hfma
healthcare financial management association

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

[RIN 0955-AA01]

On March 4, 2019, the Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS), published in the *Federal Register* a proposed rule that would implement certain provisions of the 21st Century Cures Act. The provisions for implementation are concerned with conditions and maintenance of certification requirements for health information technology (health IT) developers under the ONC Health IT Certification 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. Also proposed are 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. **The deadline for submission of comments is Monday, May 3, 2019.**

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 Recover 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 the technological capability, functionality, and security requirements adopted by HHS.

The 21st Century Cures Act (Cures Act) (Pub. L. 114-255), signed into law on December 13, 2016, made changes to the PHS Act related to health IT. In the proposed rule, ONC provides draft 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 of 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 (OUD));
- 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

The Cures Act required the Secretary, in consultation with stakeholders, to develop a strategy and recommendations to reduce the regulatory and administrative burdens associated with the use of EHRs by December 2017. Additionally, 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. ONC describes prior experiences with regulatory reform initiatives and provides examples of past actions taken to reduce Program burden (e.g., adopting a gap certification policy).[2] In support of the 2016 and 2017 reform initiatives, ONC undertook a year-long evaluation of existing regulations and identified 6 deregulatory actions that are included in the proposed rule. **ONC welcomes comment on the proposed deregulatory actions and any other potential deregulatory actions that should be considered.**

A. Removal of Randomized Surveillance Requirements

ONC Authorized Certification Bodies (ONC-ACBs) must conduct in-the-field surveillance of certified health IT for continued conformance to certification requirements. ONC-ACBs currently perform reactive surveillance (e.g., in response to complaints) and must randomly surveil 2% of the certificates they issue annually. Stakeholders have stated that the provider time burden of random surveillance exceeds the potential benefit, and they support reactive surveillance alone as more logical and economical. ONC believes that performing only reactive surveillance also would create time and flexibility for ONC-ACBs to invest in their other activities. Therefore, ONC proposes regulatory changes at §170.556(c) such that ONC-ACBs could, but would not be required, to conduct random surveillance. Existing methodology followed by ONC-ACBs during random in-the-field surveillance would not be changed.

B. Removing the 2014 Edition from the Code of Federal Regulations (CFR)

Rulemaking for the ONC Health IT Certification 2014 Edition was completed in 2012 and ONC believes that edition has become increasingly outdated. ONC proposes to remove the 2014 Edition in its entirety from the CFR and believes that the benefits of so doing would include:

- The 2015 Edition would become the sole baseline for health IT certification.
  - Health IT developers would no longer be required to support maintenance infrastructure and updates for two distinct editions and could focus innovation efforts on the requirements of a single edition.
  - ONC-ACBs and ONC-Authorized Testing Laboratories (ATLs) would no longer be required to support testing, certification, and surveillance for two distinct editions.
  - Confusion and error potential would be decreased for healthcare providers who would be using EHRs built to a single set of criteria and standards.
- Widespread adoption of the 2015 Edition and its improved interoperability compared to prior editions would better support use of EHI and produce cost savings.

[2] Gap certification allows health IT developers to use prior testing results when updating modules to a new Program edition for those certification criteria that are unchanged from the preceding edition.

- Alignment with the requirement by the Centers for Medicare and Medicaid Services (CMS) for participants in the Quality Payment Program (QPP) to utilize only the2015 Edition beginning in 2019.

To remove the 2014 Edition from the CFR, ONC proposes to remove the edition's certification criteria (§170.314) and its related standards, terms, and requirements found in multiple other sections. ONC notes that while references to the 2014 Edition in the Common Clinical Data Set (CCDS) would be removed, it is also proposing later in the rule to replace the CCDS definition with the United States Core Data for Interoperability standard, Version 1 (USCDI v1). Finally, ONC notes that 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).

C. Removing the ONC-Approved Accreditor (ONC-AA) from the Program

The ONC-AA has served to accredit certification bodies and to oversee the ONC-ACBs. Experience in interacting with the ONC-ACBs, however, have led ONC to conclude that ONC-AA activities are largely duplicative of ONC's oversight of ONC-ACBs. Therefore, ONC proposes to remove the ONC-AA from the Program, with ONC assuming all oversight of the ONC-ACBs. To accomplish this, ONC proposes to remove the ONC-AA definition (§170.502) and delete all references to the ONC-AA in other sections. ONC notes that removal of the ONC-AA would allow ONC-ACBs to obtain their accreditation from multiple entities rather than only through the ONC-AA,[3] and proposes to revise the ONC-ACB application accordingly (§170.520(a)(3)). ONC estimates overall annual cost savings from this regulatory removal would be $4,500.

D. Removal of Certain 2015 Edition Certification Criteria and Standards

ONC proposes to remove several certification criteria from the 2015 Edition that are included in the 2015 Base EHR definition. The criteria proposed for removal are shown below, sorted by the reasons offered for their removal. **ONC invites comment on the proposed removal of the identified criteria and standards below, and any other 2015 Edition criteria and standards that should be considered for removal.**

- No longer needed for CMS' Promoting Interoperability programs:
  - Problem List, Medication List, Medication Allergy List;
- Widely used, essential to clinical care, would be in EHRs if criterion did not exist:
  - Problem List, Medication List, Medication Allergy List, Smoking Status;
- Used for internally recording EHI rather than to support interoperability:
  - Problem List, Medication List, Medication Allergy List; or
- Would be captured in an interoperable form by USCDI:
  - Problem List, Medication List, Medication Allergy List, Smoking Status.

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

ONC also proposes to remove the following 2015 Edition criteria (not part of the 2015 Base EHR definition) for the reasons shown below.

- Drug Formulary and Preferred Drug Lists:
  - Functionality widely adopted and does not facilitate interoperability.
- Patient-Specific Education Resources:
  - No longer needed for CMS' Promoting Interoperability programs, and
  - Certification requirement may be constraining innovation.
- CCDS Summary Record (Create and Receive):
  - Little market demand, significant overlap with "transitions of care" criterion.
- Secure Messaging:
  - Inherent in other patient engagement criteria and included in patient portals.

ONC estimates 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 projection that some developers would still be newly certifying their products to these criteria in 2018 and 2019.

E. Removal of Program Disclosure Requirements

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 (information blocking). Elsewhere in this rule, ONC is proposing robust Conditions of Certification for health IT developers that address information blocking in detail and that will eliminate the necessity for and utility of the existing disclosure requirements. (See section VII below.) Therefore, ONC proposes to remove existing regulations (§170.523(k)(1)(iii)(B), §§170.523(k)(1)(iv)(B) and (C)) that would be replaced by the new Conditions of Certification and Maintenance information blocking requirements. Relatedly, health IT developers are currently required as a Principle of Proper Conduct (PoPC) to attest to their compliance with existing mandatory disclosure regulations (§170.523(k)(2)). ONC proposes to delete this PoPC as over 90% of developers have attested and the information to be disclosed is already easily available on developers' websites.

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

In 2019, the FDA will begin testing a pilot precertification program for software-based medical devices; under this program, approval shifts from the device level to the manufacturer level. Requests from sponsors who pass an Excellence Appraisal could be eligible for pre-market "streamlined review" of their products for safety and effectiveness, and the streamlined review could be applied to multiple products from any single manufacturer who has demonstrated excellence effectiveness.[4] ONC proposes to "recognize" health IT developers who are pre-

[4] The origins of the FDA pilot program are found in the FDASIA Health IT Report of 2014, issued by the FDA, ONC, and the Federal Communications Commission to describe a risk-based regulatory framework for health IT. The report, mandated by the FDA Safety and Innovation Act (FDASIA) (Pub. L. 112-144), is found at https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHRe

certified under the FDA's pilot program, exempting them from some testing and certification requirements of the ONC Health IT Certification Program for the 2015 Edition. The exemption would be applied initially to the "quality management systems" and "safety-enhanced design" criteria but ONC anticipates potential expansion to several other clinical certification criteria.[5] **ONC requests input on whether it should establish its own new regulatory processes that are based primarily on evaluating the health IT developers rather than their health IT products.** Factors that ONC might consider in evaluating developers for exemptions could include specific functionalities already demonstrated to ONC, prior successful certification under ONC's certification Program, and results from real-world interoperability testing. **ONC seeks more specific input on the health IT developer selection criteria, what the associated Conditions and Maintenance of Certification requirements should be, and any related operational concerns**.

III. Updating the 2015 Edition Certification Criteria

A. 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 proposes to make four exceptions in this rule:

- Replacing the Common Clinical Data Set (CCDS) with a government-unique standard, the USCDI (§170.213);
- Adopting a government-unique implementation specification, the API Resource Collection in Health (ARCH) Version 1 (§170.215(a)(2));
- Adopting market-driven consortia standards for application programming interfaces (APIs) (§170.215(a)(3) through (5)); and
- Replacing Health Level 7 (HL7) standards with government-unique standards to support the associated certification criterion's use case, reporting eCQM data to CMS (§170.205(h)(3) and (k)(3)).

ONC notes that compliance with the entire standard or implementation specification document would be required for each of the exceptions if finalized. (Summaries and URLs for the excepted materials are provided in section XI of the proposed rule).

ports/UCM391521.pdf The Excellence Appraisal would determine whether a manufacturer has demonstrated a robust culture of quality and organizational excellence and is committed to monitoring real-world performance.

[5] ONC indicates that expansion might include "computerized provider order entry", "drug-drug" and "drug-allergy interaction checks", "clinical decision support", and "implantable device list" criteria.

[6] National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 3701 et. seq.) and the Office of Management and Budget Circular A–11914.

B. Adopting the USCDI Standard: Background and Process[7]

In its early focus on CMS' EHR Incentive Programs (now called Promoting Interoperability). ONC relatedly defined a common set of meaningful use data types, elements, and associated vocabulary standards applicable to multiple certification criteria. As the Program expanded beyond CMS to generally emphasize open, accessible, and nationally interoperable EHI exchange, the common data set definition was renamed as the Common Clinical Data Set and its content revised for the 2015 Edition final rule. Stakeholders and ONC have come to believe that moving beyond the inherent limitations of the CCDS structure would enhance interoperability. ONC proposes to replace the CCDS definition with the USCDI standard and to remove the CCDS definition and all its references from the 2015 Edition. ONC further proposes to include in the USCDI v1 the newest versions of the CCDS "minimum standard" code sets that are available at the time of publication of a subsequent final rule. ONC notes several 2015 Edition certification criteria whose code sets might be updated as part of USCDI v1 adoption and **invites comments about any potential interoperability concerns that might be caused by the updates.**[8] ONC also states its intent to implement a process for future USCDI expansion that would be predictable, transparent, and open to stakeholder participation.

Certification criteria affected by the switch would include "transitions of care" (§170.315(b)(1)); "view, download, and transmit to 3rd party" (§170.315(e)(1)); "consolidated CDA creation performance" (§170.315(g)(6)); "transmission to public health agencies – electronic case reporting" (§170.315(f)(5)); and "application access – all data request" (§170.315(g)(9)).[9] Health IT developers would be required to update their certified modules for these 5 affected criteria once the USCDI is adopted in a final rule. Developers also would be required to provide the updated certified modules to all their customers whose health IT was certified to the CCDS-based criteria within 24 months after a final rule becomes effective. To comply timely, developers could update their modules without new mandatory testing but would be required to factor the update into their next real word testing plan (discussed further in section VI.B.5 below) and to notify their ONC-ACBs on the dates they achieve compliance.

The USCDI standard would comprise data classes containing groupings of specific data elements necessary for EHI exchange nationwide (e.g., "patient name" is an element of the "patient demographics" data class). ONC notes that the USCDI is agnostic to "content exchange" standards, and ONC believes that all data classes in the USCDI v1 can be supported by standards in common use, including HL7 C-CDA Release 2.1 and Fast Health Interoperability Resources (FHIR®). Relatedly, when adopting USCDI v1, ONC also proposes 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)(4)(i). The guide provides help and technical clarification for specifying data in the C-CDA Release 2.1, supporting data classes added by USCDI v1 (e.g.,

[7] Version 1 is available at https://www.healthit.gov/isa/sites/isa/files/inline-files/USCDI-v1-2019.pdf and is updated from the *Draft United States Core Data for Interoperability (USCDI)* that was made available for public comment.
[8] Potentially affected criteria are "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)).
[9] Two more criteria would be affected but are proposed for deletion and replacement: ""data export" (§170.315(b)(6)) and "application access – data category request" (§170.315(g)(8)).

Clinical Notes). Incorporating the guide would affect 6 certification criteria that reference C-CDA Release 2.1: “transitions of care” (§170.315(b)(1)); “clinical information reconciliation and incorporation” (§170.315(b)(2)); “care plan” (§170.315(b)(9)); “view, download, and transmit to 3rd party” (§170.315(e)(1)); “consolidated CDA creation performance” (§170.315(g)(6)); and “application access – all data request” (§170.315(g)(9)). ONC proposes to require health IT developers to update their certified modules that address the 6 affected criteria, once the USCDI is adopted in a final rule. Developers also would be required to provide updated certified modules to all their customers whose health IT was previously certified to the 6 criteria within 24 months after a final rule becomes effective. To comply timely, developers could update their modules without new mandatory testing but would be required to factor the update into their next real word testing plan and to notify their ONC-ACBs on the dates they achieve compliance.

C. Adopting the USCDI Standard: Specific Additions

ONC proposes to add the following to the current CCDS data classes and elements as part of USCDI v1: Address & Phone Number, Pediatric Vital Signs, Clinical Notes, and Provenance; and also proposes revisions to two data classes: Unique Device Identifier (UDI) and Medication.

Address & Phone Number. These proposed elements would align with existing patient data matching elements.

Pediatric Vital Signs. These elements are optional under CCDS; their proposed inclusion in USCDI is intended to support the Cures Act mandate to expand voluntary health IT certification to specialties and settings not yet fully covered, while contributing to a patient’s longitudinal EHI.[10] **ONC requests comment on the inclusion of pediatric vital signs, especially about potential benefits and costs for all, not simply pediatric, stakeholders.**

Clinical Notes: Stakeholders have told ONC 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 proposes 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.[11] **ONC invites comment on whether to include additional note types.** ONC estimates a one-time cost to developers of $104 to $262 million to add the clinical note types list above.

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

[10] Elements would include head occipital-frontal circumference for children less than 3 years of age, BMI percentile per age and sex for youth 2-20 years of age, weight for age per length and sex for children less than 3 years of age, and the reference range/scale or growth curve, as appropriate.

[11] 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.

added-value when data exchange involves APIs that may lack the full clinical encounter context compared to exchange using the (typically larger) Consolidated Clinical Architecture (C-CDA) documents.[12] ONC proposes 3 data elements as part of the 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.

ONC further proposes that Provenance would be included in its proposed "API Resource Collection in Health" (ARCH) Version 1 implementation specification, as described in section VI.B.4 of below.

UDI. ONC identifies a potentially useful, recently released implementation guide (IG) for this USCDI data class dealing with implantable medical devices; the IG describes changes to improve UDI component data exchange (e.g., serial number, manufacturing date).[13] Given the IG's recent release, **ONC seeks comment on whether to adopt the IG as a requirement to be met under the UDI data class. ONC also requests comment on the cost and burden of complying with this potential requirement.**

Medication. Currently the Medication data class contains two data elements, Medications and Medication Allergies**. ONC seeks 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 non-medication substances based on SNOMED CT©.**[14]

D. Revising the Electronic Prescribing ("e-Rx") Criterion

ONC and CMS have historically aligned health IT certification criteria with Medicare Part D e-Rx standards. CMS has finalized retiring NCPDP SCRIPT version 10.6, the current standard, and adopting NCPDP SCRIPT 2010771 as the new standard beginning January 1, 2020; the transition is contingent upon adoption of NCPDP SCRIPT 2010771 by ONC as the standard for its "e-Rx" certification criterion. Therefore, ONC proposes adopting NCPDP SCRIPT 2010771 for all transactions listed in its current "e-Rx" criterion (§170.315(b)(3)) along with those adopted by CMS for NCPDP SCRIPT 2010771 (42 CFR 423.160(b)(2)(iv)). Transactions to be included under the new "e-Rx" certification criterion are listed in the table below. ONC intends

[12] 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.

[13] Health Level 7 (HL7®) CDA R2 Implementation Guide: C-CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1-US Realm. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=486

[14] 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 and maintained by the non-profit entity Snomed International. http://www.snomed.org/snomed-ct/five-step-briefing

for its updated “e-Rx” criterion based on NCPDP SCRIPT 2010771 to be available by January 1, 2020; if finalized earlier, ONC will permit continued use of the current criterion (based on NCPDP SCRIPT version 10.6) until NCPDP SCRIPT 2010771 becomes effective in CMS’ Medicare Part D and QPP Promoting Interoperability programs.[15] Of note are the new transactions involving Risk and Mitigation Strategies (REMS), proposed by ONC and already adopted for Medicare Part D e-Rx. The FDA can require a REMS program from a manufacturer for a drug whose risks can outweigh its benefits when used in uncontrolled circumstances (e.g., opioids). REMS program complexity varies across drugs but all programs include periodic reporting of program efficacy to the FDA.[16]

[15] Clinicians, hospitals, and critical access hospitals have the option of reporting on a Query of Prescription Drug Monitoring Program (PDMP) quality measure in their respective Promoting Interoperability programs.

[16] The NCPDP SCRIPT 2010771 testing tool under development is being designed to support testing the proposed REMS transactions.

Transactions proposed for inclusion under the updated (NCPDP SCRIPT 2010771) “e-Rx” health IT certification criterion

Transaction Purpose	Transaction Terms	Sender	**Recipient**
Create new prescription	NewRx NewRxRequest NewRxResponseDenied	Prescriber Pharmacy Pharmacy	Pharmacy Prescriber Prescriber
Change prescription	RxChangeRequest RxChangeResponse	Pharmacy Prescriber	Prescriber/Payer* Pharmacy
Cancel prescription	CancelRx CancelRxResponse	Prescriber Pharmacy	Pharmacy Prescriber
Renew prescription	RxRenewalRequest RxRenewalResponse	Prescriber Pharmacy	Pharmacy Prescriber
Receive fill status notification	RxFill RxFillIndicatorChange	Pharmacy Prescriber	Prescriber/LTPAC** Pharmacy
Request and receive medication history	RxHistoryRequest RxHistoryResponse	Prescriber Varies	PDMP*** Prescriber
Query the mailbox for transactions	GetMessage	Prescriber/Pharmacy	Varies#
Relay acceptance of a transaction back to sender	Status	Recipient	Sender
Report that there was a problem with the transaction	Error	Recipient	Sender
Confirm receipt of a transaction that requests return receipt	Verify	Varies	Pharmacy/Prescriber
Request that additional supply of medication be sent	Resupply	LTPAC**	Pharmacy
Communicate drug administration events	DrugAdministration	Prescriber/Facility	Pharmacy/Other
Transfer prescription(s)	RxTransferRequest RxTransferResponse RxTransferConfirm	Pharmacy 1 Pharmacy 2 Pharmacy 1	Pharmacy 2 Pharmacy 1 Pharmacy 2
Recertify continued med administration order	Recertification	Facility (for Prescriber)	Pharmacy
Complete REMS transactions	REMSInitiationRequest REMSInitiationResponse REMSRequest REMSResponse	Varies Varies Varies	Varies Varies Varies

*For purposes of prior authorization; **Long-term or Post-Acute Care facility; ***Prescription Drug Monitoring Program; #May be PDMP or REMS Administrator

E. Electronic Health Information (EHI) Export

1. Overview

ONC proposes to add a new certification criterion for "EHI export" to the 2015 Edition and to the 2015 Edition Base EHR definition along with proposing the corresponding removal of the existing "data export" criterion (§170.315(b)(6)). ONC does not propose a transition period between the "data export" and "EHI export" criteria, and the "data export" criterion would be removed from the 2015 Edition effective with a final rule. Developer rollout of the "EHI export" criterion as part of a revised 2015 Edition Base EHR definition would be required within 24 months of the effective date of the final rule. ONC believes this timeline would suffice for health IT developers to create, test, and certify the new functionality and for providers to implement it. **ONC invites comment on the timeline while noting that the new criterion does not function in support of any CMS Promoting Interoperability program objective or measure.** ONC states that the proposed criterion represents a standards-agnostic first step towards a future-state of providing "persistent" (or continuous) access to patients' EHI through open, standards-based APIs. ONC adds that the minimum requirement of the new criterion would be a discrete data export capability rather than persistent, real-time EHI access, although refusal to provide persistent or real-time access where a developer could reasonably do so might raise information blocking concerns. The new criterion is intended to support two specific use cases: exporting a single patient's entire EHR upon request by the patient (patient access) and exporting the entire health IT database for a patient group upon request by a provider (system transition).

2. Scope

The scope of the "EHI export" criterion would encompass all EHI that a health IT system "produces and electronically manages" for a patient or a patient group and applies to that health IT product's entire database. Included would be clinical, administrative, and claims data; data stored in separate data warehouses would also fall under this criterion. Applicable EHI also would range from the oldest to the most recently available for the patient or patient group regardless of electronic format (e.g., includes PDFs). **ONC requests comment on whether the capability to permit providers to request time-delimited, exported EHI should be required as part of the criterion (e.g., "the past month of EHI").**[17] The proposed criterion refers to EHI rather than to EHRs and would apply to imaging information stored outside of EHRs. **ONC seeks comment about the minimum image elements that should be shared and would be needed for data transfer under the proposed criterion (e.g., image type, narrative text). Comment is also sought on whether health IT developers should be required to attest to the types of EHI they cannot support for export or publish that information with the export format documentation.** Finally, ONC proposes metadata categories for exclusion from the "EHI export" criterion as those present in internal databases used for physically storing the data (e.g., internal database field names); potentially unnecessary for interpretation of the exported EHI (e.g., encryption keys, local codes for internal use); or refers to data not included in the EHI

[17] Section VI.B.2 discusses the proposed timeframe in which developers of certified health IT would be required to certify to the proposed "EHI export" criterion and make it available to their customers.

export (e.g., links to external attachments). **ONC invites comment on metadata exclusion and inclusion categories as well as about types of EHI that might pose special challenges for meeting the "EHI export" as proposed.**

3. Export format

ONC notes that the proposed criterion does specify a content standard for the EHI export. However, to assist the receiving health IT system's processing of the EHI without loss of information or its meaning, developers would be required to provide the format for the exported EHI (e.g., data dictionary, export support file). ONC proposes to require that the developer's export format would be made available via a hyperlink that would be kept current by the developer. The export format could differ from that used internally by the sending health IT system. ONC notes that the proposed criterion does not specify how the exported information would be made available to the user or requestor; however, ONC expects that unreasonable burden would not be placed upon the user or requestor.

4. Patient access use case

ONC proposes that: 1) a user must be able to execute a single patient data export timely whenever the user chooses and without the necessity for health IT developer assistance; 2) the developer should enable efficient user data request and receipt without unreasonable burden (e.g., not requiring separate requests for different EHI types); 3) export delays would be permissible only to avoid interfering with the sending health IT system's other clinical functions; and 4) non-conformity with the criterion would exist if delays, detected by surveillance, resulted in a user receiving data that were no longer current, accurate, or valid. The typical user in this case would be a provider's office staff requesting EHI export on behalf of a patient. For provider-mediated requests, ONC proposes to mitigate privacy and security concerns by permitting design of modules certified to the "EHI export" criterion to incorporate limitations of user types able to access and initiate export functions. Limitations should be designed for discretionary use by the provider organization and not for user access prevention by developers. The "EHI export" criterion could allow direct patient data access using a technology application (e.g., API) rather than through a provider or other intermediary**. ONC requests comment as to whether the criterion should allow only the patient/authorized representative to be the export requestor.**

5. System transition use case

The "EHI export" criterion is also structured to support migration of health IT for a group of patients from one system to another when requested by a customer of the originating system (e.g., a provider plans to implement new health IT). The originating developer would have flexibility to meet the request (e.g., successfully exporting could require the receiving providerto obtain support from the originating developer) but must do so in a timely and efficientmanner.

Health IT developers would be required to assure the provision of reasonable cooperation and assistance.[18]

6. Impact

ONC estimates a one-time cost to developers of $9 to $88 million plus an annual cost of $9 to $88 million related to the “EHI export” criterion.

F. Privacy and Security Attestations

1. Authentication credential encryption

ONC proposes to adopt a new “encrypt authentication credentials” certification criterion (§170.315(d)(12)). While the 2015 Edition already requires encryption of EHI saved on end-user devices (§170.315(d)(1)) and specifies an encryption standard[19] (§170.210(a)(2)), encryption has not been explicitly required for the credentials used to access the EHI. ONC proposes that the new criterion would apply to any 2015 Edition certified module and to all future modules. A “Yes” attestation would mean that authentication credentials, if stored, are encrypted according to the standard. Testing to the criterion would not be required but certified modules would be subject to ONC-ACB surveillance. A “No” attestation means that any stored credentials are not encrypted. Although a “No” response is sufficient to satisfy the new criterion, this response would be made publicly available on the CHPL. ONC proposes that health IT initially certified after the effective date of a final rule would need to meet the new criterion at the time of certification. Health IT certified prior to the final rule’s effective date would be required to certify to the new criterion within 6 months after the effective date. **ONC invites comment on modification of the proposed criterion to explicitly accommodate health IT that is not designed to store authentication credentials, as has been done for the “end-user device encryption” criterion (§170.315(d)(7)(ii)).**

2. Multi-factor authentication (MFA)

ONC also proposes to adopt a new “multi-factor authentication” certification criterion (§170.315(d)(13)), noting that single-factor authentication is particularly prone to cyber-attack. ONC proposes that the new criterion would apply to any 2015 Edition certified module and to all future modules. A “Yes” attestation would mean that the certified module supports authentication of user identity through multiple elements to industry recognized standards.[20] ONC proposes that health IT initially certified after the effective date of a final rule would need to meet the new criterion at the time of certification. Health IT certified prior to the final rule’s effective date would be required to certify to the new criterion within 6 months after the effective date. ONC enumerates some of the challenges inherent to MFA, including the interference with

[18] Proposed assurances (§170.402) required of health IT developers are reviewed in section VI.B.2.

[19] 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

[20] 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.

clinical workflow by an added authentication step(s), the continued use of passwords in most MFA applications, the as yet unknown extent to which MFA mitigates security risks in the healthcare setting, and unmeasured MFA costs. **ONC requests comment on the general value of adopting the criterion as proposed, on the method for attestation, and about requiring additional information when a developer attests "Yes"** (e.g., the MFA technique used).

3. Impact

ONC assesses the costs associated with the new attestations to be de minimis.

G. Data Segmentation for Privacy (DS4P) and Consent Management Criteria

1. Background

Section IV.B.7 of the preamble (and this summary section III.G), address several topics related to data segmentation (restriction) for achieving EHI privacy protection while still facilitating interoperable EHI exchange. Two DS4P certification criteria ("DS4P-send" and "DS4P-receive") were adopted in the 2015 Edition final rule; these support data exchange using C-CDAs tagged as restricted, and subject to re-disclosure restrictions, at the document level. Security labeling allows proper data handling across computer systems and enables access-control decisions. The DS4P standard and associated HL7 Healthcare Classification System (HCS) specifications describe security label application to HL7 CDA documents; the labels facilitate a common understanding between the sender and recipient of the record about the privacy policies to be applied when handling sensitive EHI (e.g., substance abuse treatment, child abuse) captured in the record. ONC characterized adopting the initial two DS4P criteria as a first step on a glide path towards using technical standards to ensure interoperable sharing of sensitive EHI in accordance with applicable laws, policies, and patient preferences. ONC notes that only about 20 products were certified to the initial 2015 Edition DS4P criteria by the startof the third quarter of calendar year 2018. Stakeholders have told ONC that targeting certification to the document level is insufficient to meet provider needs for more granular segmentation, resulting in burdensome manual clinical workflow usage in complex DS4P use cases (e.g., pediatric care, behavioral health). Stakeholders have also requested that ONC explore health IT standards that could work with DS4P to manage consent for sharing documents with segmented data (e.g., through API use). ONC, therefore, is proposing a next step on the glide path beginning with removal of the existing "DS4P-send" and "DS4P-receive" criteria effective with a subsequent final rule.

2. Implementation using C-CDA

ONC proposes replacement certification criteria using C-CDA and the HL7 DS4P standard: a new "DS4P-send" (§170.315(b)(12)) and a new "DS4P-receive" (§170.315(b)(13)). The new criteria would require capability for security tagging at the document, section, and entry levels. This enhanced capability could support more practice settings and use cases (e.g., pediatric care, behavioral health), reduce the use of burdensome workarounds by providers, and potentially increase care efficiency while reducing costs. **ONC welcomes comment on the DS4P criteria removal and replacement as proposed.**

3. Implementation using FHIR

ONC reports having worked with the Substance Abuse and Mental Health Services Administration (SAMHSA) in developing the Consent2Share application. Consent2Share is an open source application for data segmentation and consent management designed to integrate with existing FHIR systems to provide privacy protections for patients with substance use disorders who are covered by the federal confidentiality regulation, 42 CFR Part 2. The associated FHIR implementation guide (Consent IG) created by SAMHSA describes how Consent2Share uses the FHIR Consent resource to represent patient consent for treatment, research, or disclosure.[21] ONC expects that their proposed new 2015 Edition certification criterion "standardized API for patient and population services" if finalized would accelerateAPI development. ONC further expects that API infrastructure could be leveraged by the health IT industry for secure, scalable sharing of segmented data. Therefore, ONC proposes to add a new certification criterion "consent management for APIs" (§170.315(g)(11)) for support of data segmentation and consent management in accordance with the FHIR-based Consent IG. Health IT module certification to the new criterion would indicate a system's capability to use an API with standards-based security labeling when responding to requests for patient consent directives. Certification to this criterion would be discretionary for health IT developers.

ONC notes a version mismatch on the glide path: the Consent IG for support of the new criterion is based on the newer FHIR Release 3 while the "standardized API for patient and population services" references FHIR Release 2. ONC identifies the mismatch's origin: SAMHSA prepared an IG using FHIR Release 2 whose implementation was curtailed for technical reasons, so SAMHSA moved quickly to an IG based on FHIR Release 3. ONC chose the FHIR Release 3 IG for its new criterion due to that guide's broader range of use cases that are desired by stakeholders (e.g., HIV/AIDS and reproductive health); further, ONC anticipates that developers electing to certify to the new criterion would be facile with both FHIR 2 and FHIR 3. Standards version alignment could also be facilitated by the proposed Standards Version Advancement (see section VII.B.5 below.) [22]

4. Impact

ONC estimates a one-time cost to developers of $2.4 million to $7.4 million related to the new criteria.

ONC invites comment on the proposed "consent management for APIs" criterion and its applicability to a greater range of use cases; using other API-based options and resources in creating additional certification criteria; and the potential burden to developers and

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

[22] In brief, this process allows a developer discretion to voluntarily use a newer version of a previously adopted standard if certain defined conditions are met.

implementers due to the FHIR version mismatch involving the proposed new criterion. ONC ends by noting SAMHSA's ongoing work to expand data segmentation use cases while addressing FHIR compatibility.

H. Other New and Unchanged Certification Criteria

1. 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 implementation guides. 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 proposes to reduce the burden of multiple standards for developers and providers by removing the HL7 QRDA standards from the 2015 Edition CQMs, while also requiring that certification to the "CQM–report" criterion would ensure support of the most recent CMS QRDA I (for hospital reporting) and QRDA III (for eligible providers) IGs available when the subsequent final rule is issued. **ONC invites comment on whether to allow health IT modules certified to the "CQM–report" criterion to be tailored only to the standard (QRDA I or III) that matches the care setting targeted by the module's developers**. Finally, ONC notes that the emerging FHIR standards combined with APIs are likely to prove more efficient for quality reporting than current approaches, and **ONC seeks comment on the potential replacement of QRDA-based reports by FHIR-enabled APIs**.

2. Standardized API for Patient and Population Services

As part of Cures Act implementation, ONC proposes 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. Features of the proposed criterion include required use of FHIR standards, adoption of several implementation specifications, and support for the two "EHI export" criterion use cases (i.e., patient access and system transition). The API criterion is discussed in section VI.B.4 below.

3. Program Reference Alignment for Otherwise Unchanged Criteria

ONC remarks on the renaming by CMS of its EHR Incentive programs to Promoting Interoperability programs. To align with the name change, ONC proposes to replace references to the incentive programs with the new name in two otherwise unchanged criteria: "automated numerator recording" (§170.315(g)(1)) and "automated measure calculation" (§170.315(g)(2)).

IV. Modifications to the ONC Health IT Certification Program

A. Corrections and Other Updates

ONC describes a set of regulatory changes that include clarifications, corrections, and codification of previously issued guidance:

- Codifying guidance about exemptions from the "end-user device encryption" criterion that are applicable to the "auditable events and tamper resistance" criterion;
- 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); and
- Removing a cross-reference that references testing that is no longer a part of certifying to the "view, download, and transmit to 3rd party" criterion.

ONC also proposes to update the 2015 Edition Privacy and Security 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" (discussed in section III.F of this summary). Other updates to the framework could be required during final rulemaking to accommodate the proposed changes to the 2015 Edition Base EHR definition criteria (e.g., problem list removal), if finalized (discussed in section II.D above). A draft table that accounts for adding the "encrypt authentication credentials" and "multi-factor authentication" criteria but not for changes to the Base EHR criteria is presented as Table 1 in the rule.

B. Principles of Proper Conduct (PoPC)

1. ONC-Authorized Certifying Bodies

Records retention. ONC proposes to revise and clarify the records retention requirement for ONC-ACBs (§170.523(g)). The 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 be clarified to begin with the codification of an edition of certification criteria in the CFR and to extend through the rulemaking effective date that removes that edition from the CFR. The ONC-ACBs also would be required to make records available upon to HHS upon request during the entire retention period (life of the edition plus 3 years).

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

- ONC-ACBs now would be permitted to evaluate and certify health IT modules that have not first passed through an ONC-ATL for conformance with certification criteria;

  - Methods to determine conformity would require approval in advance by the National Coordinator;
    - Methods could range from testing with an ONC-ATL to health IT developer self-declaration.
  - Certification by an ONC-ACB could only be issued to health IT modules and not to "Complete EHRs", as "Complete" certification is not available under the 2015 Edition and the 2014 Edition would be removed from the Program and the CFR.
- ONC-ACBs would no longer be able to use test results from National Voluntary Laboratory Accreditation Program (NVLAP)-accredited testing laboratories for determining conformance;
  - The regulatory transition period from NVLAP-accredited labs to ONC-ATLs has expired.
  - The provision allowing gap certification is proposed for removal along with other parts of the 2014 Edition;
    - The gap provision already is no longer functional; its applicability required the absence of interval new certification criteria and all modules now eligible for certification to the 2015 Edition would have at least one new or revised certification criteria.

Acceptable Test Results. ONC proposes 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[23] because: 1) all ONC-ATLs are accredited by NVLAP and authorized to participate in the certification Program by ONC, and 2) all ONC-ATLs must conduct testing using test methods approved by ONC against established certification criteria. Thus all ONC-ATLs are held to the same set of standards. Further, should an ONC-ACB have concerns about a specific ONC-ATL's results, the ONC-ACB would have an opportunity to share those concerns with ONC or NVLAP; ONC would make the final determination about acceptability of the test results on a case-by-case basis.

Mandatory Disclosures and Certifications. ONC proposes to remove a provision that addresses certification issued to a pre-coordinated, integrated health IT module bundle as such bundles are no longer certifiable under the Program. Finally, ONC proposes to extend the required public disclosure of all types of user costs and fees charged by an ONC-ACB-certified health IT developer for usage of its certified health IT modules, regardless of whether such usage is for HHS programs or for another purpose within the scope of the developer's certified health IT.[24]

2. <u>ONC-Authorized Testing Laboratories</u>

ONC proposes to make changes to the records retention requirements for ONC-ATLs that parallel the changes proposed for ONC-ACBs (i.e., related to "life of the edition").

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

[24] Additional PoPCs for ONC-ACBs are proposed and discussed in sections VI.B.5 and VI.D of this summary.

V. Health IT for the Care Continuum

A. Health IT for the Pediatric Setting

ONC reiterates that the initial focus of its health IT certification program was to support CMS' EHR Incentive Programs. With adoption of the 2015 Edition final rule, ONC purposefully expanded its certification program to be more open and accessible to a broader range of health IT including previously unaddressed care and practice settings, but without creating a series of more narrowly focused, separate, parallel certification tracks. Section 4001 of the Cures Act directs the Secretary to make recommendations and adopt certification criteria in support of the voluntary certification of health IT for the care of children, and ONC complies by addressing pediatric health IT needs within the context of ONC's existing, overarching certification program. ONC details its efforts to collaborate with stakeholders (e.g., American Academy of Pediatrics, AAP) and to incorporate available resources (e.g., Children's Model EHR Format) into recommendations for and design of certification program criteria to meet the needs of pediatric healthcare providers.[25]

1. Proposed Recommendations for Voluntary Certification of Health IT for Pediatric Care

ONC's process to formulate recommendations included reviewing AAP's 8 clinical priorities and correlating them with the detailed technical requirements of the Children's Format. Of ONC's 10 recommendations, listed below, the first 8 are based upon the AAP-identified priorities and the final 2 were added by ONC based on stakeholder input.

- Use biometric-specific norms for growth curves and support growth charts for children;
- Compute weight-based drug dosage;
- Ability to document all guardians and caregivers;
- Segmented access to information;
- Synchronize immunization histories with registries;
- Age- and weight- specific single-dose range checking;
- Transferrable access authority;
- Associate maternal health information and demographics with newborn (referred to later in the rule by ONC as "recommendation 8"); and,
- Track incomplete preventative care opportunities
- Flag special health care needs

2. Proposed Certification Criteria and Standards for Pediatric Health IT

a. Existing 2015 Edition Criteria and Standards that Support the Recommendations
(These 13 criteria do not reflect any of the updates proposed for them in the rule. Criteria having proposed changes, other than purely technical revisions, are indicated by an *.)

[25] Portions of the Children's Format are available at https://ushik.ahrq.gov/mdr/portals/cehrf?system=cehrf.

(i)* *"API functionality"(§170.315(g)(7)-(g)(9))*
May assist caregivers (e.g., parents, guardians) by allowing them to aggregate and manage health information from multiple sources in a web or mobile application of their choice.

(ii) *"Care plan" (§170.315(b)(9))*
The structured format may facilitate care coordination by caregivers

(iii) *"Clinical decision support" (CDS) (§170.315(a)(9))*
Enables interventions based on captured biometric data

(iv)* *CCDS standard (§170.315(b)(4) and (b)(5))*
Includes pediatric vital sign elements as optional

*(v) "*DS4P-send" and "DS4P-receive" (current) (§170.315(b)(7) and (b)(8))*
Support security labeling at the document level for sensitive EHI

(vi) "Demographics" (§170.315(a)(5))
Captures information that improves data matching; matching complexity is increased for children (e.g., matching maternal and newborn data)

*(vii) * "Electronic Prescribing" §170.315(b)(3))*
Includes options within the NCPDP SCRIPT 10.6 standard related to weight-based dosing and limits use of metric standard units, as metric units are not uniformly used for pediatric dosing

(viii) "Family health history" (§170.315(a)(12))
Familial conditions often play a key role in pediatric care

(ix) "Patient health information capture" (§170.315(e)(3))
Facilitates documentation of decision-making authority of patient representative(s) (e.g., guardian)

(x) "Social, psychological, and behavioral data" (§170.315(a)(15))
Supports integration of behavioral health data using SNOMED CT® and LOINC® codes[26]

(xi) "Transitions of care" (§170.315(b)(1))
Structured summaries may facilitate care coordination

(xii) "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

(xiii) "View, download, and transmit to 3rd party" (VDT) (§170.315(e)(1))
Transferrable access authority allows data access by patient representatives (e.g. parents)

b. New/Revised 2015 Edition Criteria and Standards (as proposed) that Support the Recommendations

(i) *"Standardized API for patient and population services" (§170.315(g)(10))*
Facilitates access, exchange, and use of EHI "without special effort" as required by the Cures Act

(ii) *"DS4P-send" and "DS4P-receive"(new) (§170.315(b)(12)), (§170.315(b)(13))* and *Consent management for APIs" (§170.315(g)(11))*

[26] Logical Observation Identifiers Names and Codes (LOINC) is an international standard for identifying health measurements, observations, and documents. More information about LOINC can be found at https://loinc.org/

The DS4P criteria support security labeling at the document, section, and entry level for sensitive EHI in C-CDAs, and the "consent management" criterion adopts the FHIR-based IG for using the Consent2Share application developed by SAMHSA. Together these criteria support a more facile and granular approach for senders and recipients to the myriad, complicated issues of exchanging sensitive pediatric EHI, and may improve clinical workflows and reduce costs.

(iii) *"Electronic Prescribing" (§170.315(b)(11))*

Increased configurability of the NCPDP 2010771 standard

(iv) *USCDI standard (§170.213)*

The USCDI standard would replace the CCDS definition and requires use of pediatric vital signs data elements for all criteria that specify the USCDI.

3. Resource Guide Development

ONC believes that non-regulatory information resources can facilitate consistent health IT implementation in clinical settings and has collaborated with various stakeholders and governmental partners in resource development. ONC further believes that such a resource would bring value to pediatric health IT certification implementation although it does not mention participating in any pediatric-focused resource development that is underway or planned.

4. Comment Requests

a. Health IT Certification for Pediatric Care

ONC seeks input about the recommendations and criteria as proposed for voluntary certification of health IT for pediatric care, noting comments should be framed in the context of pediatric use cases and sites of service. ONC specifically invites comment about the following:

a) Relevant gaps, barriers, safety concerns, and resources (including available best practices, activities, and tools) that may impact or support feasibility of the recommendation in practice;
b) Effective use of health IT itself in support of each recommendation as it involves provider training, establishing workflow, and related safety and usability issues;
c) Whether any of the 10 recommendations should not be included in ONC's final recommendations for voluntary certification of health IT for pediatric care; and
d) Any certification criteria from the Program linked to the 10 recommendations that should not be included to support the specific recommendation.

b. Health IT for Opioid Use Disorder (OUD) Prevention and Treatment

ONC believes that health IT can contribute significantly in multiple ways across the healthcare continuum to the national effort to combat opioid use disorder, and provides the example of the advanced health IT that is required by new opioid-related measures being implemented by CMS across its Promoting Interoperability programs (Query of PDMP and Verify Opioid Treatment Agreement).[27] ONC briefly reviews some health IT implementation approaches that could support OUD prevention and treatment: the current 2015 Edition certification criteria; therevised or new 2015 Edition criteria as proposed; and current industry initiatives that intersect with ONC policy goals. During its review, ONC poses questions and invites input framed in the context of how ONC's existing and proposed Program requirements could support use cases related to OUD prevention and treatment.

1. 2015 Edition Certification Criteria

ONC identifies 5 existing criteria that could support care coordination and the prevention and detection of opioid misuse, abuse, and diversion:

- *"Transitions of care" (§170.315(b)(1))*
  - Structured summaries could facilitate accurate information exchange when apatient with OUD moves between providers or across care settings.
- *"Clinical information reconciliation and incorporation" (§170.315(b)(2))*
  - Incorporating data from external sources enhances record completeness, particularly valuable for OUD patients visiting multiple clinicians and using multiple pharmacies.
- *"Electronic prescribing" (§170.315(b)(3)); update proposed in the rule)*
  - Electronic transmission limits prescription tampering and diversion andallows prescription capture by PDMPs.
- *"Patient health information capture" (§170.315(e)(3))*
  - Data from sites not linked to EHRs could provide valuable information, as when an ambulance call to an OUD patient results in treatment (e.g., naloxone injection) but not transport to a healthcare facility.
- *"Social, psychological, and behavioral data" (§170.315(a)(15))*
  - This information is vital to the "whole-patient" approach inherent inMedicated-Assisted Treatment (MAT) of OUD.

ONC requests comment on 1) how these criteria, and what other 2015 Edition criteria, may be considered as clinical and interoperability priorities in OUD treatment or prevention, and 2) the value of developing a nonbinding informational resource or guide for OUD providers and care sites, focused for specific clinical priorities and use cases.

2. Revised or New 2015 Edition Certification Criteria

ONC lists 4 criteria or standards, proposed elsewhere in this rule for addition or revision to the 2015 Edition that could support treatment and prevention of OUD:

[27] Query of Prescription Drug Management Program (PDMP) tracks whether the prescriber of a Schedule II opioid queries the state's PDMP database about a patient's prescription history before providing an opioid prescription to the patient. Verify Opioid Treatment Agreement tracks whether the prescriber looks for the existence of an opioid treatment agreement when a patient's Schedule II opioid prescriptions cumulatively span ≥ 30 days.

- *USCDI (§170.213)*
    - This standard, proposed for adoption in place of the CCDS definition, would establish a minimum set of data classes required to be interoperable nationwide. The Provenance data class would attach information about the source of EHI, allowing the recipient clinician to assess the reliability of the transmitted data.
    - This standard would be eligible for the proposed Standards Version Advancement Process, allowing more rapid adoption of newer versions by health IT developers. **ONC invites comment about the added value of the Standards Version Advancement Process when applied across OUD care and practice settings.**
- *"Standardized API for patient and population services" criterion (§170.315(g)(10))*
    - By facilitating access, exchange, and use of EHI "without special effort" as required by the Cures Act, this criterion could enable collaborative, patient-driven, integrated care for individuals recovering from OUD.
- *"DS4P-send" and "DS4P-receive" criteria (§170.315(b)(12)), (§170.315(b)(13)) and "Consent management for APIs" criterion (§170.315(g)(11)) (as proposed)*
    - The DS4P criteria support security labeling at the document, section, and entry level for sensitive EHI in C-CDAs, and the "consent management" criterion adopts the FHIR-based IG for using the Consent2Share application developed by SAMHSA. Together these criteria support a more facile and granular approach for senders and recipients of OUD patient data that are subject to multiple privacy laws and regulations. **ONC requests comment about the potential for these criteria to improve the processes and methods for OUD information display in EHRs**.
- *"Electronic prescribing" (§170.315(b)(11)) (as proposed)*
    - The proposed criterion includes the addition of Risk Evaluation and Mitigation Strategy (REMS) messages, alerting prescribers and dispensers of opioids to their required REMS activities that would encourage proper patient screening and appropriate monitoring.

ONC seeks comment on the applicability of the above 4 criteria to the OUD use case.

3. Emerging Standards and Innovation

To inform future health IT policy, ONC regularly participates in health IT and standards initiatives that explore IT innovation and emerging standards. **ONC describes two initiatives and invites comment potential consideration of them as part of future ONC policy-making.**

a. Clinical Decision Support (CDS) Hooks

The Centers for Disease Control and Prevention's (CDC) Guideline for Prescribing Opioids for Chronic Pain has not been consistently utilized nationwide for multiple reasons, including the need for real-time access at the point of care. CDS Hooks is an emerging health IT specification that invokes patient-specific clinical decision support from within a clinician's EHR workflow. ONC and CDC are collaborating to translate the opioid prescribing guideline into standardized, sharable, computer decision support-capable, code "artifacts" that ultimately could present the relevant guideline in real-time to the clinician who is accessing an OUD patient's EHR.

Although CDS Hooks is still an emerging technology, ONC seeks input about its adoption for opioid prescribing and OUD prevention and treatment. Comment is also requested on other health IT solutions and effective approaches to improve opioid prescription practices and clinical decision support for OUD.

b. Care Plan FHIR Resource

A shared care plan is a critical concept for managing an individual's health across a continuum that includes both clinical and non-clinical settings, as is typically required for patients in recovery from OUD. ONC has been exploring standards development that would allowtransition from current static care plan documentation to a dynamic shared care plan. ONC further notes that numerous efforts are underway within HL7 and other collaborations to standardize care plans and their content using FHIR and C-CDA. ONC envisions that USCDI, ARCH, and the proposed "standardized API for patient and population services" certification criterion (§170.315(g)(10)) could converge to allow a dynamic care plan accessed using a certified API. **ONC requests comment on the current maturity of existing and forthcoming technical specifications to support care plans and care plan data, as well as specific information that could be prioritized within a future USCDI data class focused on care plans.** ONC also encourages stakeholders to participate in the Interoperability Standards Advisory (ISA) process, the model by which ONC coordinates the identification, assessment, and public awareness of interoperability standards and implementation specifications. ONC indicates having plans to develop further ISA content to highlight standards and implementation specifications OUD/ substance use disorder

c. Additional Comment Areas

ONC requests comments concerning the following additional topics:

1) **Effective approaches (policy, technical, or combined) for the successful dissemination and adoption of standards (e.g., NCPDP SCRIPT 2017071) that can support the exchange of PDMP data for integration into EHRs and stimulate increased use of electronic prescribing for controlled substances such as opioids.**
2) **How successful implementation of health IT that supports OUD care can spur the achievement of national and programmatic goals, especially where they may align with initiatives across HHS (e.g., CMS Promoting Interoperability programs) and with stakeholder and industry led efforts.**
3) **Issues related to neonatal abstinence syndrome (NAS):**
   - **effective use of health IT to support the NAS use case, targeting provider training, workflow, and other related safety and usability considerations;**
   - **existing and potential tools (e.g., decision support or clinical quality measurement) for supporting children with NAS, as well as specific data elements needed in clinical care or for use of these tools in practice; and**
   - **Identification of any related criteria, and the respective corresponding proposed pediatric recommendation for the voluntary certification of health IT for use in pediatric care, that supports the NAS use case, including but not limited to**

recommendation 8.

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 proposes these 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 proposes 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 proposed 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 proposed 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.

B. Provisions

The proposed Conditions and Maintenance of Certification requirements are set forth in regulatory text in 45 CFR Part 70 in a new Subpart D, including sections 170.400 through 170.406.

1. Information Blocking (§170.401)

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

(b) *Maintenance of Certification*. No Maintenance of Certification requirements are proposed for this condition in this rule.

2. Assurances (§170.402)

(a) *Condition of Certification*. (1) A health IT developer would be required to assure 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.

(2) A health IT developer would have to 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 would result in assurances and documentation.

(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 VII.B.6 below for a discussion of the proposed 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 would be required to certify health IT criterion in §170.315(b)(10) regarding electronic health information export. This EHI export criterion is discussed in section III.E above.) For the maintenance of certification requirements, a health IT developer would be required to provide all of its customers of certified health IT with the health IT certified to the EHI export certification criterion within 24 months of the final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer. Finally, at proposed §170.550, ONC-ACBs would be required to certify health IT to the proposed 2015 Edition EHI export criterion when the developer of the health IT presented for certification produces and electronically manages EHI.

(b) *Maintenance of certification.* In addition to the proposed maintenance requirement pertaining to the EHI export described immediately above, another proposed maintenance of certification requirement is proposed pertaining to record retention. Specifically, ONC would require a health IT developer to 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 would apply 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 and others that many users of certified health IT participate in. (Section VI.D below includes more discussion of the records access.) ONC further proposes that if applicable certification criteria are removed from the CFR before the 10 years have expired, records would 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 proposed provision aligns with other records retention requirements for ONC-ACBs and ONC-ATLs under the Program.

ONC encourages comment on whether the assurances proposals would provide adequate assurances that certified health IT developers are demonstrating initial and ongoing compliance with Program requirements to support interoperability and appropriate exchange, access and use of EHI.

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

After reviewing the inception of the TEFCA[28], **ONC seeks 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 expects that such a requirement, if proposed in subsequent rulemaking, would apply to health IT developers that have a Health IT Module(s) certified to any of the certification criteria in §§170.315(b)(1), (c)(1) and (c)(2), (e)(1), (f), and (g)(9) through (11); and that provide services for connection to health information networks (HINs). These services could be routing EHI through a HIN or responding to requests for EHI from a HIN.

ONC believes that those health IT developers that certify health IT to the criteria listed above would be best suited to participate in the Trusted Exchange Framework and adhere to the Common Agreement. Such participation would provide assurances that developers are not taking actions that constitute information blocking or otherwise inhibit exchange, access and use of EHI.

ONC particularly welcomes comment on the certification criteria listed above as the basis for developer participation in TEFCA, whether other certification criteria would serve as a basis, and whether the current structure of the TEFCA are conducive to health IT developer participation and in what manner.

3. Communication (§170.403)

In this section ONC proposes a condition of certification to implement Cures Act requirements barring a health IT developer from prohibiting or restricting certain protected communications. ONC proposes a broad general rule with specific narrow exceptions.

[28] For more information on TEFCA, ONC refers readers to https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement.

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.

The proposed protections would apply regardless of the form or medium of the communication. Developers could not prohibit or restrict communications whether written, oral, electronic or any other method. The identity of communicators that would benefit from the protection would not be limited except that employees and contractors of the IT developer may be treated differently as specified in the permitted prohibitions and restrictions (described below). Customers, potential customers, patients, health IT researchers, industry groups, and health information exchanges would be able to make protected communications as would, for example, a data analytics vendor who is required to sign a non-disclosure agreement before being granted access to the developer's health IT.

In the preamble ONC lists examples of other protected communications: 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.

ONC proposes that this Condition of Certification would not be limited to formal prohibitions or restrictions (i.e., contracts or agreements) but would also encompass any conduct by a developer that would be likely to restrict a communication protected by the condition. The conduct would have to be designed to directly or indirectly influence the making of a protected communication, and any written terms would have to have the operative effect of restricting or prohibiting communication. Examples of conduct that ONC says could implicate the proposed communication condition of certification include taking steps to enforce a right that contravenes the condition or a legal right that purports to prohibit or restrict a communication (e.g., a cease and desist letter to a researcher who has made a protected communication); using a technological measure that a health IT user would need to circumvent to make a protected communication; making threats or taking retaliation against a person that has made a protected communication; having policies that disadvantage those who make protected communications; refusing to publish protected communications made in an online forum controlled by the developer; or causing the removal of protected communications from any publication.

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

ONC proposes to protect communications about whether a health IT product and developer 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 would be 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 proposed rule a developer could 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.

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

ONC says it believes that "if the user had the experience, the experience isrelevant."

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

For this provision ONC proposes that 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. Switching costs imposed by a developer would be considered protected communications.

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

This would include 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. A health IT developer could 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;

ONC seeks comment on whether the unqualified protection afforded to communications made to patient safety organizations should be limited by the nature of the patient safety organization or the nature of the communication, such as limiting to only material that was created by a patient safety work product (PSWP).

- Communicating information about cybersecurity threats and incidents to government agencies;

ONC seeks comment on whether it would be reasonable to permit health IT developers to imposed limited restrictions on these communications to safeguard the confidentiality and security of EHI. For example, should developers be permitted to require that users notify the developer about the existence of a security vulnerability prior to or simultaneous with any communication about the issue to a government agency?

- Communicating information 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.

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 would violate the condition of certification. A developer choosing to avail itself of a permitted type of communication prohibition or restriction would be required to 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 proposed rule:

- A health IT developer could prohibit or restrict the communications of its employees or contractors.
- A health IT developer could prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

ONC proposes that non-user facing aspects of health IT would include source and object code, software documentation, design specifications, flowcharts, and file and data formats. **ONC welcomes comments on whether these and other aspects of health IT should be treated as not being user-facing.** ONC believes that protecting the user-facing aspects of health IT is necessary to allowing communication of useful information about the usability or interoperability of the product or the experience of users and it is consistent with the treatment of software products under trade secret law.

- A health IT developer could prohibit or restrict communications that would infringe the intellectual property rights of the developer's health IT (including third-party rights), provided that the developer did not prohibit or restrict communications that would be a fair use of a copyright work and the developer did not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions on screenshots described immediately below.

ONC welcomes comments on whether it has struck an appropriate balance between protecting legitimate intellectual property rights of developers and ensuring that stakeholders who use and work with health IT can openly discuss and share experiences and information about its performance.

- A health IT developer may prevent communicators from altering screenshots other than to annotate or resize it, and may restrict disclosure of a screenshot on the basis that it would infringe third-party intellectual property rights provided that the developer first put all potential communicators on sufficient written notice of those parts of the screen display that contain trade secrets or intellectual property rights and cannot be communicated. In that case, communicators would still be permitted to disclose redacted versions of screenshots that do not reproduce those parts. In addition, developers could restrict communication of screenshots that include any HIPAA-protected health information unless the information was redacted, or the communicator has all necessary consents or authorizations to use the information.
- A health IT developer may prohibit or restrict communications that disclose information acquired only through participation in developer-led product development and testing. This permission would not apply to communications about the released version if it otherwise met the requirements under this Condition of Certification and the information communicated could be discovered by any ordinary user of the health IT.

To ensure that the permission is not abused such as by maintaining a product in beta release indefinitely, **ONC requests comment on whether it should limit the time for this testing protection to no longer than one year after release of the product or update, for example.** Further, ONC says that it expects that a product would be shared with *certain* customers before being made generally available to the market and **seeks comment on whether it should more specifically limit the extent a product can be distributed to customers for testing purposes.**

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

- Health IT developers would be required to issue a written notice to all customers and those with which it has agreements within six months of the effective date of the final rule that any communication or contract provision that contravenes the Condition of Certification regarding communication will not be enforced by developer. The notice would be required annually until the developer has amended the contract to remove or void the offending language. Further, the developer would have up to two years from the effective date of the rule to amend the contract or agreement to remove or void the contractual provision.

4. Conditions and Maintenance of Certification: Application Programming Interfaces

Section 4002 of the Cures Act requires the Secretary of HHS, through notice and comment rulemaking, to establish Conditions and Maintenance of Certification requirements for the Program. Specifically, health IT developers or entities must adhere to certain Conditions and Maintenance of Certification requirements concerning application programming interfaces (APIs) and other elements. ONC's approach in the proposed rule is to use the Conditions and

Maintenance of Certification to express both initial requirements for health IT developers and their certified Health IT Module(s) as well as ongoing requirements that must be met by both health IT developers and their certified Health IT Module(s) under the Program.

To implement the Cures Act's API Condition of Certification, ONC proposes new standards, new implementation specifications, and a new certification criterion as well as detailed Conditions and Maintenance of Certification requirements. The Base EHR definition would also be modified.

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 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 proposes to adopt standards, implementation specifications, and a new API certification criterion to implement the technical 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." The Cures Act's API Condition of Certification also states that a developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws."

ONC notes that these provisions include key phrases and requirements for health IT developers that go beyond just the technical functionality of the products they present for certification. The term "without special effort" is interpreted by ONC to have three attributes applicable to all health IT developers seeking certification:

- <u>Standardized</u>. The same technical API capabilities would be used.
- <u>Transparent</u>. Business and technical documentation necessary to interact with the APIs in production would be freely and publicly accessible.
- <u>Pro-competitive</u>. Business practices would promote efficient access, exchange, and use of electronic health information (EHI) to support a competitive marketplace that enhances consumer value and choice. ONC states that health IT developers must not interfere with a health care provider's use of their acquired API technology in any way, especially ways that would impact its equitable access and use based on (for example) another software developer's size, current client base, or business line. Developers together with health care providers that deploy APIs are accountable to patients who should be able to access their EHI via any API-enabled app they choose without special effort, including without

incurring additional costs and without encountering access requirements that impede their ability to access their information in a persistent manner.

Key terms would be defined in the proposed regulatory text at 45 CFR 170.102: "API Technology Supplier," "API Data Provider," and "API User." In addition, ONC uses the term "API technology" to generally refer to the capabilities of certified health IT that fulfill the proposed API certification criteria at §170.315(g)(7) through (11). The term "(g)(10)-certified API" refers to health IT certified to the proposed criterion at §170.315(g)(10), and the term "app" refers to any software designed to interact with (g)(10)-certified APIs.

New API standards at 45 CFR 170.215

ONC proposes to add a new 45 CFR 170.215 with the following standards and associated implementation specifications for APIs as summarized here.

(a)(1) *Adoption of FHIR Standard*. ONC proposes at §170.215(a)(1) to adopt the HL7® Fast Healthcare Interoperability Resources (FHIR®) standard as a foundational standard for its proposals. Specifically, FHIR Draft Standard for Trial Use (DSTU) 2 (hereafter referred to as "FHIR Release 2") is proposed as a baseline standard conformance requirement. While the 2015 Edition final rule did not include specific standards or implementation specifications, industry was encouraged to coalesce around a standardized specification for its API functionality, such as the FHIR standard. ONC reports that 32% of developers have published their use of FHIR Release 2; 51% appear to be using a version of FHIR and OAuth 2.0[29] together. It estimates that 87% of hospitals and 57% of clinicians are served by developers with a FHIR Release 2 API and 87% of hospitals and 69% of clinicians are served by developers with any version of an FHIR API.

Because it is used in the 2015 Edition systems that are being deployed, ONC believes this proposal would pose an incremental burden on IT developers to get certified, largely limited to the added security and registration conformance requirements that are proposed in this rule. Some developers would have to make more substantial changes, however.

Although a FHIR Release 3 is available, ONC says it is not in widespread use. However, **ONC believes that the improvements included in FHIR Release 4 mean that it will be the standard the industry would coalesce behind, and it seeks comments on several options for the final rule.**

- Option 1 is proposed in the regulatory text and would adopt just FHIR Release 2 for reference in proposed §170.315(g)(10). This would require health IT developers seeking certification to build, test, and certify systems solely to FHIR Release 2 and its associated

[29] The proposed rule does not describe OAuth 2.0. A Google search identifies it as the industry-standard protocol for authorization used by web applications, desktop applications, mobile phones, etc. https://tools.ietf.org/html/rfc6749

implementation specifications. Under this option, if the National Coordinator approved the use of FHIR Release 3 or 4 (pursuant to the Standards Version Advancement Process) it would occur, at the earliest, one year after a final rule was issued. Given that timing, and the compliance deadlines proposed, health IT developers would have no option but to develop to FHIR Release 2 in order to meet the proposed compliance deadlines.

- Under Option 2, ONC would adopt both FHIR Release 2 and FHIR Release 3 with IT developers given a choice for compliance with §170.315(g)(10). Given the timing of potential approval of Release 4 health IT developers would have no option but to develop to FHIR Release 2 or Release 3 in order to meet the proposed compliance deadlines.
- Option 3 would adopt FHIR Release 2 and FHIR Release 4 with health IT developers given a choice for compliance with §170.315(g)(10). ONC sees this as the best option for the industry, but implementation depends on all applicable corresponding FHIR Release 2 implementation specifications also being published in their FHIR Release 4 formats and available prior to the issuance of a final rule. Unlike Options 1 and 2, the Standards Version Advancement Process would not be necessary for this option. ONC also seeks comment on a variant of Option 3 that would include a pre-defined cut-over for the permitted use of and certification to FHIR Release 2. If this variant were implemented, ONC would likely also need to add a maintenance of certification requirement in the final rule to establish an upgrade timeline to FHIR Release 4 for those health IT developers who originally sought certification for FHIR Release 2.
- Option 4 would adopt only FHIR Release 4 in the final rule for reference in proposed §170.315(g)(10). Developers seeking certification would be required to build, test, and certify systems solely to FHIR Release 4 and its associated implementation specifications. Again, finalizing this option is dependent on all applicable FHIR Release 4 implementation specifications being published in time for a final rule. ONC believes that by the time a final rule associated with these proposals is issued, health IT developers would have close to or more than a year's worth of development experience with FHIR Release 4.[30] Many may be poised to introduce FHIR Release 4 products into production. If ONC were to offer certification to FHIR Release 2 (as in Option 3) this flexibility could unintentionally delay the industry's transition to FHIR Release 4.

ONC notes that if it adopts a FHIR Release in the final rule other than or in addition to Release 2, it would also adopt applicable implementation specifications and FHIR profiles in order to support US Core Data for Interoperability (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,) **Commenters are highly encouraged to explicitly note their preferred option.**

(2) *Implementation specifications. API Resource Collection in Health (ARCH) Version 1.* This proposal for new §170.215(a)(2) lists a set of base FHIR resources that Health IT Modules certified to the proposed §170.315(g)(10) would need to support. The ARCH would align with the proposed USCDI standard. The ARCH would require 15 FHIR resources, 13 of which ONC

[30] As an example, compliance timeline ONC states that if the final rule were effective January 2020, developers would have until January 2022 to rollout (g)(10)-certified API technology. At that point, FHIR Release 4 would have been available for nearly 3 years.

says it knows map to and support the equivalent data classes specified in the USCDI: AllergyIntolerance; CarePlan; Condition; Device; DiagnosticReport; Goal; Immunization; Medication; MedicationOrder; MedicationStatement; Observation; Patient; and Procedure. For the patient resource it proposes to include Patient.address and Patient.telecom elements. For the device resource, device.udi element would be included.

The proposed two resources in addition to these 13 are Provenance and DocumentReference. It believes the latter is best capable of handling the exchange of clinical notes and that stakeholders have frequently indicated are important data to exchange. ONC clarifies that the clinical note text would need to be represented in its raw text form and not converted from another file or format (e.g., a PDF). With respect to the Provenance resource ONC argues that it is best to include this requirement now as it would be more burdensome to add it in the future. The Provenance.recorded (author's time stamp) and Provenance.agent.actor (author and organization) elements would be required.

ONC expects to update this implementation standard over time as the USCDI is expanded. ONC also notes that under its proposed rule (the Standards Version Advancement Process proposals), developers could voluntarily update their certified health IT to include (g)(10)-certified API access to a broader set of data once a new version of the ARCH is approved.

(3) *Implementation specifications – FHIR profiles*. ONC proposes to adopt in §170.215(a)(3) the Argonaut Data Query Implementation Guide version 1.0.0 (Argonaut IG) hosted by HL7. It specifies FHIR profile constraints for 13 of the FHIR resources proposed for the ARCH Version 1.

(4) *Implementation specifications – FHIR server conformance*. Proposed §170.215(a)(4) would require adoption of The Argonaut Data Query Implementation Guide Server conformance requirements. While this is a specific portion of the Implementation Guide and covered by adoption of the guide, ONC elects to explicitly propose this requirement because it is essential that all FHIR servers are consistently configured to support the defined data queries and searches. ONC notes that the Server IG includes conformance requirements for the "DocumentReference Profile," a specification produced in support of the 2015 Edition certification criterion adopted in §170.315(g)(9). As a result, ONC clarifies that this specific portion of the Server IG and conformance requirement would be out of scope for the purposes of proposed §170.315(g)(10).

(5) *Implementation specification – Application authorization.* At proposed §170.215(a)(5) ONC would require support of the SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for "refresh tokens," "Standalone Launch," and "EHR Launch" requirements. ONC says this guide is referenced by the Argonaut IG and is generally being implemented in the health IT community as a security layer within FHIR deployment. Three components are specified for support. ONC believes "refresh tokens" is needed to enable persistent access by apps in a patient access context; a minimum refresh token life of 3 months would apply. Standalone launch and (from a smartphone or browser outside the EHR) and within-EHR launch would both need to be supported.

ONC notes that by separately proposing the FHIR standard and implementation specifications, it may evaluate industry progress and possibly update each separately in the future. It plans to coordinate with other agencies that may be adopting the FHIR standard and implementation guides.

(b) *Application authentication*. *Standard*. To support user authentication and app authorization processes, ONC proposes at §170.215(b) to adopt the OpenID Connect Core 1.0 incorporating errata set 1 standard, which it says complements the SMART Guide. The OpenID standard is usually paired with OAuth2.0 and focuses on user authentication.

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

ONC proposes new API certification criterion at §170.315(g)(10) to replace the existing criterion set forth at §170.315(g)(8). It says the current criteria need to be replaced because they focus on a Health IT Module's ability to provide API functionality that can respond to data categories specified in the Common Clinical Data Set. Current requirements at (g)(7) and (g)(9) would remain unchanged because they do not prescribe specific technical approaches that need to be replaced. By placing the new criteria separately (as opposed to modifying (g)(8)) it would be easier for industry to distinguish compliance requirements.

The proposed new API certification criterion would require FHIR servers to support API-enabled services for which a single patient's data is at focus and services for which multiple patients' data are at focus ("population-level"). API services that focus on a single patient would include those that interact with software applications controlled and used by a patient to access their data as well as software applications implemented by a provider to enhance their own "internal" clinical care tools and workflow. Most of these types of interactions are typically orchestrated in a synchronous, real to near-real-time mode via APIs. By contrast, population-level API services would include software applications used by a health care provider to manage various internal patient populations as well as external services to support a provider's quality improvement, population health management, and cost accountability vis-à-vis health plans and other partners.

Population-level uses may range from a small group to many hundreds or thousands of patients. ONC expects that such access and associated privacy and security protocols would be established consistent with existing legal requirements under the HIPAA Privacy and Security Rules and other applicable state or federal laws. For the purposes of the proposed certification criterion, ONC seeks to ensure through testing and certification that a set of baseline API functionalities exists and is deployed for providers to use at their discretion to support their own clinical priorities and to engage with their partners. ONC notes that FHIR Release 4 includes technical specifications to support standardized population-level services in a more efficient manner than is currently possible and if Options 3 or 4 for the FHIR standard described above are selected or Release 4 is approved under the Standards Version Advancement process, it could be used to meet these technical expectations. Finally, ONC says inclusion of a population-level API conformance requirement in the criterion would allow these capabilities to be evaluated post-certification for compliance with this criterion and the information blocking and real-world testing conditions of certification.

Under the Standardized API for patient and population services Condition of Certification criterion proposed at §170.315(g)(10) API technology would need to meet the following technical requirements for certification. All data elements indicated as mandatory would be in scope for testing.

(i) *Data response*. The technology would have to be capable to respond to requests for data (based on an ID or other token) for each of the FHIR resources in ARCH Version 1 and consistent with FHIR Release 2 and the Argonaut IG implementation specification.

(ii) *Search support*. The technology would have to be capable of responding to all supported searches identified in the Argonaut Data Query Implementation Guide Server (proposed at §170.215(a)(4)). For population-level searches a developer would be permitted to choose the most efficient manner because there is not a standardized specification for FHIR services to handle searches for multiple patients. **ONC seeks comment on the minimum search parameters that would need to be supported for the DocumentReference and Provenance resources, which are currently included in the base FHIR standard.**

(iii) *App registration*. The technology would be required to be capable of enabling apps to register with the technology's "authorization server." The API Technology Supplier would have to demonstrate its registration process, but ONC would not require that it be done according to a specific standard. **ONC seeks public comment on whether it should require the OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591) standard ("Dynamic Registration") as the only way to support registration for this certification criterion.** ONC considered proposing Dynamic Registration as a requirement but did not do so because it has not been widely adopted. It believes it is more prudent to require the function and let the industry reach consensus on the best techniques to enable registration. ONC notes that a specific maintenance requirement associated with the API Condition of Certification around the timeliness of this registration process is proposed to ensure that patients can use their apps in a timely manner. (See discussion of §170.404(b) below.) **ONC requests comment on its plan to not test registration capabilities for apps that would be executed within an API Data Provider's clinical environment** because it believes that API Technology Suppliers and API DataProviders are best poised to innovate and execute various methods for app registration within a clinical environment.

(iv) *Secure connection*. The technology would be required to demonstrate capability to establish a secure and trusted connection with an application that requests data in accordance with the SMART Guide. This would require that an authorization server be used and that it support at least "authorize" and "token" endpoints and the publication of the endpoint URLs via FHIR server's metadata as specified in the SMART Guide. Initial conformance would focus on secure connection parameters for a single patient's data and the developer could approach secure connections for multiple patients as it deems most efficient to meet the proposed certification criterion.

(v) *Authentication and app authorization – 1st time connection*. The first time an application connects to request data the technology would have to demonstrate that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the OpenIDConnect Core 1.0 incorporating errata set 1 standard. ONC notes that this standard is agnostic to the authentication mechanism itself. Further, the technology would be required to demonstrate that a user can authorize applications to access data in accordance with the SMART Guide and issue a refresh token that is valid for a period of at least 3 months. ONC intends to test health IT in both the Standalone Launch and EHR Launch modes. ONC clarifies that the provision does not require support for OpenID Connect Standard capabilities that are not specified in the SMART Guide. Further, it notes that the proposed refresh token requirement differs from providing an access token with extended life which is discouraged from a security standpoint.

(vi) *Authentication and app authorization – Subsequent connections*. The technology would be required to demonstrate that an application can access data without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new periods no shorter than 3 months. ONC says this renewal requirement responds to stakeholder concerns that a constant need for patients to re-authenticate and re-authorize their apps creates usability challenges and may otherwise contradict the Cures Act's intent associated with the phrase "without special effort." **It seeks comment on whether there are available specifications it should review as well as whether there should be a reasonable upper bound from a timing perspective (e.g., one year) after which the user should be required to re-authenticate and re-authorize.** ONC notes that it expects FHIR Release 4 to specify handling of population-level data requests; under this proposal a developer could use any approach to these requests it deems most efficient.

(vii) *Documentation*. An API Technology Supplier would be required to include complete 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.

All documentation would have to 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.

ONC notes that the 2015 Edition final rule included transparent documentation requirements for the API certification criteria adopted at §170.315(g)(7) through (g)(9) and proposes to modify these provisions as well as §170.315(g)(10) and (11). Specifically, it proposes to focus the documentation requirement on solely the technical documentation associated with the API technology and therefore would remove provisions associated with "terms of use" which are not technical and are more reflective of business practice. In addition, the proposed technical documentation would be broadened to require the API Technology Supplier to provide detailed information for all aspects of its (g)(10)-certified API, especially for any unique technical requirements and configurations such as optional elements of the Argonaut IG Patient Profile, for example. For aspects fully specified by the FHIR standard, hyperlinks could be provided as part of its overall documentation.

API Condition of Certification Requirements (§170.404)

ONC says that to implement the Cures Act it is proposing API Condition of Certification to complement the technical capabilities described above while addressing the broader technology and business context within which the API will be used. The following sections describe the requirements as proposed in §170.404. They are proposed to apply to developers of Health IT Modules certified to *any* of the criteria under current and proposed §170.315(g)(7) through (11). ONC notes that the proposed policies would 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 proposed rule, such as information blocking, could still apply to the non-API-focused certification criteria.

(a) *Condition of Certification*. (1) *General.* An API Technology Supplier would be requiredto publish APIs and to allow health information from APIs to be accessed, exchanged, and used without special effort using APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws. By the term "all data elements" ONC means the scope of the ARCH and its associated implementation specifications and the policy expressed around the data elements that must be supported by (g)(10)-certified APIs. ONC expects that these APIs will be able to support access to more data over time as the USCDI and the ARCH are updated.

(2) *Transparency conditions*. ONC proposes that the business and technical documentation published by an API Technology Supplier 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 would have to include all terms and conditions for the API technology, including any restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

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

Any and all fees charged by an API Technology Supplier 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 proposes a compliance date of six months from the final rule's effective date for developers with products already certified to §170.315(g)(7),(8) or (9) to meet the specific transparency conditions. In addition, it recognizes that API Technology Suppliers will need to update the publicly available information from time to time. 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.

Under the proposed rule, an API Technology Supplier would be permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology. ONC notes that this proposal is needed because it did not propose to adopt the Dynamic Registration standard in (g)(10). **ONC seeks comments on factors that would enable registration with minimal barriers,** such as allowing suppliers to do one-time verification of app developers. However, it is concerned about the potential for a malicious app developer to spoof the app of another and other trade-offs. Under the proposal suppliers would have the discretion to develop a verification process as long as it is objectiveand the same for all developers and reasonably completed within the five business days. **Comments are requested on other timing considerations.**

The use of an application developer verification process would be optional, and ONC reminds stakeholders that even when an API Technology Supplier chooses not to use such a process, apps would not have carte blanche access to a health care provider's data. They would still be registered and could be de-activated by an API Technology Supplier or health care provider if they behave in anomalous or malicious ways. A patient seeking access to their data using the app will have to authenticate themselves, authorize the app to connect to the FHIR server and specify the scope of data which the app may access.

ONC notes that, separate from this provision, API Technology Suppliers may establish additional mechanisms to vet app developers. Such mechanisms could fit into the "value-added services" permitted fee and result in the app being acknowledged or listed by the health IT developer in some special manner (e.g., in an "app store," "verified app" list). No explicit limits to the nature of these approaches are specified but ONC cautions that in addition to offering an extra layer of trust they can be used to prevent, limit, or otherwise frustrate innovation, competition, and access to the market. This use could directly violate the specific Condition of Certification associated with fees permitted for value-added services and could constitute information blocking.

(3) *Permitted fees conditions*. In general, an API Technology Supplier would be prohibited from imposing any fees, but certain permitted fees would be allowed, and these are described below. The prohibition is meant to ensure that Suppliers do not engage in pricing practices that create barriers to entry and competition for apps that health care providers seek to use. The permitted fees are intended to recognize that suppliers need to recover costs and earn a reasonable return for providing certified API technology. ONC emphasizes that fees would not be allowed in any way in connection with a supplier's work to support use of API technology to facilitate a patient's ability to access, exchange or use their EHI. Other than those for value-added services, fees would always be between an API Technology Supplier and an API Data Provider.However, ONC notes that the conditions do not address who may pay the fee, although this may be affected by other federal or state laws and regulations addressing relationships involving remuneration. ONC notes that the proposed "permitted fees conditions" described below align with the requirements of the information blocking exceptions proposed in 45 CFR 171.204 and 171.206. (The Information Blocking provisions are summarized in section VII of this summary.)

For any permitted fee imposed by an API Technology Supplier on an API Data Provider, several general assurances would be required. First, a Supplier would be required to ensure that the fee was based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. Second, the fees imposed would need to be reasonably related to the Supplier's costs of supplying and supporting API technology to the user being charged. For example, a fee would not be permitted if the underlying costs had already been recovered. ONC states further that a supplier that conditioned access to API technology on revenue sharing or entry into a royalty agreement would be at risk of violating this condition. 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 supplier's customers using the technology. For example, the supplier could not recover the total of its core costs from each customer. However, costs unique to a customer would not have to be distributed among customers. Finally, fees could not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the supplier. **ONC requests comments on these conditions for permitted fees and whether it has provided sufficient guardrails to ensure that fees do not prevent EHI from being accessed, exchanged and used through APIs without special effort.**

ONC reminds readers that the scope of API technology subject to the proposals includes only certified health IT that fulfill the current or proposed certification criteria at §170.315(g)(7) through (11). Other API functionality provided by a supplier would not be subject to the Condition of Certification proposed at §170.404.

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

<u>Permitted fee – Development, deployment, and upgrades</u>. An API Technology Supplier would be permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider. Fees for developing API technology could not include the supplier's costs of updating

non-API related capabilities, including its databases, as part of its development of the API technology because ONC says 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 Data Provider 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 Data Provider—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 Data Provider. Costs would depend on the scope of work undertaken by the supplier. ONC proposes that any fees under this category of permitted fees could be charged only to the data provider(s) for whom the capabilities are deployed. It expects the fees would be negotiated between these parties. ONC believes it would be inappropriate to pass the costs on to API Users.[31]

<u>Permitted fee – Supporting API uses for purposes other than patient access.</u> An API Technology Supplier would be permitted to charge usage-based fees to an API Data Provider to recover the incremental costs reasonably incurred by the supplier to support the use of API technology deployed by or on behalf of the provider. This permitted fee could not include:

- Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient’s ability to access, exchange, or use their electronic health information;
- Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or
- Opportunity costs, except for the reasonable forward-looking cost of capital.

ONC expects 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

[31] Under the definitions proposed at 170.102, an API User creates software applications that interact with the APIs developed by the API Technology Supplier, and an API Data Provider is the organization that deploys the API technology (e.g., a health care provider).

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.

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 ofthe information contained in a patient's electronic record because it was documented in the course of providing health care services to patients, and it would be inappropriate to charge patients additional costs to access this information, whether charged directly or passed on as a result of fees charged to persons that provide apps, technologies, and services on a patient's behalf. ONC notes that any unreasonable fees associated with a patient's access to their EHI may be suspect under the information blocking provision and inconsistent with an individual's right of access to their PHI under the HIPAA Privacy Rule.

ONC also proposes to explicitly exclude two additional costs from this permitted fee. The fee could not include costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets. Nor could the fee include opportunity costs, which ONC considers speculative except for the reasonable forward-looking cost of capital.

Permitted fee – Value-added services. An API Technology Supplier would be permitted to 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 such software. 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 API technology. ONC emphasizes that fees would not be permitted if they interfere with an API User's ability to develop and deploy production-ready software. A fee would only be permitted if it relates to a service that a software developer can elect to purchase. ONC believes this type of fee is appropriate because API Technology Suppliers may offer a wide-range of market differentiating services to API Users such as advanced training, premium development tools and distribution channels, and enhanced compatibility/integration testing assessments. However, suppliers are cautioned that API value-added services would have to be made available in a manner that complies with other requirements of this Condition of Certification and with the information blocking provision. Examples of permitted and not-permitted activities under this fee are offered in the proposed rule.

Prohibited Fees. ONC says it continues to receive evidence that some health IT developers are engaging in practices that create special effort when it comes to API technology. These practices include fees that create barriers to entry or competition as well as rent-seeking and other opportunistic behaviors. For this reason, the proposed rule identifies the following examples of prohibited fees.

- Any fee for access to the documentation that an API Technology Supplier 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.

Permitted Fees Request for Comment. **ONC requests comment on any additional specific "permitted fees" that API Technology Suppliers should be able to recover in order to assure a reasonable return on investment.** Furthermore, the agency requests comment on whether it would be prudent to adopt specific, or more granular, cost methodologies for the calculation of the permitted fees. Commenters are encouraged to consider, in particular, whether the approach ONC has described will be administrable and appropriately balance the need to ensure that patients, providers, app developers, and other stakeholders do not encounter unnecessary costs and other special effort with the need to provide adequate assurance to API Technology Suppliers, investors, and innovators that they will be able to earn a reasonable return on their investments in API technology. ONC welcomes comments on whether the approach adequately balances these concerns or would achieve its stated policy goals, and it welcomes comments on potential revisions or alternative approaches. Detailed comments are encouraged to include, where possible, economic justifications for suggested revisions or alternative approaches.

Permitted Fees Record-keeping Requirements. An API Technology Supplier 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. Separately, an API Technology Supplier would need to document the criteria it used to allocate any costs across relevant customers, requestors, or other persons. The criteria must be documented in a level of detail that would enable determination as to whether the supplier's cost allocations are objectively reasonable and comply with the cost accountability requirements.
ONC notes that the supplier would have to meet the records retention requirement proposed elsewhere in the proposed rule as part of the Assurances Condition of Certification (proposed for adoption in §170.402). **ONC requests comment on whether these requirements provide adequate traceability and accountability for costs permitted under this API Condition of Certification**. Comments are also requested on whether to require more detailed accounting records or to prescribe specific accounting standards.

(4) *Openness and pro-competitive conditions*. *General condition.* An API Technology Supplier would be required to grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the provider. More specific provisions are also proposed as summarized below, and ONC says these proposed conditions are intended to provide clear rules and expectations for API Technology Suppliers. ONC notes that the API technology required by this Condition of Certification is subject to strict protections under the

information blocking provision. To the extent that API Technology Suppliers claim an intellectual property right or other proprietary interest in the API technology, ONC admonishes that they must take care not to impose any fees, require any license terms, or engage in any other practices that could add unnecessary cost or other burden that could impede the effective use of the API technology for facilitating access, exchange, or use of EHI. Moreover, ONC believes that, as developers of technology certified under the Program, API Technology Suppliers owe a special responsibility to patients, providers, and other stakeholders to make API technology available in a manner that is truly open and minimizes any costs or other burdens that could result in special effort.

- Non-discrimination. An API Technology Suppler would be required provide API technology to API Data Providers 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 would have to 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 or service could not be offered on the basis of whether the API User with whom a provider has a relationship is or could be a competitor; or whether the revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.
- Rights to access and use API technology. An API Technology Supplier would be required to have and grant upon request to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment. The proposal would not extend to intellectual property of the supplier that has no nexus with the access and use of API technology. Suppliers would need to grant rights that could include the following to support use of the API technology:
    - For the purposes of developing products or services designed to be interoperable with the supplier's health information technology or with health information technology under the supplier's control;
    - Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and
    - Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

  None of the rights described above could be conditioned on a requirement that the recipient of the rights do, or agree to do, any of the following:
    - Pay a license fee, royalty, or revenue-sharing arrangement for such rights.
    - Not compete with the API Technology Supplier in any product, service, or market.
    - Deal exclusively with the API Technology Supplier in any product, service, or market.
    - Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.

    - License, grant, assign, or transfer any intellectual property to the API Technology Supplier.
    - Meet additional developer or product certification requirements.
    - Provide the API Technology Supplier or its technology with reciprocal access to application data.

  ONC notes that these prohibitions mirror those proposed under exceptions to the information blocking definition but offers an important distinction in that under the API Condition of Certification would not permit any royalty, license fee or other type of fee whereas the information blocking definition would permit a developer to charge a reasonable royalty to license interoperability elements. The different treatment is due to the statutory requirement that APIs facilitate access exchange and use of patient information from EHRs "without special effort."

- Service and support obligations. An API Technology Supplier would be required to provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments. The following obligations are specified:
    - Changes and updates to API technology: A supplier would have to make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of 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 would have to provide notice and a reasonable opportunity for its data provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

  ONC clarifies that this requirement would not prevent a supplier from making improvement to its technology, but the supplier would need to demonstrate that its actions were necessary and that it afforded the licensee a reasonable opportunity to update its technology to maintain interoperability. ONC recognizes that an API Technology Supplier may have to suspend access or make other changes immediately and without prior notice in response to legitimate privacy, security, or patient safety-related exigencies, and these actions would be permitted provided they do not unnecessarily interfere with the use of API technology. The overlap between these provisions and information blocking requirements are discussed in the proposed rule.

(b) *Maintenance of Certification*. (1) *Registration for production use.* An API Technology Supplier with (g)(10)-certified health IT would have to register and enable all applications for production use within 1 business day of completing its verification of an application developer's authenticity (as described in the application developer verification provision above). ONC believes this proposed requirement is needed to ensure that a patient's ability to use an app of their choice is not slowed by a supplier, causing special effort by the patient to access their EHI. A supplier that chooses not to engage in developer verification would need to meet this one business day requirement from the point of having received a request for registration.

(2) *Service Base URL publication*. An API Technology Supplier would have to support the publication of Service Base URLs for all its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider and make such information publicly available (in a computable format) at no charge. In order to interact with a FHIR RESTful[32] API, an app needs to know the FHIR Service Base URL, also called the FHIR server's endpoint. To enhance the ease with which Service Base URLs could be obtained and used, ONC strongly encourages suppliers, providers, health information networks and patient advocacy organizations to coalesce around the development of a public resource or service from which all stakeholders could benefit.

(3) *Rollout of (g)(10)-Certified APIs.* An API Technology Supplier with API technology previously certified to the certification criterion in §170.315(g)(8) would be required to provide all API Data Providers with such API technology deployed with API technology certified to the (g)(10) criterion within 24 months of the final rule's effective date.

In addition, ONC proposes to add compliance timeline language to the 2015 Edition Base EHR definition in §170.102 to provide for a transition from §170.315(g)(8) to §170.315(g)(10) that would reflect a total of 24 months from the final rule's effective date. ONC believes this approach is best because it identifies a single, specific date for both API Technology Suppliers and API Data Providers by which upgraded API technology would need to be deployed in production. It believes that 24 months is enough because its proposals reflect a large portion of capabilities API Technology Suppliers have already developed and deployed to meet §170.315(g)(8). Moreover, this single date enables API Technology Suppliers (based on their client base and IT architecture) to determine the most appropriate timeline for development, testing, certification, and product release cycles in comparison to having to meet an arbitrary "must be certified by this date" requirement.

5. Real World Testing (§170.405)

The Cures Act requires health IT developers to successfully test the real world use of the technology for interoperability in the type of setting in which that technology would be marketed; this requirement is imposed as a Condition and Maintenance of Certification. As a related matter, ONC proposes to codify the Cures Act definition of interoperability.[33]

Condition of Certification

For purposes of the Condition of Certification, ONC proposes that successful real world testing means the following:

[32] "RESTful" interfaces" are those that are consistent with Representational State Transfer (REST) architectural style and communications approaches to web services development.

[33] 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.

- The certified health IT continues to be compliant to the certification criteria to which it is certified, including the required technical standards and vocabulary codes sets;
- The certified health IT is exchanging EHI in the care and practice settings for which it is intended for use; and
- EHI is received by and used in the certified health IT.

ONC proposes to limit the applicability of this Condition of Certification to developers with health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange; they are as follows:

- Care coordination criteria (§170.315(b)).
- Clinical quality measures (CQMs) criteria (§170.315(c)(1) through (c)(3)).
- View, download, and transmit to 3rd party criterion (§170.315(e)(1)).
- Public health criteria (§170.315(f)).
- Application programming interface (API) criteria (§170.315(g)(7) through (g)(11)).
- Transport methods and other protocols criteria (§170.315(h)).

ONC seeks comment on whether to also include other certification criteria, such as the "patient health information capture" certification criteria (§170.315(e)(3)).

Maintenance of Certification

ONC proposes to require developers to submit publicly available annual prospective real world testing plans as well as annual retrospective real world testing results for certified health IT products that include certification criteria focused on interoperability. Annual prospective testing plans must be submitted to ONC-ACBs through a publicly accessible hyperlink by December 15 of each year for each health IT product certified to the 2015 Edition through August 31 of the preceding year. A testing plan would have to 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.
- At least one measurement or metric associated with the real world testing.
- A justification for the developer's real world testing approach.

ONC does not believe that testing through ONC-approved test procedures would suffice for real world testing. ONC also clarifies that developers may design their testing plans to test a combination of their products where appropriate as long as there is "traceability" to each of the specific Modules. **ONC seeks comment on whether there should be an exemption for services that support all of a developer's customers through a single interface or engine and whether this would be sufficient to meet the intent of the real world testing requirement**.

Developers would have to submit testing results to ONC-ACBs through a publicly accessible hyperlink no later than January 31 of each year. The testing results would have to report on the following:

- 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.

On implementation, ONC acknowledges that if it finalizes a rule later this year, developers may not have time to develop and submit plans for a full year of real world testing in 2020 in which case it would treat 2020 as a pilot year.

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.

Standards Version Advancement Process

Noting that promulgating standards through ONC rulemaking has slowed the pace of standards development and deployment in the market and that stakeholders have been technologically restricted "and innovation-stunted," ONC proposes a more nimble or flexible process to make newer versions of standards available to developers, which it calls the Standards Version Advancement Process (SVAP). Noting that use of the SVAP would be voluntary, developers with health IT certified to the criteria specified for interoperability and data exchange could 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 would require ONC-ACBs to offer certification to newer versions of all standards approved by the National Coordinator to which real world testing requirements apply.

Developers using the SVAP would have to 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 would have to 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 would also include use of an SVAP standard or specification. ONC also notes that all Conditions of Certification and Maintenance of Certification requirements would apply, meaning, for example, that real world testing plans and results would have to include the newer standards versions under the SVAP and that developers would have to maintain their Health IT Modules consistent with the requirements of those newer SVAP standards. If a nonconformity with a newer standard is discovered, it would have to be addressed in the same manner as a nonconformity with a standard specified in regulation; in other words, surveillance and enforcement under the Program would apply to Health IT Modules certified or updated under the SVAP.

Developers updating their Health IT Modules under the SVAP would have to provide notice of its anticipated impact which would include 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 would have to 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 seeks comment on what stakeholders would consider to be a reasonable minimum timeframe before implementation of an updated standard or specification version to allow for time to plan for potential implications of the update for operations and exchange relationships**. ONC proposes to require ONC-ACBs to 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 proposes to implement this new flexibility by making adjustments to the way ONC-ACBs process certifications pursuant to §170.550.

Advanced Version Approval Approach

When a standard or implementation specification is adopted under the Program through rulemaking, ONC would then annually identify updated versions of those standards and specifications for use under the SVAP. ONC expects to use an expanded section of the Interoperability Standards Advisory web platform to facilitate the public transparency and engagement process. ONC anticipates providing for a comment period of between 30 and 60 days and would approve (or not) newer versions based on Program and market factors, such as ability to enhance interoperability, compatibility with other adopted versions, burden of updating, scope and scale of the changes, availability of test tools, and whether the new version would be required for reporting by a corresponding program (e.g., CMS or CDC). ONC views this list as providing a single, comprehensive, and authoritative index of versions of adopted standards and implementation specifications under the Program. **ONC welcomes comment on these proposals**.

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 ONC-ACBs to review and confirm that applicable developers submit real world testing plans and real world testing results. ONC-ACBs would have to submit testing plans to ONC by December 15 and testing results by April 1. 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. **ONC seeks comment on whether to require ONC-ACBs to evaluate testing plans and results as opposed to simply checking them for completeness**.

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 proposed new §170.406, ONC would require developers to attest to compliance with those Conditions and Maintenance of Certification requirements every 6 months. ONC proposes a 14-day attestation period that would most likely occur in the middle and at the end of each year. Developers presenting health IT for certification for the first time would 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. The first attestation will depend on when the final rule is published.

ONC also proposes to 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 would have the flexibility to specify non-compliance per certified Health IT Module, if necessary.

Developers would have to submit their attestations to ONC-ACBs. ONC-ACBs would review and submit the attestations to ONC. ONC would then make the attestations publicly available through the CHPL. Before issuing certifications, ONC-ACBs would need to 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 would be able to 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.

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 would 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 proposes 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. Table 2 in the proposed rule provides an overview of the proposed approach. Essentially, for proposed certification criteria at §§170.401 through 170.406, developers would be able to undertake a corrective action plan to correct a nonconformity with a condition of certification; failure to do so could 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 proposes 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 first priority would be to work with the developer to remedy the matter through a corrective action process. By direct review, ONC says that it would be the sole party responsible for enforcing compliance; ONC-ACBs would not be involved in enforcement though their surveillance activities would continue and could supplement ONC enforcement efforts. In essence, the proposed rule expands the reasons for which ONC may conduct direct review to include these non-conformities.

ONC would be able to initiate direct review if it has a reasonable belief that a developer has not complied with a Condition of Certification. ONC would issue a notice to the developer of a potential or actual non-conformity; the developer could 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 proposes to give 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 (which would include issue logs and help desk tickets). This requirement would also extend 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 would be able to issue a certificate ban or termination for a certified Health IT Module if it determined that a developer was not cooperating with the fact-finding process, was not working with ONC to develop a corrective action plan or was not carrying out the plan. The ban would apply to the developer, its subsidiaries and successors and would prohibit prospective certification activity by the developer. If ONC determined there was a nexus between the developer's actions or business practices and the certified Health IT Module, it could terminate the certificate. ONC would 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 would include information for the developer on appeals as well as instructions for requesting reinstatement using current procedures.

ONC does not propose to include in its enforcement proposal 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 would prefer to be able to move directly to termination if the developer does not take appropriate and timely corrective action.

Public Availability. ONC proposes to publicly list on its website developers and certified Health IT Modules that are subject to a certification ban or that have been terminated. **It seeks comment on this proposal, including the appropriate amount of time to list the affected developers and Modules**. ONC proposes to require ONC-ACBs to 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 proposes that all general Conditions and Maintenance of Certification requirements apply to such developers. However, **it seeks comment on which aspects of the Conditions and Maintenance of Certification requirements may not be applicable to self-developers**. For example, when considering the Communications Condition of Certification, a self-developer of health IT may not have customer contracts, but could have other agreements in place, such as nondisclosure agreements, that would be subject to the Condition of Certification.

VII. Information Blocking

Section 4004 of the Cures Act added section 3022 of the PHS Act to define and prohibit information blocking by health care providers, IT developers of certified health IT, health information exchanges, and heath information networks. 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 several activities that do not constitute information blocking, and it refers to these activities as exceptions. The exceptions would apply to certain activities that do in fact interfere with the access, exchange, or use of EHI but that may be reasonable and necessary if certain conditions are met. In the preamble, 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 proposes seven exceptions which are described in detail below. In developing the exceptions, ONC says it was guided by three overarching policy considerations.

1. The exceptions would be limited to certain activities that clearly advance the aims of the information blocking rule; promote public confidence in health IT infrastructure by supporting the privacy and security of EHI and protecting patient safety; and promote competition and innovation in health IT and its use to provide health care services to consumers.
2. Each exception is intended to address a significant risk that health care providers, health IT developers of certified health IT, health information networks, and health information exchanges will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking.
3. Each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt.

To qualify for any of these exceptions, an individual or entity would, for each relevant activity and at all relevant times, have to satisfy all of the applicable conditions of the exception. The burden of proof would be on the individual or entity to demonstrate compliance with all the conditions.

Section 3022 of the PHS Act imposes penalties for individuals or entities that commit information blocking. In the case of health IT developers of certified health IT, health information networks, and health information exchanges, violations are subject to a civil monetary penalty determined by the Secretary for all such violations, which may not exceed $1,000,000 per violation. The amount of the penalty takes into account factors such as the nature and extent of the information blocking and harm resulting from such information blocking, including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted. For health care providers who commit information blocking, the statute requires the provider to be referred to the appropriate agency that will determine "appropriate disincentives using authorities under applicable Federal law," as the Secretary establishes through notice and comment rulemaking. On this issue, **ONC requests information on appropriate disincentives under federal law, including modification to current penalties or disincentives, as well as on avoiding duplicate penalty structures for information blocking.**

The preamble to the proposed rule describes the legislative background and purpose of the information blocking rule. ONC proposes to add a new Part 171 to title 45 of the Code of Federal Regulations to implement the information blocking rules of section 3022. **ONC seeks comment on all aspects of its proposals to implement the information blocking rule**.

A. Definitions

1. Information Blocking (§171.103)

ONC proposes to codify with only technical changes the definition of information blocking contained in section 3022(a)(1) of the PHS Act. The proposed regulation text is as follows:

> *Information blocking*. Information blocking means a practice that—
> (a) Except as required by law or covered by an exception set forth in subpart B of this part, is likely to interfere with, prevent, or materially discourage access, exchange, oruse of electronic health information; and
> (b) If conducted by a health information technology developer, health information exchange, or health information network, such developer, exchange, or networkknows, 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
> (c) 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.

ONC proposes to define or clarify a number of terms or concepts contained in information blocking definition.

(1) *Required by law*. ONC proposes to clarify 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.

(2) *Likelihood of interference.* Noting that the information blocking rule is preventive in nature, the proposed 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, it may violate the information blocking rule even if harm does not actually materialize.

ONC describes a number of different practices that always will, almost always will, or are likely to implicate the information blocking rule.

- Observational health information. ONC believes that a practice to interfere with access, exchange, or use of EHI in the context of observational health information will always implicate the information blocking rule. Observational health information refers to information created or maintained during the practice of medicine or the delivery of patient care, such as patient information in an electronic health record (EHR) or other clinical information management systems when it is clinically relevant, directly supports patient care, or facilitates delivery of health care to consumers. By contrast, EHI created through aggregation or algorithms that transform observational health information to fundamentally new data (such as population trends, risk scores, etc.) are not observational health information.

- Purposes for which information may be needed. ONC believes that a practice that interferes with access, exchange, or use of EHI in any of the following circumstances 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 would almost always implicate the information blocking rule.

- Control over essential interoperability elements. ONC proposes 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 elements—or that could unnecessarily increase the cost or other burden of using the elements—would 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.

- Practices likely to interfere. ONC believes the following practices 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 would occur 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.

2. Other definitions (§171.102)

ONC proposes to establish definitions for a number of additional terms, some of which are described below:

(1) *Actor*. ONC proposes to define the term actor to refer 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.

(2) *Health care provider*. ONC proposes to use the very broad definition of health care provider established under the HITECH ACT under section 3000(3) of the PHS Act which includes all individuals and entities covered by the HIPAA definition.[34] 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.

(3) *Health Information Exchange* or *HIE*. ONC proposes to define the term to mean an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. ONC notes this would include regional health information organizations, state health information exchanges, and other types of organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used among particular types of parties or for particular purposes.

(4) *Health Information Network* or *HIN*. ONC would define the term to mean an individual or entity that satisfies one or both of the following:

- Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.
- Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.

ONC notes that a health care provider or other entity that enables, facilitates, or controls movement of EHI within its own organization, or among its affiliated entities, would not be considered a health information network vis-à-vis that movement of information.

(5) *Health IT developer of certified health IT.* ONC would define the term to mean an individual or entity that develops or offers health IT certified under the ONC Health IT Certification Program (Program) at the time the actor engaged in a practice that is the subject of an information blocking claim. ONC highlights that the definition would apply to individuals or entities that develop *or offer* certified health IT. ONC also notes that the information blocking rule is not limited to practices related only to certified health IT; it would apply to any practice by an individual or entity that develops or offers certified health IT that is likely to interfere with

[34] 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.

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. It would also apply to 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 is considering additional approaches to ensure developers and offerors are subject to the information blocking rule for an appropriate period of time after leaving the Program. Self-developers of certified health IT (as understood under the Program) would be treated as a health care provider.

(6) *Electronic Health Information (EHI)*. ONC proposes to define this term to mean—

- Electronic protected health information (ePHI); and
- Any other information that—
  - is transmitted by or maintained in electronic media;
  - identifies an individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
  - relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

ONC notes the definition is intended to include an expansive set of EHI, and would encompass 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.

(7) *Interoperability element.* ONC's intent is to define this term very broadly so it captures all potential means by which EHI may be accessed, exchanged or used for any relevant purpose, both now and as conditions evolve. The agency clarifies that the means of accessing, exchanging, and using EHI are not limited to functional elements and technical information but also encompass technologies, services, policies, and other conditions necessary to support the many potential uses of EHI. ONC would define the term as follows:

- Any functional element of a health IT, whether hardware or software, that could be used to access, exchange, or use EHI for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.
- Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements.
- Any technology or service that may be required to enable the use of a compatible technology in production environments, including any system resource, technical infrastructure, or health information exchange or health information network element.
- Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.
- Any other means by which EHI may be accessed, exchanged, or used.

3. Price information not defined

ONC does not propose a definition of the term price information but, noting that it "has a unique role" in possibly establishing a framework to prevent the blocking of price information, **it seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care**.

B. Exceptions for Reasonable and Necessary Activities That Do Not ConstituteInformation Blocking

Consistent with section 3022, ONC proposes 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. The first three exceptions address activities to promote public confidence in the use of health IT and the exchange of EHI. These exceptions are intended to protect patient safety, promote the privacy of EHI, and promote the security of EHI.

The next three exceptions address activities to promote competition and consumer welfare. These exceptions would allow for the recovery of costs reasonably incurred, excuse an actor from responding to requests that are infeasible, and permit the licensing of interoperability elements on reasonable and non-discriminatory terms.

The last exception addresses activities that promote the performance of health IT; it recognizes that actors may make health IT temporarily unavailable for maintenance or improvements that benefit the overall performance and usability of health IT.

Pursuant to proposed §171.200, 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 would have the burden of proof to demonstrate that compliance.

1. Exception — Preventing harm (§171.201)

ONC proposes an exception for reasonable and necessary practices to prevent harm to a patient or another person, subject to certain conditions which must be met at all relevant times. The conditions are as follows:

(1) *Types of Risks of Patient Harm.* The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from—

- Corrupt or inaccurate data being recorded or incorporated in a patient's EHR;
- Misidentification of a patient or patient's EHI; or
- Disclosure of a patient's EHI in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, providedthat,

if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

ONC notes that the term patient does not necessarily require a clinician-patient relationship with the individual at risk of harm; health IT developers could benefit from this exception for individuals receiving care from a provider using the developer's health IT. The scope of the exception is limited to the risks specifically enumerated above. With respect to data corruption and inaccuracies, ONC clarifies that the recognized risk is limited to corruption and inaccuracies caused by performance and technical issues affecting health IT. For misidentification, ONC notes that the exception may apply to practices designed to promote data quality and integrity and support health IT applications properly identifying and matching patient records or EHI, which the agency notes is a complex task. Thus, where clinicians know a specific EHI in a patient's record is misattributed, it is reasonable for them not to share or incorporate that EHI. With respect to endangering life or physical safety, ONC envisions restrictions on disclosure of an individual's EHI where a health care professional determines that disclosure is reasonably likely to pose a danger to the life or physical safety of the patient or another person.

To qualify for the exception, the actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person. ONC proposes two methods to meet this condition: through a qualifying organizational policy or through a qualified individual finding.

(2) *Requirements for qualified organizational policies.* If the practice implements an organizational policy, it must be—

- In writing;
- Based on relevant clinical, technical, and other appropriate expertise;
- Implemented in a consistent and non-discriminatory manner; and
- No broader than necessary to mitigate the risk of harm.

For the practice to meet the third condition above (i.e., consistent and non-discriminatory implementation), ONC believes the actor should take reasonable steps to educate its directors, officers, employees, contractors, and authorized personnel on how to apply the policy and to provide appropriate oversight to ensure that the policy is not applied in an arbitrary, discriminatory, or otherwise inappropriate manner. For the fourth condition (i.e., narrowing the scope of the practice), ONC believes the policy should identify the relevant risks and mitigate those risks based on current patient safety evidence and best practices, supplemented by input from clinical, technical, and other staff.

(3) *Requirements for qualified individual finding*s. 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. ONC proposes that health care professional's independent and individualized judgment about the safety of the actor's patients or other persons would be entitled to substantial deference, taking into account all relevant facts under the particular circumstances.

2. Exception — Promoting the privacy of electronic health information (§171.202)

ONC proposes an exception to protect the privacy of an individual's EHI. 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 under this exception 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 proposed under the rule, the terms and conditions of each "sub-exception" must be met at all relevant times. ONC notes 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 its privacy exception does not conflict with the HIPAA Privacy Rule framework and that it does promote patient privacy rights. However, ONC acknowledges that its information blocking rule may require actors to provide access, exchange, or use 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 proposed exceptions.

Definition of individual. For purposes only of this exception and its four "sub-exceptions," ONC proposes 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. ONC proposes to define individual as meaning one or more of the following:

(1) An individual (as defined under 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, including as a personal representative, in accordance with the HIPAA Privacy Rule;
  (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). The purpose of the proposed expansive definition is to protect information about all individuals, not just individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates.

(1) *Sub-exception: Precondition imposed by law not satisfied.* Because state and federal privacy laws may impose conditions before disclosure of PHI is permitted, ONC proposes to protect actors who do not provide access, exchange or use EHI because a necessary precondition imposed under law for that disclosure has not been met. Thus, an actor in this situation may elect

not to provide access, exchange, or use such EHI if the precondition under law has not been satisfied, subject to a number of conditions. However, ONC is concerned that an actor could use protection of an individual's privacy as a pretext for information blocking.

An actor could qualify for this exception by written organizational policies that specify the criteria an actor will use, and the steps the actor will take, to satisfy the legal precondition. This could 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.

Alternatively, an actor could document, on a case-by-case basis, the criteria it uses to determine when the legal precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met. The documentation would have to identify the specific circumstances of the practice, the criteria the actor used 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 would have to do all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization. This might mean a legally compliant consent form; ONC notes that a best practice would include informing the individual of the right to revoke consent. ONC cautions that the actor could not improperly encourage the individual to refuse to provide the consent or authorization.

ONC would also require that the actor's practice be tailored to the specific privacy risk or interest being addressed. ONC believes this would require the actor to carefully evaluate the privacy requirements imposed on the actor and the privacy interests to be managed by the actor, and to 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.

(2) *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 notes that some direct-to-consumer products and services would not benefit from that sub-exception. For these developers of certified health IT not required to comply with the HIPAA Privacy Rule (referred to by ONC in this sub-exception as non-covered actors), ONC proposes to create this sub-exception. 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 of EHI if the practice meets all the following conditions:

- The practice complies with applicable state or federal privacy laws.
- The practice implements a process described in the actor's organizational privacy policy. ONC clarifies it expects detailed documentation of the processes and procedures used to

determine when the actor will not provide access, exchange or use of EHI as well as a description of the specific requirements imposed on individuals giving consent.

- The practice had previously been meaningfully disclosed to the persons and entities that use the actor's product or service. In evaluating whether the disclosure is meaningful, ONC will consider whether the disclosure was in plain language and conspicuous. However, ONC notes non-covered actors would not have to disclose organizational privacy policy to its customers or to the public generally; rather, only the privacy-protective practices it has adopted must be described in sufficient detail.
- The practice is tailored to the specific privacy risk or interest being addressed.
- The practice is implemented in a consistent and non-discriminatory manner.

(3) S*ub-exception: Denial of an individual's request for their ePHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3).* 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. This exception would apply to both the unreviewable grounds and reviewable grounds of denials of access.

Unreviewable grounds. 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; and
- 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[35] and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Reviewable grounds. The reviewable grounds of denial of access to PHI permit a covered entity to deny access if the individual is given a right to have that denial reviewed under certain circumstances. For example, a licensed health care professional, in the exercise of professional judgment, may determine that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. If access is denied, then the individual has the right to have the denial reviewed by a licensed health professional who did not participate in the original decision to deny access.

ONC proposes a limited exception to permit a covered entity or business associate to deny an individual's request for access to their PHI on the basis of these unreviewable and reviewable grounds as long as the denial complies with HIPAA Privacy Rule requirements.

[35] 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)).

(4) *Sub-exception: Respecting an individual's request not to share information.* ONC believes an exception is necessary to ensure actors are confident that they may respect an individual's privacy choices when that individual specifically asks an actor not to provide access, exchange, or use EHI. Thus, ONC proposes that 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 requests 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 or its agent 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 would be 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.

3. Exception — Promoting the security of electronic health information (§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 proposes 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 proposed exception.

(1) *Conditions.* 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 would 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.

Actors could meet the requirements for this exception through practices that implement either security policies and practices developed by the actor (i.e., organizational security policies) or through case-by-case determinations.

(2) *Organizational security policies.* If the practice implements an organizational securitypolicy, the policy must—

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

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.

(3) *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. Exception — Recovering costs reasonably incurred (§171.204)

ONC proposes an exception to permit actors to recover certain costs they reasonably incur in providing access to, exchange of, or use of EHI that would promote innovation, competition, and consumer welfare. 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. ONCbelieves that absent an exception, actors may be unable to recover costs they incur to develop technologies and provide services that enhance interoperability. To qualify for this exception, each practice by an actor must meet all the following conditions. 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.

(1) *Types of costs*. ONC would tailor 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 would not include speculative or subjective costs. Further, ONC says that the exception would not apply to fees (e.g., those based on profit or revenue for use of EHI) that exceed the actor's reasonable costs for providing access, exchange or use of EHI.

(2) *Method for recovering costs*. The method by which the actor recovers its costs would have to be reasonable and non-discriminatory. Specifically, the method for recovering costs must meet all the following conditions:

- It must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.
- It must be reasonably related to the actor's costs of providing the type of access, exchange, or use to the person or entity to whom the fee is charged. ONC clarifies that an actor is not required to apply the same prices or price terms for everyone to whom it provides services; however, any price differences would have to be based on actual differences in costs the actor incurred or on other reasonable or non-discriminatory criteria.
- It must be reasonably allocated among all customers 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. ONC also cautions that actors may not recover all core costs from each customer.
- It must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor.
- It must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of EHI (including the secondary use of such information) that <u>exceeds</u> the actor's reasonable costs for providing access, exchange, or use of EHI. ONC emphasizes revenue-sharing or profit-sharing arrangements would only be covered by the exception if they are designed to provide an alternative way to recover costs reasonably incurred for providing the services.

(3) *Costs specifically excluded*. ONC excludes certain types of costs from protection under this exception to the information blocking rule. Specifically, the exception would not apply to any of the following costs or fees:

- Costs due to non-standard design or implementation choices. These are costs actors incur because the health IT is designed or implemented in non-standard ways that <u>unnecessarily</u> increase the complexity, difficulty or burden of accessing, exchanging, or using EHI.
- Subjective or speculative costs. These are costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets, or opportunity costs, except for the reasonable forward-looking cost of capital.
- The types of fee 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.[36]

- A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's EHI. 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[37] to switch health IT or to provide patients their EHI.
- A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

ONC also 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 be a practice that implicates the information blocking rule as long as the fee charged for that access complied with the HIPAA Privacy Rule. ONC believes the last two examples of costs specifically excluded from this exception (those relating to export and portability of EHI in EHR systems) are the types of costs specifically contemplated by the information blocking rule. 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.

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 as well as the exception for requests that are infeasible under the exception proposed at §171.205 (described below). These fees would have to be agreed to in writing when the technology is acquired.

(4) *Compliance with the Conditions of Certification*. ONC notes that a health IT developer of certified health IT subject to the API Condition of Certification[38] may not charge certain types of fees and also are subject to more specific cost accountability rules than apply under this proposed exception. ONC proposes 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. Additionally, ONC proposes that an API Data Provider (including a health care provider that acts as an API Data Provider) may only charge the same

[36] 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.

[37] See 45 CFR 170.315(b)(10).

[38] See 45 CFR 170.404.

fees that an API Technology Supplier may charge to recover costs consistent with the permitted fees specified in the API Condition of Certification.

5. Exception — Responding to requests that are infeasible (§171.205)

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 proposes 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 would use 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.

(1) *Request is infeasible*. ONC proposes a two-step test to determine when a request is infeasible: the actor must demonstrate that the request poses a substantial burden and that assuming that burden is plainly unreasonable under the circumstances.

Substantial burden. The actor must demonstrate that complying with the request in the manner requested would impose a substantial burden on the actor. ONC believes that actors would most likely meet this requirement by showing that they did not have, and could not readily obtain, the requisite technological capabilities, legal rights, or other means necessary to facilitate the particular type of access, exchange, or use requested. Actors could also show that complying with the request would have caused a significant disruption to its health care or business activities or that it would have incurred significant unbudgeted costs.

In determining whether a burden is substantial for this test, ONC would take a fact-specific approach and consider an actor's particular circumstances, including the type of actor, the nature and purpose of its business or other activities, and the financial, technical, and other resources and expertise at its disposal. It would also consider any possible offsetting benefits of complying with the request, such as meeting statutory or regulatory requirements.

Plainly unreasonable. ONC proposes a number of factors it would consider to determine whether a substantial burden is plainly unreasonable 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 provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged;
- Whether the actor maintains ePHI on behalf of a HIPAA covered entity or maintains EHI on behalf of the requestor or another person whose access, exchange, or use of EHI will be enabled or facilitated by the actor's compliance with the request;
- Whether the requestor and other relevant persons can reasonably access, exchange, or use the EHI from other sources or through other means; and
- The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

ONC would consider the type of EHI at issue, the purposes for which the EHI is needed, the severity of the burden imposed on the actor, and the frequency of the type of request at issue. ONC would balance the burdens against the costs to the requestors (and other persons) who would be harmed by the refusal to provide the access, exchange or use, including whether the requestor could have acquired the EHI through other means. Finally, ONC would also consider the balancing of relative burdens in conjunction with the actor's control over interoperability elements; for example, a dominant health system that provides local health IT infrastructure would have to demonstrate an extreme hardship to justify denying interconnection requests or access to interoperability elements.

ONC notes that an actor could be covered under this exception if it is unable to provide access, exchange or use of EHI due to a natural disaster (e.g., hurricane or earthquake) or war.

Plainly not burdensome. ONC indicates that the following circumstances do not constitute a burden to the actor for purposes of this exception; ONC would not consider them in determining whether a request is infeasible.

- Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.
- Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(2) *Responding to requests*. The actor would have to respond to all requests relating to access, exchange, or use of EHI in a timely manner, including requests to establish connections and to provide interoperability elements. ONC would analyze whether a response is timely based on what is objectively reasonable for the actor.

(3) *Written explanation*. The actor would have to provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(4) *Provision of a reasonable alternative*. 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.

6. Exception — Licensing of interoperability elements on reasonable and nondiscriminatory terms (§171.206)

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 licensed 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 includes examples of situations that do and do not implicate the information blocking rule. ONC is concerned by the use of contractual and intellectual property rights to extract rents for access to EHI or to prevent competition from developers of interoperable technologies which it believes undermines the fundamental objectives of the information blocking rule.

ONC proposes 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. Acknowledging that its proposal to prevent intellectual property owners from extracting rents for access to EHI differs from standard intellectual property policy, ONC believes its proposal to limit rents to RAND terms is essential because rents will likely frustrate access, exchange and use of EHI. ONC notes that actors who do not want to license a particular technology may choose to develop and provide alternative means to access, exchange and use EHI as long as it is similarly efficient and efficacious. To qualify for this exception, each practice by an actor would have to meet the following conditions at all relevant times.

(1) *Reasonable and non-discriminatory (RAND) terms*. To qualify for this exception, actors must license interoperability elements on terms that are reasonable and nondiscriminatory. ONC notes that standards development organizations have policies requiring members who contribute technologies to a standard to voluntarily commit to license those technologies on RAND terms. ONC believes its proposed RAND requirement balances the need for robust intellectual property (IP) protections with the need to ensure that this proposed exception does not permit actors to exercise their IP or other proprietary rights in inappropriate ways that block the development, adoption, or use of interoperable technologies and services. To meet the RAND condition, actors must comply with the following requirements:

Responding to requests. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request. That response would require negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed and offering an appropriate license with reasonable and non-discriminatory terms. ONC notes that actors are not required to grant a license in all instances as long as the negotiations are conducted under RAND terms and an offer pursuant to those negotiations is made. ONC does not propose to establish a deadline by which negotiations must be concluded.

Scope of rights. ONC proposes that an actor must license the requested interoperability elements with all rights necessary for access and use for the following purposes, as applicable:

- Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control. ONC notes this would include the right to incorporate and use the interoperability elements in the licensee's own technology to the extent necessary.
- Marketing, offering, and distributing the interoperable products and/or services to potential customers and users. This would include the right to copy or disclose the interoperability elements as necessary.
- Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of EHI.

Reasonable royalty. If the actor charges a royalty for the use of interoperability elements, the royalty would have to be reasonable. To qualify for this exception, a royalty would have to meet the following requirements:

- The royalty must be non-discriminatory.
- The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using EHI.
- If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on RAND terms, the actor may charge a royalty that is consistent with those policies.

ONC lists 10 factors that it may consider in determining whether a royalty is reasonable which the agency says mirror factors used by courts considering the reasonableness of royalties charged under a commitment to a standards development organization to license technologies on RAND terms.

Non-discriminatory terms. ONC would require that the terms on which an actor licenses and otherwise provides the interoperability elements must be non-discriminatory; this would apply to terms that relate to the price as well as other terms such as royalties. The actor would have to comply with the following requirements:

- 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.
- The terms must not be based in any part on—
  - o 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
  - o The revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements, including the secondary use of the EHI.

ONC notes that actors do not have to apply the same terms for all persons requesting a license, but 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 arms-length transactions. However, ONC reminds developers of certified health IT that the Condition of Certification under proposed §170.404 would preclude the developer from offering APIs on different terms.

Collateral terms. ONC proposes 5 additional conditions that it says would provide "bright-line prohibitions" for certain types of collateral terms or agreements that it believes will interfere with access, exchange, or use of EHI. To qualify for this exception, ONC proposes to prohibit an actor from requiring 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. ONC is concerned that actors could require licensees to take license to interoperability elements it does not want; this would permit the actor to extract royalties inconsistent with the requirement for RAND terms and conditions. However, nothing would preclude an actor and licensee from voluntarily agreeing to such an arrangement.
- License, grant, assign, or transfer to the actor any intellectual property of the licensee. However, a willing agreement between the parties to cross-license or co-market intellectual property would be permissible.
- Pay a fee of any kind (other than a reasonable royalty described above) unless the practice meets the requirements of the proposed exception for costs reasonably incurred at §171.204 (described above).

Non-disclosure agreement. ONC proposes 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 would have to specify all information the actor claims as trade secrets, and the information would have to meet the definition of a trade secret under applicable law. ONC notes that a developer of certified health IT may be subject to the Condition of Certification proposed in the ONC proposed rule at §170.403 (which prohibits certain health IT developer prohibitions and restrictions on communications about the developer's technology and business practices), and if so, this exception would not affect the developer's obligations to comply with that condition.

(2) *Additional requirements relating to the provision of interoperability elements*. To qualify for this exception, an actor could also 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.

ONC says the intent behind these additional conditions is to ensure that actors who license interoperability elements on RAND terms do not engage in separate practices that impede theuse 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 does clarify that this condition would not prevent an actor from making improvements to its technology or responding to its customers' or users' needs; however, the actor's practice would need to be necessary to accomplish these purposes, and the actor must provide the licensee a reasonable opportunity to update its technology to maintain interoperability.

(3) *Compliance with conditions of certification*. ONC notes that a health IT developer subject to the conditions of certification proposed in the ONC rule at §§170.402, 170.403, or 170.404 must comply with all requirements of such conditions for all practices and at all relevant times.

7. Exception — Maintaining and improving health IT performance (§171.207)

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 proposes 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. This exception would apply to both planned and unplanned maintenance and improvement. ONC acknowledges that health IT performance is often measured by service level agreements that provide flexibility to ensure that system availability is balanced with essential maintenance and improvements. Where the provision of health IT is subject to an allowance for maintenance or improvement that has been agreed to by the recipient of that health IT, ONC proposes that neither that agreement, nor the performance of it, should constitute information blocking, provided that certain conditions are met.

(1) *Maintenance and improvements to health IT*. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT if the actor's practice is—

- For a period of time no longer than necessary to achieve the maintenance or improvements;
- Implemented in a consistent and non-discriminatory manner; and
- If the unavailability is initiated by an actor that is a health IT developer of certified health IT, a HIE, or a HIN, the practice is agreed to by the individual or entity to whom the actor supplied the health IT.

ONC notes that it would be more difficult to evaluate what time period is "no longer than necessary" in the case of unplanned maintenance or improvement since these are typically initiated by a threat or risk that must be responded to urgently and for as long as the risk persists. 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 also notes that 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.

(2) *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 would not need to satisfy the requirements of this exception; however, the actor would have to comply with all the requirements for the exception for preventing harm proposed at §171.201 (described above) at all relevant times to qualify for an exception.

(3) *Security-related practices*. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to EHI, the actor would not need to satisfy the requirements of this exception; however, the actor would have to comply with all requirements for the exception for promoting the security of EHI proposed at §171.203 (described above) at all relevant times to qualify for an exception.

ONC is considering whether to expand this 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.

C. Additional Exceptions—Request for Information

ONC is considering 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. This would be intended to support adoption of the Common Agreement and encourage other entities to participate in trusted exchange. The exception would provide protection for practices expressly required by the Common Agreement or necessary to implement those requirements. ONC expects that its proposed exception would apply only to contract terms, policies and other practices that are strictly necessary to comply with the Common Agreement, and the exception would apply to practices that are no broader than necessary under the circumstances.

ONC seeks feedback on this potential exception, including whether it is necessary and whether there could be negative effects.

Separately, ONC welcomes comment on potential additional exceptions it should consider for future rulemaking.

D. Complaint Process

Section 3022 of the PHS Act 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.

ONC indicates that it will implement the process by building on existing mechanisms, including the current complaint process at https://www.healthit.gov/healthit-feedback. **ONC seeks comment on this approach as well as on the following specific issues:**

- What types of information are most important to collect in order to identify potential instances of information blocking?
- What types of information are contemplated by the following categories: the originating institution; location; type of transaction; system and version; timestamp; terminating institution; locations; system and version; failure notice; and other related information?
- What types of information or data elements should be collected under each of the above categories?
- What additional types of information beyond the above may be relevant to complaints and allegations of information blocking, especially practices that involve contractual or other business practices for which some of the categories of technical or transactional information above may not apply?
- How can ONC encourage and streamline the collection of such information so as to minimize burden and encourage the submission of complaints, especially complaints about practices that raise the types of information blocking concerns described in this proposed rule?
- How can ONC facilitate the inclusion of sufficient detail and granularity in complaints to enable effective investigations?
- What safeguards should be provided to support adequate confidentiality and handling of information that could: (1) identify the source of the complaint or allegation; (2) contain other individually identifiable information; and (3) contain confidential or proprietary business information?

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 seeks information on existing disincentives, as well as potential modifications to them, that would serve as effective deterrents. ONC also seeks information 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.

VIII. Registries Request for Information

ONC discusses its activities related to implementation of sections 4005(a) and (b) of the Cures Act, which pertain to interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. It describes the myriad of public reporting requirements for which a lack of standardization has contributed to slow adoption of health IT systems among registries[39]. Working with stakeholders, ONC has identified a wide range of areas where the use of standards could significantly improve bidirectional exchange with registries for purposes of public health, quality reporting, care quality improvement and others.

Among its actions, ONC included certification criteria in the 2015 Edition final rule on bidirectional exchange and this proposed rule includes processes for updating standards and new policies on real world testing focused on functionality in a practice setting. Additionally, ONC has worked with CMS on guidance for qualified clinical data registries under the Merit-based Incentive Payment System and with the CDC and states to support enhancements of prescription drug monitoring programs.

ONC seeks information on how IT solutions and the proposals in this rule can aid bidirectional exchange with registries for a wide range of public health, quality reporting and clinical quality improvement activities. Specifically, ONC seeks comment on use cases where an API using FHIR Release 4 might support improved exchange between a provider and a registry. Comments are sought on how this may:

- Reduce the burden of implementing multiple solutions for various types of exchange, while still supporting the variability needed to exchange information with registries devoted to the care of a population defined by a disease, condition, exposure, or therapy;
- Allow for the collection of detailed, standardized data on an ongoing basis formedical procedures, services, or therapies for diseases, conditions, or exposures;
- Support an overall approach to data quality, including the systematic collection ofclinical and other health care data, using standardized data elements and procedures to verify the completeness and validity of those data;
- Improve and enhance the ability of providers to leverage feedback from a registry to improve patient care; and
- Address a sufficiently wide range of use cases to warrant the prioritization of technical innovation on API-based options over the continued development of use-case-specific solutions in future rulemaking.

Other comments stakeholders may have on implementation of the registries provisions under section 4005 of the Cures Act are welcomed.

[39] See ONC draft report for public comment: *Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs*. December 2018. https://www.healthit.gov/topic/usability-and-provider-burden/strategy-reducing-burden-relating-use-health-it-and-ehrs

IX. Patient Matching Request for Information

ONC reviews the legislative history[40] and its own efforts to improve "patient matching," or the linking of one patient's data within and across health care providers in order to obtain a comprehensive and longitudinal view of that patient's health care. At a minimum, patient matching is accomplished by linking demographic data fields such as name, birth date, sex, phone number, and address. ONC notes that accurate and standardized data capture and exchange and optimized algorithm performance are critical components to accurate patient matching. Among its activities, ONC launched in 2017 the Patient Matching Algorithm Challenge, to bring about greater transparency and data on the performance of existing patient matching algorithms, spur the adoption of performance metrics for patient matching algorithm developers, and improve other aspects of patient matching such as deduplication and linking.

ONC seeks comment on additional opportunities for patient matching and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. (CMS also issued an RFI in its recent proposed rule on interoperability and patient access.) ONC is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability. It considers patient matching a quality of care and patient safety issue because inaccurate patient matching can lead to inappropriate and unnecessary care; unnecessary burden on both patients and providers to correct misidentification; time consuming and expensive burden on health systems to detect and reconcile duplicate patient records and improper record merges; and poor oversite into fraud and abuse. Stakeholder input is sought on creative, innovative, and effective approaches to patient matching within and across providers.

In particular, ONC ask for responses to the following:

- It is a common misconception that technology alone can solve the problem of poor data quality, but even the most advanced, innovative technical approaches are unable to overcome data quality issues. Thus, input is sought on the potential effect that data collection standards may have on the quality of health data that is captured and stored and the impact that such standards may have on accurate patient matching. Input is also sought on other solutions that may increase the likelihood of accurate data capture, including the implementation of technology that supports the verification and authentication of certain demographic data elements such as mailing address, as well as other efforts that support ongoing data quality improvement efforts.
- In concert with the January 2019 GAO study on patient matching[41], ONC seeks input on what additional data elements could be defined to assist in patient matching as well as input on a required minimum set of elements that need to be collected and exchanged. Stakeholders are encouraged to review the Patient Demographic Record Matching section of

[40] See House Report 114-699, Departments of Labor, HHS, and Education and Related Agencies Appropriations Bill, 2017. July 2016. https://www.congress.gov/congressional-report/114th-congress/house-report/699/1 and section 4007 of the Cures Act (GAO study).

[41] U.S. Government Accountability Office, *Approaches and Challenges to Electronically Matching Patients' Records across Providers,* GAO-19-197, https://www.gao.gov/assets/700/696426.pdf.

the Interoperability Standards Advisory[42] and comment on the standards and implementation specifications outlined. Public comments and subject matter feedback on all sections of the Interoperability Standards Advisory are accepted year-round.

- Also in alignment with the GAO study, ONC seeks input on whether and what requirements for electronic health records could be established to assure data used for patient matching is collected accurately and completely for every patient. For instance, the adopted 2015 Edition "transitions of care" certification criterion (§170.315(b)(1)) currently includes patient matching requirements for first name, last name, previous name, middle name, suffix, date of birth, address, phone number, and sex. These requirements also include format constraints for some of the data.
- There are unique matching issues related to pediatrics, and ONC seeks comment on innovative and effective technical or non-technical approaches that could support accurate pediatric record matching.
- Recent research suggests that involving patients in patient matching may be a viable and effective solution to increase the accuracy of matching, and giving patients access to their own clinical information empowers engagements and improved health outcomes. ONC seeks comment on potential solutions that include patients through a variety of methods and technical platforms in the capture, update and maintenance of their own demographic and health data, including privacy criteria and the role of providers as educators and advocates.
- Comments are sought on standardized metrics for the performance evaluation of available patient matching algorithms. Health IT developers are each relying on a number of patient matching algorithms, however, without the adoption of agreed upon metrics for the valuation of algorithm performance across the industry, existing matching approaches cannot be accurately evaluated or compared across systems or over time.
- Input is sought on transparent patient matching indicators such as database duplicate rate, duplicate creation rate, and true match rate, for example, that are necessary for assessment and reporting. ONC believes that the current lack of consensus, adoption, and transparency of such indicators makes communication, reporting, and cross-provider or cross-organizational comparisons impossible, impedes a full and accurate assessment of the extent of the problem, prohibits informed decision making, limits research on complementary matching methods, and inhibits progress and innovation in this area.
- Emerging private-sector led approaches in patient matching may prove to be effective, and ONC seeks input on these approaches in general. Matching services that leverage referential matching technology have emerged in the market recently, yet evaluations of this type of approach have either not been conducted or have not been made public. Other innovative technical approaches such as biometrics, machine learning and artificial intelligence, or locally developed unique identifier efforts, when used in combination with non-technical approaches such as patient engagement, supportive policies, data governance, and ongoing data quality improvement efforts may enhance capacity for matching.
- Finally, ONC seeks input on new data that could be added to the United States Core Data for Interoperability (USCDI) or further constrained within it in order to support patient matching.

[42] https://www.healthit.gov/isa/patient-demographic-record-matching

X. Incorporation by Reference

In this section of the proposed 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.

XI. 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 proposed 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 proposed rule are either considered minimal burden or are not subject to the PRA.

OMB has determined that this proposed 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 proposed rule. The analysis concludes that in the aggregate, the net benefit of the proposed rule would fall in the range of $2.7 billion to $8.2 billion for the first year after it is finalized averaging $5.5 billion. The total "perpetual" annual net benefit starting in year 2, would range from $2.9 billion to $8.7 billion, averaging $5.8 billion.

For most estimates a wide range of possible dollar effects is provided because of the uncertainty of the precise impact of the proposed rule policies, and ONC notes that not all the effects of proposed 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 $642 million 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 $6.1 billion, including $2.5 billion garnered by payers and patients and $2.3 billion by hospitals and clinicians. (Costs in the second year and later are lower, averaging $340 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 proposed 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 UCSDI data elements ($183 million); development and maintenance of the EHI export criterion ($96 million); development and maintenance of APIs ($300 million); and real-world testing ($46 million).

- While some cost savings would accrue to developers from the proposed deregulatory actions, the main benefits would be gained by hospitals and clinicians from the addition of the data export criterion ($1.1 billion); the proposed API criterion ($1.9 billion) and real world testing ($279 million).