of the definition of EHI discussed above, the content of EHI that must be fulfilled in response to a request, during the first 24 months after publication of the final rule in the *Federal Register*, is not required to be greater than EHI identified by the data elements represented in the USCDI standard. After that 24-month period, the broader definition of EHI under §171.102 will apply (meaning ePHI, as defined in the HIPAA Rules, to the extent that ePHI is included in a designated record set).

b. Manner

This condition is similar to the "reasonable alternative means" policy that was proposed as part of the Infeasibility Exception which requires an actor to work with a requesting party on a timely basis to identify and provide alternative means of accessing, exchanging, or using EHI. ONC believes this policy better fits its Content and Manner Exception.

(i) Manner requested.

As a general rule, an actor must fulfill a request in any manner requested. This applies unless the actor is either technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request. ONC clarifies that technically unable means that the actor cannot fulfill a request due to a technical limitation. ONC notes that an actor will be considered as having fulfilled a request for EHI in the manner requested where the actor first receives a request for EHI through an API which it could not fulfill and then subsequently receives a request for that EHI to be provided by email which the actor can and does fulfill.

If the actor fulfills a request in the manner requested, then any fees that may be charged by the actor are not subject to the conditions (or limitations) of the Fee Exception under §171.302 (described below). Similarly, if the actor must grant a license of interoperability elements to fulfill the request, that licensing is not required to meet the terms and conditions of the License Exception under §171.303 (described below).

(ii) Alternative manner.

If an actor does not fulfill a request in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the actor must fulfill the request in an alternative manner. The alternative manner requires that the request be fulfilled without unnecessary delay; the requirement to avoid unnecessary delay clarifies that actors using the alternative manner do not get extra time to fulfill the request. They are subject to the same considerations to avoid unnecessary delays as apply to actors under other exceptions.

Additionally, the regulation sets forth a priority and process to fulfill the request under the alternative manner. The actor must first try to fulfill the request using technology certified to ONC standards adopted in part 170. Failing that, the actor must next try to fulfill the request using content and transport standards specified by the requestor and published by the federal government or by a standards developing organization accredited by the American National Standards Institute (ANSI). If the actor is still unable to fulfill the request, it must use an alternative machine-readable format agreed upon with the requestor which must include a means to interpret the EHI. ONC emphasizes that fulfillment using the alternative machine-readable format requires the actor to provide the means to interpret the EHI.

Unlike requests fulfilled in the manner requested, fees charged by actors using the alternative manner must satisfy the Fees Exception. Similarly, any license of interoperability elements granted by the actor using the alternative manner to fulfill the request must satisfy the License Exception.

7. Fees Exception (§171.302)

ONC proposed an exception to permit actors to recover certain costs they reasonably incur in providing access to, exchange of, or use of EHI. This is necessary because ONC interprets the definition of information blocking to include *any fee* likely to interfere with access, exchange or use of EHI. ONC believes that absent an exception, actors may be unable to recover costs they incur to develop technologies and provide services that enhance interoperability. It also notes that failure to satisfy the exception does not necessarily mean that an actor's practice of charging fees meets the definition of information blocking.

The agency finalizes its proposal with some modifications. To qualify for this exception, each practice by an actor must meet all the applicable conditions of the exception. ONC is concerned

by rent-seeking, opportunistic fees, and exclusionary practices that interfere with access, exchange and use of EHI as well as by discriminatory pricing policies that exclude competitors from use of interoperability elements. ONC emphasizes that all the conditions would have to be satisfied *for each and every fee* charged by an actor.

ONC emphasizes that nothing in this exception (or final rule) supports or encourages the sale of EHI. The exception permits recovery of certain costs reasonably incurred in providing access to, exchange of, or use of EHI. The agency notes that many actors are also subject to the HIPAA Privacy Rule and thus are prohibited from selling PHI or receiving remuneration for a disclosure of PHI.

The exception as finalized provides that actors may charge fees, including fees that include a reasonable profit margin, for access, exchange or use of EHI without implicating the information blocking rules if they meet all applicable conditions. The conditions are "basis for fees," "excluded fees," and, as applicable, "compliance with the conditions of certification."

a. Basis for fees

Any fee charged by an actor must meet all the following criteria:

- It must be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests.
- It must be reasonably related to the actor's costs of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged.
- It must be reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported. ONC notes that an actor must allocate costs using reasonable criteria and allocate them among customers that caused the costs to be incurred or that benefit from the technology.
- It must be based on costs not otherwise recovered for the same instance of service to a provider and third party.

The last criterion (based on costs not otherwise recovered for the same instant of service) is a new addition intended to prohibit double-billing for the exact same service. ONC also notes that the exception is limited to EHI as defined in 171.102 (which includes the phased-in scope of ePHI covered under the definition and described earlier). ONC hopes to eliminate ambiguity over what information subject to the information blocking rules and protected under the exception. It specifically notes it is not limiting fees, profits, or both related to access, exchange or use of information outside its definition of EHI.

With respect to the criterion related to allocation among recipients of the technology or services, ONC reduced the standard in the final rule from its propels to require "allocation among all substantially similar and similarly situated individuals" to "all similarly situated individuals" which it believes provides a clearer condition for actors to follow.

ONC tailors the exception to the actor's costs reasonably incurred to provide access, exchange, or use of EHI. While noting that this is a factual determination, ONC states these do not include speculative or subjective costs. Further, the agency emphasizes that charges must not be based on sales, profit, revenue or other value the requester or other persons may derive from subsequent use of EHI. The types of considerations on which an actor may not base fees under the final rule are as follows:

- Whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor;
- Sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of the EHI;
- Costs the actor incurred due to the health IT being designed or implemented in a nonstandard way, unless the requestor agrees to the fee associated with the non-standard design or implementation to access, exchange, or use the EHI;
- Costs associated with intangible assets other than the actual development or acquisition costs of such assets;
- Opportunity costs unrelated to the access, exchange, or use of EHI; or
- Any costs that led to the creation of intellectual property, if the actor charged a royalty for that intellectual property pursuant to Licensing Exception under §171.303 and that royalty included the development costs for the creation of the intellectual property.

ONC added the criterion relating to intellectual property rights in the final rule to prevent actors from recovering for the same costs of creating intellectual property under both the Fees Exception and the Licensing Exception. It also modified its position on nonstandard design to permit fees which a requester agrees to pay. ONC refers readers to the preamble of the proposed rule for a discussion of what non-standard means (84 FR 7521). With respect to intangible assets, the agency emphasizes that these costs cost may not be based on costs unrelated to access, exchange, or use of EHI.

Commenters noted that the potential recordkeeping and administration burden caused by this exception would be extraordinary. While not contradicting those comments, ONC noted other areas in the final rule that it believes will substantially reduce burden, implying that there is a net burden reduction overall.

b. Excluded fees

ONC excludes the following types of costs from protection under this exception to the information blocking rule:

- The types of fees that covered entities may not impose under the HIPAA Privacy Rule for requests by an individual for a copy of PHI. Examples of these prohibited costs include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; and recouping capital for data access, storage, or infrastructure.[25]

[25] See 45 CFR 164.524(c)(4): https://www.ecfr.gov/cgi-bin/text-idx?SID=7a76846e7aa7284ba0e5cb99dcdea8c4&mc=true&node=se45.1.164_1524&rgn=div8.

- A fee based in any part on the electronic access of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual. ONC distinguishes these fees from cost-based fees that a covered entity may charge individuals for copies of ePHI under HIPAA and similar allowable costs under state laws and which may be excluded under this exception.
- A fee to perform an export of EHI via the capability of health IT certified to the EHI certification criterion to switch health IT or to provide patients their EHI.
- A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

ONC clarifies that access to EHI that is provided by physical media (e.g., paper copies, or where EHI is copied onto a CD or flash-drive) would not implicate the information blocking rule as long as the fee charged for that access complies with the HIPAA Privacy Rule. The agency also adds a definition of electronic access for this exception; it means an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request. ONC further clarifies that electronic access involves completion of the process where no manual effort is required to fulfill the request at the time of the request. Manual effort involved in collating or assembling EHI from various systems in response to a request falls outside the definition.

ONC also reaffirms that this exception does not apply to practices where actors charge individuals a fee to access their EHI using an internet-based delivery method, including where the individual uses patient chosen apps, personal help apps and other consumer-directed technology to request or receive their EHI. ONC views these practices as inherently suspect.

ONC believes that costs relating to export and conversion of EHI in EHR systems are the types of costs specifically contemplated by the information blocking statute. ONC notes that providers often encounter rent-seeking and opportunistic pricing practices when they export EHI from their systems for use with other technologies that compete with or reduce revenue opportunities with an EHR developer's own products and services. ONC also notes that even where a fee to export or convert EHI is agreed to in writing at the time the technology was acquired, that fee must still comply with the other conditions of the exception.

However, ONC clarifies that a developer could still charge a fee to deploy EHI export capabilities in a health care provider's production environment or to provide additional services on top of those reasonably necessary to enable its intended use. Additionally, because the EHI certification criterion provides only a baseline capability for exporting data, developers of certified health IT may need to provide other data portability services to facilitate the smooth transition of data from health care providers between different health IT systems. Fees for those services may qualify for protection under the exception if they meet the conditions for this exception. These fees must be agreed to in writing when the technology is acquired.

c. Compliance with the Conditions of Certification.

ONC notes that a health IT developer of certified health IT subject to the API Condition of Certification[26] may not charge certain types of fees and also is subject to more specific cost accountability rules than apply under the exception. ONC finalizes its proposed condition that the developer must comply with all requirements of such conditions of certifications for all practices and at all relevant times to qualify for this exception from the information blocking rule. However, the agency does not finalize the proposal that an API Data Provider (including a health care provider that acts as an API Data Provider) may only charge the same fees that a Certified API Developer may charge to recover costs consistent with the permitted fees specified in the API Condition of Certification; its rationale for this decision is that not all permitted fees in the API Condition of Certification apply to API Data Providers.

8. License Exception (§171.303)

ONC states that the information blocking rule would be implicated if an actor refuses to license or allow the disclosure of interoperability elements to persons who require those elements to develop and provide interoperable technologies or services (including those that might complement or compete with the actor's own technology or services), or if the actor licenses interoperability elements subject to terms or conditions that have the purpose or effect of excluding or discouraging competitors, rivals, or other persons from engaging in pro-competitive and interoperability enhancing activities. The preamble to the proposed rule included examples of situations that do and do not implicate the information blocking rule. ONC remains concerned that the use of contractual and intellectual property rights to extract rents for access to EHI or to prevent competition from developers of interoperable technologies will undermine the fundamental objectives of the information blocking rule.

ONC proposed to establish an exception to permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, subject to certain strict conditions to ensure that actors license interoperability elements on those terms and that they do not impose collateral terms or otherwise impede use of interoperability elements. The agency finalizes its proposal with some modifications. The major changes in the final rule are that all references to the RAND framework in the regulation text are removed and the process and timeframe for negotiating a license are modified.

In response to general comments, ONC clarifies that an actor will not implicate the information blocking provision or have to use this exception where the entity requesting to license or use the interoperability element is not seeking to use the interoperability element to interoperate with either the actor or the actor's customers in order for EHI to be accessed, exchanged, or used. There must be a nexus between the requestor's need to license an interoperability element and existing EHI on one or more patients; a request must always be based on a need to access,

[26] The final rule states that this applies to requirements under 45 CFR 170.402(a)(4), 45 CFR 170.404, or both.

exchange, or use EHI at the time the request is made – not on the requestor's prospective intent to access, exchange, or use EHI at some point in the future.

ONC also explains that licensing agreements already in place that contravene the information blocking rules must comply with the new conditions of this exception as of the compliance date (i.e., six months after the date of publication of the final rule in the *Federal Register*). ONC expects actors to take immediate steps to comply with the information blocking rules.

As finalized, to qualify for this exception, each practice by an actor would have to meet the negotiating a license condition, the licensing condition, and additional conditions at all relevant times.

a. Negotiating a license condition

ONC had proposed to require actors to complete negotiations for the license or use within 10 days of receipt of a request to license or use an interoperability element. In response to comments, ONC substantially revises this condition. The final rule requires an actor to begin negotiations within 10 business days of receipt of a request and to complete negotiations within 30 business days.

ONC still expects the actor to negotiate with the requestor in good faith and in compliance with all the conditions of this exception. ONC reiterates that actors are not required to grant a license in all instances as long as the negotiations are conducted in good faith and an offer pursuant to those negotiations is made.

Throughout the proposed regulatory text of this exception, ONC referred to a request to "license or use" an interoperability element; in the final rule, it omits references to "use" because it believes "use" in this context is synonymous with license.

b. License condition

Commenters complained that compulsory licensing of health IT on RAND terms was inconsistent with the usual use of RAND for standards development and would not provide adequate protection for IP rights. In response, ONC removes all references to RAND in the final regulation text; however, it finalizes the majority of substantive conditions for the licensing of interoperability elements as proposed.

In response to comments, ONC clarifies or reiterates the following points. First, a practice that meets all the conditions of the exception will be protected if the actor demonstrates the requisite intent under the statute. Second, an actor (i.e., a health IT developer) is not required to license all of its IP; there must be a nexus to access, exchange or use of EHI. Third, if an actor licenses an interoperability element to one requestor, must license that same interoperability element to future similarly situated requestors with the same terms.

Scope of rights. In the final rule, ONC revises the proposed regulatory text to eliminate examples and to provide for a more streamlined expression of the requirement. An actor must license the requested interoperability elements to provide all rights necessary (i) to enable the access, exchange, or use of EHI and (ii) to achieve the intended access, exchange, or use of EHI through the interoperability element(s).

The agency clarifies that actors may require that licensees of the proprietary IP embodied in an interoperability element may only use that IP for the licensed purpose, so long as such limits are in compliance with all the conditions of the exception.

Reasonable royalty. If the actor charges a royalty for the use of interoperability elements, the royalty must be reasonable. Under the final rule, to be considered reasonable, a royalty must meet the following requirements:

- It must be non-discriminatory.
- It must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using EHI.
- If the actor has licensed the interoperability element through a standards developing organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on terms consistent with those in this exception, the actor may charge a royalty that is consistent with those policies.
- An actor may not charge a royalty for intellectual property if the actor recovered any development costs under the Fees Exception in §171.302 that led to the creation of the intellectual property.

ONC makes two modifications to the proposed regulation text. It removes references to RAND terms throughout, and it adds a fourth criterion to preclude an actor from a double recovery of costs under this exception and the Fees Exception.

Non-discriminatory terms. This proposed criterion is finalized as proposed with non-substantive language changes in the regulation text. The terms on which an actor licenses and otherwise provides the interoperability elements must be non-discriminatory; this applies to terms that relate to the price as well as other terms such as royalties. The actor must comply with the following requirements:

- The terms must be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons and requests.
- The terms must not be based in any part on—
    - Whether the requestor or other person is a competitor, potential competitor, or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor; or
    - The revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements.

ONC notes that actors do not have to apply the same terms for all persons requesting a license; however, differences in terms must be based on actual, legitimate differences in costs the actor incurs or on other non-discriminatory criteria that are objectively verifiable. For example, an actor could provide more favorable terms under a joint venture or co-marketing agreement than it might provide under an arm's length transaction. However, ONC reminds developers of certified health IT that the Condition of Certification under §170.404 precludes the developer from offering APIs on different terms.

Collateral terms. ONC finalizes without change from the proposed rule 5 additional conditions that it believed would provide "bright-line prohibitions" for certain types of collateral terms or agreements that interfere with access, exchange, or use of EHI. To qualify for this exception, an actor may not require a licensee or its agents or contractors to do, or to agree to do, any of the following:

- Not compete with the actor in any product, service, or market.
- Deal exclusively with the actor in any product, service, or market.
- Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.
- License, grant, assign, or transfer to the actor any intellectual property of the licensee.
- Pay a fee of any kind (other than a reasonable royalty described above) unless the practice meets the requirements of Fees Exception at §171.302 for costs reasonably incurred.

Non-disclosure agreement. ONC finalizes its proposal to allow an actor to require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets. The agreement must specify all information the actor claims as trade secrets, and the information must meet the definition of a trade secret under applicable law.

In response to comments, ONC clarifies the following points. First, interoperability elements may be protected as trade secrets; trade secrets are a type of IP that consist of information and can include, for example, a formula, pattern, compilation, program, device, method, technique, or process which may fall under the definition of interoperability element. Second, ONC is not requiring non-disclosure agreements. Third, ONC does not permit to permit actors to "generally" identify the information they claim as trade secrets.

c. Additional requirements relating to the provision of interoperability elements

To qualify for this exception, an actor may not engage in any practice that has any of the following purposes or effects:

- Impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose.
- Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

- Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

This criterion is unchanged from the proposed rule. ONC says the intent behind these additional conditions is to ensure that actors who license interoperability elements do not engage in separate practices that impede the use of those interoperability elements or otherwise undermine the intent of this exception. ONC notes these additional conditions address a broader range of practices that may not be affected through license agreements or that occur outside licensing negotiations. ONC reiterates that this criterion does not prevent an actor from making improvements to its technology or responding to its customers' or users' needs; however, the actor's practice must be necessary to accomplish these purposes, and the actor must provide the licensee a reasonable opportunity to update its technology to maintain interoperability.

c. Compliance with conditions of certification

ONC removes this proposed condition in the final rule because it believes it is unnecessary for purposes of this exception.

C. Additional Exceptions—Request for Information

In the proposed rule, ONC sought comment on whether it should propose in future rulemaking a narrow exception to the information blocking rule for practices that are necessary to comply with the requirements of the Common Agreement. It received many comments reflecting a variety of viewpoints that it will consider for future rulemaking.

ONC also welcomed comment on potential additional exceptions it should consider for future rulemaking. It received a number of suggestions for new exceptions as follows.

- For sensitive and/or privileged information. ONC responds that actors could seek protection under a number of the final exceptions, including exceptions for preventing harm, privacy, security, or infeasibility.
- For research. ONC responds that protection for research may be available under the final exceptions for privacy or infeasibility. Also, where federal or state law prohibits access, exchange or use of EHI, actors are not required to share it.
- For independent opinions from external validators regarding business practices. ONC responds that it is not restricting an actor's ability to hire a private company to assess its business practices.

D. Complaint Process

Section 3022 requires ONC to implement a standardized process for the public to submit reports on claims of health information blocking and that collects certain information, such as the

originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information. In the proposed rule, ONC indicated that it would implement the process by building on existing mechanisms, including the current complaint process at https://www.healthit.gov/healthit-feedback, and it sought comment on its approach.

ONC received a variety of comments on its approach, including a request that the public be permitted to submit comments on operational details before the complaint process goes live. ONC responds that it is not required by law to undergo notice and comment rulemaking to implement the complaint process. It will publish information materials with the rollout of the complaint process, and it intends to evolve the process over time based on experience with the complaint process and stakeholder feedback.

In response to other comments, ONC will not make complaints publicly available. Additionally, it will not require a complaint submission to meet any proof, evidentiary, or qualification standard as a pre-requisite for submission.

E. Disincentives for Health Care Providers - Request for Information

Section 3022 of the PHS Act requires the application of "appropriate disincentives" under existing federal law for health care providers who violate the information blocking rule, and directs the Secretary to establish those disincentives through rulemaking. ONC is concerned that existing law may be insufficient to cover the range of conduct that could fall under the information blocking rule.

ONC sought comment on existing disincentives, as well as potential modifications to them. It also sought feedback on avoiding duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved before the date of enactment of the Cures Act.

The agency reports having received more than 40 comments on this RFI; it says it has shared them with the relevant agencies. The comments focused on the need for disincentives, the magnitude of penalties, and enforcement.

Health care providers generally opposed additional disincentives noting than they are already subject to penalties for noncompliance with information blocking requirements under the QPP and the Promoting Interoperability Programs as well as fines imposed under HIPAA. The HITAC recommends that disincentives should be built into federal regulations for all departments and agencies of the federal government that contract with providers.

With respect to the magnitude of fines, providers suggested that any fines imposed on them be minimal (or tiered to address the magnitude of the violation) and that fines on developers should be substantial. Health IT developers returned the favor and suggested that providers should be subjected to higher fines.

Health care providers suggested that they should be allowed to come into compliance before being subjected to fines unless the violation was clear and egregious. They also recommended an appeals process, especially for small and rural providers.

VIII. Proposed Rule Requests for Information

In the proposed rule, ONC included two additional Requests for Information. One sought comment on issues regarding bidirectional exchange with registries and the other requested comment on issues pertaining to patient matching. The comments received are not discussed in the final rule, but ONC says it will use them to inform future rulemaking.

IX. Incorporation by Reference

In this section of the final rule, ONC provides summaries of the technical standards that it proposes to incorporate by reference into regulatory text, along with links to the standards themselves. These include standards related to exchange of EHI, core data for interoperability, and APIs.

X. Collection of Information Requirements and Regulatory Impact Analysis

With respect to collection of information requirements under the Paperwork Reduction Act (PRA), ONC estimates that the requirement that a health IT developer must retain compliance records for at least 10 years would require each developer to spend 2 hours per week at a total annual cost across all health IT developers of $47,632. Other reporting requirements in the final rule are either considered minimal burden or are not subject to the PRA.

OMB has determined that this final rule is economically significant (i.e., the potential costs could be greater than $100 million annually) and ONC provides a detailed regulatory impact analysis of this final rule. The analysis concludes that in the aggregate, the net benefit of the final rule would fall in the range of $953 million to $2.6 billion for the first year after it is finalized averaging $1.8 billion. The total "perpetual" annual net benefit starting in year 2, would range from $366 million to $1.3 billion, averaging $840 million. These estimated benefits are significantly lower than what CMS estimated in the proposed rule based on its finalized policies and changes regarding its estimated costs. For most estimates a wide range of possible dollar effects is provided because of the uncertainty of the precise impact of the final rule policies, and ONC notes that not all the effects of the policies, in particular benefits, can be quantified.

The aggregate figures are summarized as follows, based on a simple average of the wide ranges provided:

- First-year aggregate costs of $1.8 billion would be borne primarily by IT developers, with a small percentage of costs borne by ONC-ACBs and the ONC itself. These costs would be more than offset by estimated aggregate annual benefits of $3.1 billion, including

benefits attributable to the entire health care system, including hospitals, clinicians, payers, and patients (Costs in the second year and later are lower, averaging $840 million, as one-time costs attributed to the first year would no longer apply.) The benefits to providers assume that certain developer costs are passed through (e.g., development and maintenance of EHI export and API functions).

- The finalized policies that are estimated to generate the greatest cost burden on an estimated 458 health IT developers are one-time costs related to support for additional USCDI data elements ($192 million); development and maintenance of the EHI export criterion ($85 million); development and maintenance of APIs ($176 million); and real-world testing ($47 million).

- While some cost savings would accrue to developers from the deregulatory actions, the main benefits would be gained by hospitals and clinicians from the addition of the data export criterion ($1.4 billion); the API criterion ($2 billion) and real world testing ($296 million).