HIMSS®

transforming health through information and technology™

33 West Monroe Street
Suite 1700
Chicago, IL 60603-5616 USA
Phone 312.664.HIMSS (664.4667)
Phone 312.664.6143
www.himss.org

June 3, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
US Department of Health and Human Services
Washington, DC 20201

Dear Dr. Rucker:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments to the Notice of Proposed Rule Making (NPRM) on the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (RIN: 0955-AA01). We appreciate this opportunity to utilize our members' expertise in offering feedback in support of seamless and secure access, exchange, and use of electronic health information (EHI); the conditions and maintenance of certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program; and, the reasonable and necessary activities that do not constitute information blocking.

HIMSS is a global advisor and thought leader supporting the transformation of health through information and technology. As a mission-driven charitable organization, HIMSS offers a unique perspective with deep expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology. Through our innovation companies, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision.

As an association, HIMSS encompasses more than 76,000 individual members and 660 corporate members. We collaborate with hundreds of providers, academic institutions, and health services organizations on strategic initiatives to advance the use of innovative information and technology. Together, we work to improve health, access, as well as the quality and cost-effectiveness of healthcare. Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, United Kingdom, the Middle East, and Asia Pacific.

The 21st Century Cures Act addresses many of the issues that are critical to facilitate greater nationwide interoperability and information exchange. HIMSS commends ONC for its work in this proposed rule to tackle these issues and put our health system and stakeholders on a path to transform healthcare. We fully support the efforts from across the Department of Health and Human Services (HHS) to provide patients with secure access to actionable information that assists them in directing their own healthcare as well as inhibits the blocking of information that contributes to more seamless care delivery. In addition, the ONC regulation helps set a course for a healthcare paradigm that takes full advantage of the promise of standards-based application programming interface (API) technology, and capitalizes on the inherent opportunities for innovation and makes allowances for encouraging new market entrants. Overall, HIMSS appreciates the opportunity to help HHS create a new healthcare ecosystem that reinforces the secure access to, exchange of, and use of EHI.

Our HIMSS proposed regulation public comments are divided into two sections: an overview of our key public comments, followed by more substantive, detailed comments on each section of the regulation.

<u>Overview of Key HIMSS Public Comments</u>

Information Blocking

HIMSS supports, at a high level, the Information Blocking Exceptions in the proposed regulation, as they identify the appropriate categories that will help inform the community as well as define sharing boundaries and expectations that will lead to greater information exchange. Themes from the Information Blocking Exceptions all bolster ONC's approach: implemented in a consistent and non-discriminatory manner; reasonably related and uniformly applied; and, based on objective and verifiable criteria.

Although we support the exception categories identified, under each of the identified exceptions, we recommend specific refinements and clarifications for inclusion in the regulatory text. Each of the exceptions needs to have clearer definitions and requirements with more examples of what a valid exception in each of the seven categories would look like. If there is ambiguous regulatory text on what is and what is not information blocking, as well as the circumstances when a designated actor could make an information blocking claim, it will be exceedingly difficult for a Health Care Provider, Health IT Developer, Health Information Exchange (HIE), and Health Information Network (HIN) to do its part to support the free flow of information across the healthcare ecosystem.

We are also asking ONC to promulgate a list of best practices for broadly sharing more information, consistent with these exceptions. Such a list could serve to reinforce the positive behaviors expected of the regulated actors, establishing "safe lanes" for specific use cases and reducing compliance costs and risks. These best practices could also help communicate more detailed information around the intended roles and expectations for each of the regulated actors, developers, providers, or networks/exchanges.

In addition, HIMSS wants ONC to scale back the definitions of "Provider," "Electronic Health Information (EHI)," and "Access."

For EHI, HIMSS supports a curtailed definition that focuses on using the US Core Data for Interoperability (USCDI) data classes as the current requirement in the near-term. In the future, HIMSS would like to see USCDI expanded to include additional data classes that encompass more information streams, including: social determinants of health data, patient-generated health data, wearables data, genomics data, and healthcare cost and price information.

HIMSS is also asking ONC to combine the definitions of HIN and HIE, and tighten up this new merged category to clearly detail the entities that would and would not be considered an HIE or an HIN in the final rule.

Moreover, HIMSS wants ONC to adopt Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) Release 4 (R4) in the final rule for reference, requiring health IT developers seeking certification to build, test, and certify systems solely to FHIR R4 and its associated implementation specifications.

APIs

HIMSS supports the idea that health IT developers publish APIs and allow health information from such technology "to be accessed, exchanged, and used without special effort." Overall, HIMSS applauds the creation of the API Technology Suppliers' Development, Deployment, and Upgrade Fees as well as Value-Added Services Fees. We appreciate the proposed regulation's prohibition on any fees, except those expressly permitted, and support the idea that Technology Suppliers should not engage in pricing practices that create barriers to entry and competition for apps that health care providers seek to use.

However, we note that the complexities created in this proposed fee structure may lead to less innovation, increased administrative burden, and a focus on cost recovery rather than creation of novel ways to improve data access.

HIMSS endorses ONC's emphasis on the fact that fees cannot be used 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. We recommend changes to the parameters around API Usage-Based Fees that focus on volume thresholds being included in any contractual language related to these fees, to ensure that any incremental costs attributable to supporting API interactions at increasing volumes and scale are addressed appropriately.

Conditions and Maintenance of Certification Requirements

HIMSS supports the removal of the identified 2015 Edition Certification requirements, the direction of the updated criteria identified in the 2015 Edition, and the criteria targeted for revision. In addition, we appreciate the updated criterion for a standardized API for patient and population services, and the use of HL7 FHIR standards and the additional named implementation specifications. Overall, we recognize and support the importance of ONC's approach to promoting open APIs and the directional signal that ONC is sending to the community by specifying HL7 FHIR.

As for the Assurances requirement as a Condition of Certification under the Program, health IT developers must provide functionality within 24 months of 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. HIMSS encourages ONC to examine the potential ramifications of these aggressive timelines to ensure that burdens to implementers and providers are minimized. If possible, HIMSS suggests approaching complex new requirements in a phased fashion to incrementally require advanced features or additional data sets over set periods of time.

For the Real World Testing requirement, HIMSS strongly supports this concept and the Standards

Version Advancement Process. Tools to test conformance in healthcare settings are often a limiting factor, and HIMSS recognizes ONC's vision to advance standards in the absence of robust conformance testing tools, however HIMSS encourages ONC to invest along with the private sector to help develop more advanced conformance test tools and require conformance testing once tools become available.

Relevant Requests for Information (RFIs)
For the RFIs related to the Trusted Exchange Framework and Common Agreement (TEFCA), our position is that until a final TEFCA guidance document is released with the full parameters described around the enterprise, it is difficult to consider whether any entity should be required to participate in the Framework, or an information blocking exception should be structured around it. Overall, the underlying concept and goals of TEFCA are forward-looking: to provide a single on-ramp to nationwide connectivity and enable EHI to securely follow the patient when and where it is needed. However, we need to see the final guidance document before rendering a judgement on its usefulness toward the community's efforts to more broadly share information.

In conclusion, HIMSS is going to work across the entire stakeholder community to emphasize the importance of increased funding levels for ONC. The proposed regulation presents a greater workload for an agency that has been chronically underfunded. Although ONC plans to leverage other HHS agencies to help with the development and enforcement activities included in the regulation, this entire effort is dependent on a robust ONC. In its advocacy efforts, HIMSS will emphasize that an increased workload at ONC needs to be accompanied by a concomitant increase in funding levels to carry out its new responsibilities.

HIMSS would like to thank ONC for the opportunity to comment on the proposed rule as we strongly support its focus on advancing interoperability; supporting the access, exchange, and use of EHI; and, addressing occurrences of information blocking. We welcome the opportunity to meet with you and your team to discuss our comments in more depth. Please do not hesitate to contact Jeff Coughlin, Senior Director, Federal & State Affairs, at 703.562.8824, or Eli Fleet, Director, Federal Affairs, at 703.562.8834, with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F Wolf III

Harold F. Wolf III, FHIMSS
President & CEO
HIMSS

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

Section III – Deregulatory Actions for Previous Rulemakings

Removal of Randomized Surveillance Requirements

We propose to revise § 170.556(c) by changing the requirement that ONC-Authorized Certification Bodies (ONC-ACBs) must conduct in-the-field, randomized surveillance to specify that ONC-ACBs may conduct in-the-field, randomized surveillance.

We further propose to remove the following:

- The specification that ONC-ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year.
- Requirements regarding the exclusion and exhaustion of selected locations for randomized surveillance.
- Requirements regarding the consecutive selection of certified health IT for randomized surveillance.

Without these regulatory requirements, ONC-ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, using the methodology identified by ONC with respect to scope and selection method, and the number and types of locations for in-the-field surveillance.

Preamble FR Citation: 84 FR 7434 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7562-63 for estimates related to the removal of randomized surveillance requirements.

Public Comment Field:

HIMSS supports ONC's approach to reduce administrative burden and implement required deregulatory actions as part of the rulemaking process. HIMSS supports all of the six identified activities, including:

- The removal of requirement that ONC-Authorized Certification Bodies (ONC-ACBs) must conduct randomized in-the-field surveillance, since stakeholders have expressed concern that the benefits of in-the-field, randomized surveillance may not outweigh the cost, effort, and time commitment required by providers, particularly if non-conformities are note found. The removal of randomized surveillance requirements would also give ONC-ACBs more time to focus on other priorities. HIMSS supports the concept of submitting real-world testing plans as a requirement for certification.

Removal of Certain 2015 Edition Certification Criteria

We propose to remove certain certification criteria, including criteria that are and are not currently included in the 2015 Edition Base EHR definition at §170.102.

We propose to remove from § 170.315 and § 170.102 the following 2015 Edition Criteria that are currently included in the 2015 Edition Base EHR definition:

- "problem list"
- "medication list"
- "medication allergy list"
- "drug formulary and preferred drug list checks"
- "smoking status"

We also propose to remove from § 170.315 the following 2015 Edition certification criteria that are not included in the 2015 Edition Base EHR definition:

- Patient-specific education resources
- Common Clinical Data Set Summary (CCDS) Record – Create
- Common Clinical Data Set Summary (CCDS) Record – Receive
- Secure Messaging

Preamble FR Citation: 84 FR 7435-37 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7565-66 for estimates related to the removal of certain 2015 Edition certification criteria and standards.

Public Comment Field:

HIMSS supports the removal of the identified 2015 Edition Certification criteria. ONC Certification was designed to be a floor, not a ceiling. The requirements identified for removal make sense because they are almost all universally present in today's health IT products, and/or the requirements being removed would need to be present in order fulfill more advanced, updated certification requirements.

Request for Information on the Development of Similar Independent Program Processes

Recognition of the FDA Software Pre-Certification Program for purposes of certification of health IT to 2015 Edition criteria may eventually be determined to be infeasible or insufficient to meet our goals of reducing burden and promoting innovation. With this in mind, we request comment on whether ONC should establish new regulatory processes tailored towards recognizing the unique characteristics of health IT (e.g., electronic health record (EHR) software) by looking first at the health IT developer, rather than primarily at the health IT presented for certification, as is currently done under the Program. We also welcome more specific comments on the health IT developer criteria for such an approach, as well as what the Conditions and/or Maintenance of Certification requirements should be to support such an approach within the framework of the proposed Conditions and Maintenance of Certification requirements discussed in section VII of this proposed rule.

Preamble FR Citation: 84 FR 7439 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS recommends that ONC work with FDA to better understand the successes and challenges of the Pre-Cert Program thus far, and investigate how it could apply to health IT certification. The concept underlying the Program is sound, in terms of providing a more streamlined and efficient regulatory oversight of software-based medical devices developed by manufacturers who have demonstrated a robust culture of quality and organizational excellence, and who are committed to monitoring real-world performance of their products once they reach the U.S. market. Health IT developers would welcome the idea of applying a similar approach to health IT certification processes.

However, the current outputs of FDA's Program are modest and it remains in a testing phase. Thus far, not much is yet finalized within the Framework. In addition, it is not clear if full rollout of Pre-Cert at FDA will proceed or if Congress will need to provide FDA with additional statutory authorities to fully implement the vision underlying Pre-Cert.

Overall, ONC should work with FDA to use the Pre-Cert Program as a potential model for a revamped certification program, and build on the lessons learned from that program thus far in the design of a new certification program. We support looking at Pre-Cert as a vehicle to instill more innovation into health IT certification and to reduce the reporting and administrative burden associated with the program. HIMSS would be interested in working with ONC to produce the health IT developer criteria as well as what the Conditions and/or Maintenance of Certification requirements would be for such an approach.

Section IV – Updates to the 2015 Edition Certification Criteria

§ 170.213 United States Core Data for Interoperability (USCDI)

We propose to adopt the USCDI at new § 170.213: “Standard. United States Core Data for Interoperability (USCDI), Version 1 (v1) (incorporated by reference in § 170.299).”

We propose to revise the following 2015 Edition certification criteria to incorporate the USCDI standard in place of the “Common Clinical Data Set” (currently defined at § 170.102 and proposed for removal in this rule):

- ‘‘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)).]

Preamble FR Citation: 84 FR 7441 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7567-68 for estimates related to this proposal.

Public Comment Field:

HIMSS generally supports the direction of the updated criteria identified in the 2015 Edition Certification requirements. HIMSS supports the updated criterion for Standardized API for patient and population services, and the use of Health Level 7 FHIR standards and the additional named implementation specifications. HIMSS recognizes and supports the importance of ONC’s approach to promoting open APIs and the directional signal that ONC is sending to the community by specifying HL7 FHIR. HIMSS strongly encourages the selection of FHIR R4, the latest balloted and normative version of FHIR, over any previous versions.

HIMSS wants ONC to adopt FHIR R4 in the final regulation for reference, requiring health IT developers seeking certification to build, test, and certify systems solely to FHIR R4 and its associated implementation specifications. ONC should designate R4 as the base standard and implementation specifications should be in subregulatory guidance.

This subregulatory guidance, in conjunction with the Standards Version Advancement Process, will help ensure a more nimble and flexible process to make newer versions of standards available to developers. Moreover, as the first normative FHIR standard, R4 will help with assurances around backward compatibility so applications that implement R4 no longer risk being nonconformant to the standard. HIMSS agrees with ONC that R4’s normative resources will be compelling to the entire community from a maturity and stability perspective.

HIMSS is concerned about finalizing R4 in regulation, as we want to ensure that there is an allowance for innovation in the standard. HIMSS typically recommends that ONC include standards and technical guidelines in use case specific implementation guides incorporated by reference, rather than integrating them directly into a regulation. By the time this final regulation is issued, it is likely that health IT developers will have a year’s worth of development experience with FHIR R4, and likely two to three years of development before the final regulation’s effective date, which should help support widespread implementation of R4.

§ 170.205(k) Clinical quality measure aggregate reporting

* * *

(3) CMS Implementation Guide for Quality Reporting Document Architecture Category III Eligible Clinicians and Eligible Professionals Programs Implementation Guide for 2019 (incorporated by reference in § 170.299).

Preamble FR Citation: 84 FR 7446 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The 2015 version of CEHRT was required to support both the HL7 Implementation Guide for the QRDA I and QRDA III standards as well as the Centers for Medicare and Medicaid Services (CMS) QRDA I and III Implementation Guide to collect and report electronic clinical quality measures (eCQMs.) The CMS QRDA Implementation Guide was built off the HL7 standard and added elements necessary to facilitate eCQMs to the CMS Inpatient Quality Reporting program and the Quality Payment Program.

In the proposed regulation, ONC stated its intent to remove the HL7 QRDA standard requirements from the 2015 Edition "CQMs-report" criteria and in their place, require Health IT Modules to support the CMS QRDA Implementation Guide in order to reduce the burden for health IT developers by only having to support one form of the QRDA standard.

While HIMSS understands the desire to have a single standard, we generally recommend standards to be developed and maintained through Standards Development Organizations (SDOs) such as HL7.

HIMSS therefore cautions ONC to limit any variations from the HL7 QRDA implementation guides in the CMS implementation guides to changes only required to facilitate reporting in CMS quality reporting programs. We recognize CMS's need for program specific changes, however, there is concern that if over time CMS diverges from the base standard or the intent of the standard so that two very different versions of the same standard for quality data extraction and reporting are in use. This scenario could potentially lead to future barriers to interoperable quality reporting and sharing of quality data. HIMSS supports collaboration between ONC, CMS, HL7, and other standards organizations in standards-related activities. HIMSS also strongly recommends that CMS test any substantive changes to the implementation guides to be validated through the HL7 validation process. HIMSS wants ONC and CMS to explore the optionality of being standardized in order to meet the industry's future needs for quality reporting and quality data exchange.

The future state will require standards for quality data collection and reporting which meet the reporting needs of the much larger healthcare ecosystem including private payers, accreditation bodies, and state-based value based purchasing and also facilitates real-time access to performance data on measures of clinical quality by clinicians. HIMSS encourages HHS to work collaboratively with standards organizations to develop a future state quality data capture and report standard that meets the data measurement of private payers, accreditation bodies, and state-based value based purchasing entities. This standard should also facilitate improved data visualization, which allows eligible hospitals and providers to review and parse data to identify gaps in care and take action to improve quality outcomes.

The Future State: Data Element Reporting

In the proposed regulation, ONC solicited comments on the future possibility of FHIR-enabled APIs replacing or complementing QRDA reports for quality reporting and improvement. HIMSS has actively endorsed ONC and CMS exploring new ways to leverage information and technology to improve quality of care and reduce provider burden.

Until the technology is able to consume all the data elements of a provider's workflow, not all providers will have the capability to report on their eCQMs. FHIR-enabled APIs have the potential to address this challenge. As with all methods of quality measurement policy, HIMSS strongly encourages CMS to not adopt FHIR-enabled APIs for quality reporting and improvement until:

- Data element collection and measure calculations are thoroughly tested, including field tests in a diverse array of care settings to ensure that the data generates comparable and consistent results against the measure's intent and the measures generated through the FHIR-enabled API accurately reflect the quality of care delivered.
- Data element collection should be interoperable with data visualization technology to drive meaningful improvements in care delivery before being incorporated into a value-based care delivery program.

Finally, HIMSS members have expressed significant concern about frameworks in which regulatory reporting entities can use FHIR-enabled APIs to directly collect all the data elements required for quality reporting across entire patient populations without the ability of providers to first analyze aggregate performance of specific measures and validate accuracy of results prior to final data submissions. Ensuring the accuracy of measure results generated from EHR data elements usually requires additional data processing time and review before CMS submission of performance-based payment adjustments and/or public reporting.

§ 170.315(c)(3) Clinical quality measures – report

Included in 2015 Edition Base EHR Definition? *No*

Clinical quality measures – report. Enable a user to electronically create a data file for transmission of clinical quality measurement data in accordance with the implementation specifications specified in § 170.205(h)(3) and (k)(3).

Preamble FR Citation: 84 FR 7446 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS generally supports the criteria targeted for revision in the 2015 Edition, however we question why 170.315(c)(10) – Clinical Quality Measures (CQMs) – report criterion references a standard developed by CMS as opposed to an SDO like HL7. HIMSS strongly encourages continuing to follow the established direction to name standards and specifications that are developed and maintained by an SDO.

HIMSS supports the update and addition of 170.315(b)(11) EHI export, in order to afford health IT developers the option of pursuing innovative export capabilities outside of requiring a specific export standard. However, we question whether the resulting export will result in data that will meet the expectations of those who are looking to use it. As FHIR based APIs mature and the USCDI expands, this effort will pay off over time, but those benefits may not appear early on.

HIMSS supports adopting the USCDI to establish a set of data classes and constituent data elements that would be required to be exchanged in support of interoperability nationwide as well as the concept of health IT developers being able to take advantage of additional flexibility under the Standards Version Advancement Process. The Standards Version Advancement Process would permit health IT developers to voluntarily implement and use a new version of an adopted standard, such as USCDI, as long as the newer version is approved by the National Coordinator through the Standards Version Advancement Process for use in certification.

HIMSS also encourages ONC to require implementation guides and specifications that reference FHIR Release 4 be recognized by established standards development and profiling organizations such as HL7 and Integrating the Healthcare Enterprise (IHE). Given the rapidly evolving nature of the FHIR specification and the various ongoing efforts in the industry to mature the specification, it is important to ensure that the industry adopts vetted implementation guides that have completed an established, collaborative and open process to ensure quality and a feedback loop between standards and profile developers and implementers.

In order to direct the industry to these implementation guides as they are updated and made available, certification requirements that reference such implementation guides may need to be published as future and ongoing guidance from ONC as opposed to being specifically named in the final regulations.

§ 170.315(b)(10) Electronic health information export

Included in 2015 Edition Base EHR Definition? *Yes*

Electronic health information export.

(i) Single patient electronic health information export.

(A) Enable a user to timely create an export file(s) with all of a single patient's electronic health information the health IT produces and electronically manages on that patient.

(B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(C) Limit the ability of users who can create such export file(s) in at least one of these two ways:

(1) To a specific set of identified users.

(2) As a system administrative function.

(D) The export file(s) created must be electronic and in a computable format.

(E) The export file(s) format, including its structure and syntax, must be included with the exported file(s).

(ii) Database export. Create an export of all the electronic health information the health IT produces and electronically manages.

(A) The export created must be electronic and in a computable format.

(B) The export's format, including its structure and syntax must be included with the export.

(iii) Documentation. The export format(s) used to support single patient electronic health information export as specified in paragraph (b)(10)(i) of this section and database export as specified in paragraph (b)(10)(ii) of this section must be made available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7446-49 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7568-70 for estimates related to this proposal.

Public Comment Field:

HIMSS has mixed support for the new proposed criteria. First off, it is important that the industry is aware that some of these certification 'testing' requirements are not tested, and that they are fulfilled by attestation. Similarly, for those criteria that are 'tested' and certified via vendor or developer attestation, there should be a mechanism to ensure that these functionalities are present in certified products when implemented. HIMSS suggests working with the industry to create an updated 'Buyer's guide" that incorporates some of the findings suggested in the National Academy of Medicine's Report to ensure purchasers and users know what functionality to demand from vendors. See Procuring Interoperability - Achieving High-Quality, Connected and Person-Centered Care.

> "…interoperability is also concurrently driven by vendor actions and demand from purchasers and users of the technologies. Healthcare lags behind specifically because "*leveraging procurement specifications remains an important yet underused approach to*

drive health care integration, quality, improvement, and cost containment."

With regards to 170.315(b)(11)/(13) and specifically the Consent2Share FHIR Consent Profile, HIMSS encourages ONC to ensure that any specification profile or implementation guide that is referenced as a certification requirement have sufficient uptake and adoption. In addition, ONC should confirm that it is published by an SDO to ensure that the industry implements specifications that are designed via an established process that incorporates industry feedback, transparency, and quality. Moreover, the specifications named should have a clear owner and maintenance process to allow for the specification to be updated in alignment and coordination with other ongoing industry efforts, and that there is a process to advance the specification from development, to implementation, with an ongoing feedback loop from implementers, testers, and users.

Moreover, as ONC requests comment on what image elements should be shared such as image quality, type, and narrative text, HIMSS recommends that the minimum data elements for Digital Imaging and Communications in Medicine (Dicom imaging) or non-Dicom images shared must be:

- Patient name
- Patient date of birth
- Patient Sex
- Acquiring facility
- Type of images (mode of acquisition CT, MR, VL, US, etc)
- Anatomy
- Laterality
- Study/procedure name or other labeling to identify the images contained within
- Number of images contained in imaging set
- Image file format type (. dcm, .jpeg, .img, etc)
- Any related contextual narrative, whether a formal report or encounter note
- For Dicom imaging, the full Dicom data set.
- For visible light, the photo and video should be made available in a format that is readable by a standard clinical viewer.
- For pathology, the above criterion will make it possible to access the study, but we believe that the field is still maturing to enable seamless digital transfer.

Further, we recommend that health IT developers attest to or publish as part of the exchange (export) format documentation the types of EHI they cannot support for export *and/or ingestion.* For background, the basic image exchange (export) scenarios are as follows:

1. Exchange of representative images such as thumbnails or key images**.**
    a. This solution might seem like a moderate answer by providing more information than an imaging report alone, yet not having the technical requirements of exchanging full imaging data sets. However, creation of such images is not a routine part of an image producer’s workflow and currently there are no reliable electronic methods for creating these images. Creation of such images would require a significant alteration in image producer’s workflow.
    b. Key images will only represent that information which is prospectively identified as valuable. Future needs may require reference to other portions of the imaging data

set not recognized as important at the time of creation of key images. For example, follow up or identification of small lung nodules.

   c. Key images do not enable a consumer or a specialist to communicate sufficient information to a sub-specialty provider or request a second opinion on high-acuity care.

2. Emergent transfer to a higher level of care. This scenario, is likely to be one of the most critical in terms of patient care and frequency of use in which images are to be exchanged. Here let us discuss Dicom imaging followed by visible light. Pathology imaging is not typically relevant in this uses case.
   a. Dicom imaging:
      i. Emergency Department physicians rely on diagnostic imaging for critical treatment decisions. While key images or thumbnails may be sufficient in the earliest phases of treatment planning, most ED physicians will then order advanced imaging. This can occur even if it has previously been performed and is otherwise not available. Today, the dominate mode of providing this information is to transfer a CD strapped to a patient's chest. These CDs are often not-readable by the receiving institution. Typical scenarios are trauma cases which require CTs or complaints of other internal ailments, which require Dicom-based imaging.
      ii. Further, subspecialists desire to have the full imaging dataset prior to definitive therapy, especially if that treatment should require surgery or other highly invasive procedures. If that proactive treatment planning is to occur, the full set of images will be required to serve as a base for follow up in many cases of critical illness or injury.
   b. Non-Dicom imaging:
      i. We recommend that visible light and HD movies acquired in the context of emergency care be transferred in their full format, so they are visible by the receiving trauma center.

3. Second opinion transfer. Consumers and their providers increasingly seek advanced sub-specialty care outside of their home healthcare network. Full Dicom imaging data sets are critical to this effort. In addition, visible light will be required for dermatology-related conditions. We also recommend that we set goals for the gradual ability to transfer pathology studies, as this field matures.
   a. Dicom imaging:
      i. Today, commonly this clinical content data is transferred via CDs.
      ii. It should be easy for consumers and/or their providers to transfer a full Dicom or non-Dicom imaging set to another health care facility or sub-specialist.
      iii. Consumers should have full access to these electronic files so that they can easily transfer this information.
   b. Non-Dicom imaging:
      i. Consumers should have full access to any visible light images recorded in their care.
   c. Pathology imaging:

        i. As digital pathology matures, we recommend that transfer protocols be established to enable transfer and viewing of files across vendors.

4. Routine transfer of noncritical care. Such change of care will occur when patients move between health systems either within or between geographic regions.
    a. In this scenario, no exchange of images may be indicated.
    b. An awareness of images acquired at an external institution will be communicated through the sharing of imaging reports.
    c. If imaging data sets are not to be exchanged in these noncritical scenarios then mechanisms must be in place for ready transfer of images should they be required. The timeliness of this transfer should not delay the delivery of care.

It is important to note, in all of the above scenarios, the transference of imaging data sets alone *should not* be considered a sufficient condition. There are additional steps that the receiving entity should consider upon receipt of images, including: a proper patient matching exercise should be performed; the images are linked to the appropriate patient's medical record; and, the recipient of the images should manage the images in such a way that they are readily accepted in a standard workflow and readily identifiable and available within the EHR. An example of such a solution would be to have those images appropriately labeled and integrated into the same archive as the internally-generated images.

Along with the recognition of the need for providers to have immediate access to images generated outside of their institution, is a recognition of the significant challenges surrounding movement and storage of such large data sets. We recommend continued encouragement of new technologies that enable rapid access to externally generated images without requiring actual movement of the data (federation).

Section VI – Health IT for the Care Continuum

Approach to Health IT for the Care Continuum and the Health Care of Children

Section 4001(b)(i) of the Cures Act instructs the National Coordinator to encourage, keep, or recognize, through existing authorities, the voluntary certification of health IT under the Program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. This provision of the Cures Act closely aligns with ONC's ongoing collaborative efforts with both federal partners and stakeholders within the health care and health IT community to encourage and support the advancement of health IT for a wide range of clinical settings. Section VI of this proposed rule outlines our approach to implement Section 4001(b) of the Cures Act, which requires that the Secretary make recommendations for the voluntary certification of health IT for use by pediatric health providers and to adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children. To be clear, and consistent with past practice, we do not recommend or propose a "pediatric-specific track or program" under the ONC Health IT Certification Program. This proposed rule outlines the certification criteria adopted in the 2015 Edition which we believe support the certification of health IT for pediatric care.

Preamble FR Citation: 84 FR 7457-61 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Given that the care of children can differ significantly from that of adults, the tools used by clinicians should account for that variation. HIMSS appreciates the proposed regulation's focus to prioritize patient safety as well as usability in the implementation of new criteria for EHRs. We generally support the 10 clinical priorities identified by ONC for pediatric care, but recommend that the agency take additional steps to improve patient safety and system usability. These steps include the following:

- Map additional existing EHR certification requirements to pediatrics

ONC should further extend the approach taken in this regulation to map the agency's existing EHR certification requirements to pediatric care. For example, ONC currently requires that EHR developers test their systems using predefined scenarios that mimic real-world situations. ONC should clarify that demonstrating adherence to the 10 clinical priorities should involve pediatric-focused scenarios. Similarly, ONC currently requires that EHR developers test their systems with end-users, such as doctors and nurses. ONC should clarify that EHR developers should involve end-user clinicians who care for children—such as pediatricians and pediatric nurses—in the testing of the identified clinical priorities in pediatric care.

- Provide additional pediatric-focused resources

ONC should ensure that the appropriate resources are available to support meeting pediatric-focused criteria. For example, ONC should develop specific and detailed guidance for each proposed pediatric clinical priority. In addition, ONC should involve pediatric usability experts in the development of implementation guides and test procedures for the pediatric clinical priorities.

These recommendations will assist in improving the usability of EHRs used in pediatric care to reduce clinician burden as well as prevent medical errors.

Request for Information on Health IT and Opioid Use Disorder Prevention and Treatment

We seek comment in this proposed rule on a series of questions related to health IT functionalities and standards to support the effective prevention and treatment of opioid use disorder (OUD) across patient populations and care settings. Specifically, we request public comment on how our existing Program requirements (including the 2015 Edition certification criteria) and the proposals in this rulemaking may support use cases related to OUD prevention and treatment and if there are additional areas that ONC should consider for effective implementation of health IT to help address OUD prevention and treatment. This section also includes request for comment on furthering adoption and use of electronic prescribing of controlled substances standard and neonatal abstinence syndrome.

Preamble FR Citation: 84 FR 7461-65 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

We believe health IT offers promising strategies to help clinicians and sites of service combat Opioid Use Disorder (OUD). Health IT can make a significant contribution to improving adherence to opioid prescribing guidelines as well as physician adherence to treatment protocols, increasing the safety of prescribing for controlled substances, enhancing clinician access to PDMPs, and expanding access to addiction treatment and recovery support services. Moreover, health IT helps to improve access to data from disparate sources and ensures that key data is consistently available to the right person, at the right place, and at the right time across the care continuum. A key building block to improving access to data is through greater use of technical standards for exchanging health information.

HIMSS has previously expressed its support for efforts to improve interoperability between EHRs and state prescription drug monitoring programs (PDMPs) as well as increase adoption of electronic prescribing of controlled substances (EPCS). A growing number of states have been enacting laws that mandate EPCS use—the further broadening of EPCS adoption would help prevent additional diversion of opioids, improve patient safety, and strengthen prescribing processes toward alleviating burden. In addition, further integrating PDMP data into EHRs would help minimize clinician burden by improving workflow and eliminating the necessity of clicking between two disparate IT systems. States have the ability to leverage enhanced federal funding to build a PDMP or enhance PDMP functionality and HIMSS encourages ONC to ensure that states understand the opportunities to improve patient safety as well as address the opioid crisis.

Tools such as PDMPs are mechanisms that identify patients at risk for harm and help coordinate patient care as well as improve outcomes. Overall, we support the interoperability of PDMPs that are integrated into EHRs and dispensing systems and encourage ONC to help facilitate the sharing of best practices around user-centered design on this topic. HIMSS endeavors an environment where clinicians, including pharmacists, encounter common interface and workflow design elements when transitioning between different care settings as well as EHR technologies. HIMSS also recommends that ONC work with CMS to continue to utilize Medicare and Medicaid payment policy to address our nation's opioid crisis. HIMSS has been very supportive of the inclusion of opioid-related measures in the e-Prescribing Objective of the Promoting Interoperability Programs. We appreciated the intent of the measures in place for 2019, but recommended that CMS consider utilizing opioid measures that have a stronger focus on outcomes. The query of a PDMP would measure how often an EH or CAH queries a PDMP before prescribing a Schedule II opioid.

While this may be beneficial for identifying patients who could be at risk for opioid misuse, outcomes-based measures would help drive treatment decisions and improve patient safety. For example, HIMSS members have discussed the increasing evidence that correlates inpatient administration of opiates with subsequent dependence and overdose. Structuring a measure where the denominator is the total number of hospital encounters during a reporting period and the numerator is total Morphine Equivalent Doses (MEQ) prescribed would be much closer to an outcomes-based measure.

Ultimately, we want to support efforts to have PDMP information fully integrated or embedded in EHRs to allow for optimal provider workflows and reduced clinician burden. Over the long term, HIMSS pledges to work with HHS and other stakeholder organizations to find the appropriate clinically-focused outcomes measures for use as soon as possible beyond 2019.

In addition, through the HIMSS Nicholas E. Davies Award of Excellence, we have identified several opioid-related case studies focused on getting quality data into the hands of clinicians and making the data actionable to promote rapid cycle, clinician-driven quality care improvement projects.

For example, Ochsner Health System incorporated the use of analytics to showcase prescribing data of opioids. There work identified the importance of making the data identifiable as a critical component of success. Ochsner Health started their opioid stewardship program by creating a reporting process where their informatics team looked at the number of prescriptions being prescribed for opioids in emergency rooms.

After several months, Ochsner Health unblinded the data on the emergency department performance dashboards to show each individual provider compared to other providers for the number of prescriptions per day. Ochsner combined the dashboard with appropriate use guidance hard coded into the emergency department workflow, making it easy for a clinician to follow model practices.

Ochsner then spread the dashboard throughout the system and saw a 40 percent reduction in opioid scripts in the first year following the unblinding of the data. To date, 26,000 fewer Ochsner patients have been prescribed opioids. The averaging dosing strength of scripts that did meet appropriate use guidance also decreased significantly. This is a compelling example of how visualization of data changed practice.

Section VII – Conditions and Maintenance of Certification

Note: Because this template presents comment tables in the order in which their subject proposed provisions are discussed in the preamble of the proposed rule, this section includes tables for certain new and revised provisions in 45 CFR subparts A, B, C, and E, in complement to the proposed new subpart D.

§ 170.401 Information blocking Condition and Maintenance of Certification Requirement
(a) Condition of Certification. A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103. (b) Maintenance of Certification. [Reserved]
Preamble FR Citation: 84 FR 7465 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Not applicable
Public Comment Field: HIMSS supports ONC establishing a Condition and Maintenance of Certification requirement that a health IT developer will not take any action that constitutes information blocking.

§ 170.402 Assurances

(a) Condition of Certification.

(1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, 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 must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.

(3) A health IT developer must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification.

(4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10).

(b) Maintenance of Certification.

(1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:

(i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or

(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.

(2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within 24 months of this 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.

Preamble FR Citation: 84 FR 7465-66 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7577-78 for estimates related to this proposal.

Public Comment Field:

Health IT developers must provide functionality within 24 months of 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. HIMSS encourages ONC to examine the potential ramifications of these aggressive timelines to ensure that burdens to implementers and providers are minimized. If possible, HIMSS suggests approaching complex new requirements in a phased fashion to incrementally require advanced features or additional data sets over set periods of time.

Trusted Exchange Framework and the Common Agreement – Request for Information

We request comment as to whether certain health IT developers should be required to participate in the Trusted Exchange Framework and Common Agreement (TEFCA) as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. We also welcome comment on the certification criteria we have identified as the basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, other certification criteria that would serve as a basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, and whether the current structure of the Trusted Exchange Framework and Common Agreement are conducive to health IT developer participation and in what manner.

Preamble FR Citation: 84 FR 7466-67 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports the work undertaken by ONC to develop the Trusted Exchange Framework and Common Agreement (TEFCA). We are still completing a full analysis of TEFCA Draft 2, and will be submitting public comments on that guidance document in the next several weeks. The underlying concept and goals of TEFCA are forward-looking: to provide a single on-ramp to nationwide connectivity and enable EHI to securely follow the patient when and where it is needed.

However, without a final TEFCA, it is difficult to say if health IT developers should be required to participate in TEFCA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI.

As we described in our public comments on TEFCA Draft 1, HIMSS wants to capitalize on the significant momentum being built across the community to support broader nationwide exchange and maintain the current upward trajectory of nationwide interoperability efforts.

Thus far, TEFCA has been voluntary guidance for the community to consider implementing. It is likely that many health IT developers will be interested in participating in TEFCA, as qualified health information networks, participants, and participant members. However, until a final guidance document is released with the full parameters described for the program, it is difficult to consider whether any entity should be required to participate in the Framework.

§ 170.403 Communications

(a) Condition of Certification.

(1) A health IT developer may not prohibit or restrict the communication regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology.

(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.

(i) Unqualified protection for certain communications. A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—

§ 170.403 Communications

(A) Making a disclosure required by law;

(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;

(C) Communicating information about cybersecurity threats and incidents to government agencies;

(D) Communicating information about information blocking and other unlawful practices to government agencies; or

(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB.

(ii) Permitted prohibitions and restrictions. For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.

(A) Developer employees and contractors. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

(B) Non-user-facing aspects of health IT. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

(C) Intellectual property. A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's health IT (including third-party rights), provided that—

(1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and

(2) A health IT developer does not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section.

(D) Screenshots. A health IT developer may require persons who communicate screenshots to—

(1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(3) or to conceal protected health information;

(2) Not infringe the intellectual property rights of any third parties, provided that—

(i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;

(ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work;

(iii) The developer has put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and

(iv) Communicators are permitted to communicate screenshots that have been redacted to not disclose third-party content; and

§ 170.403 Communications

(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.

(E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.

(b) Maintenance of Certification.

(1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:

(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(2) Contracts and agreements.

(i) A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.

Preamble FR Citation: 84 FR 7467-76 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7578 for estimates related to this proposal.

Public Comment Field:

ONC's proposed regulation states that a health IT developer can prohibit or restrict communications that would infringe the intellectual property (IP) rights existing in the developer's health IT (including third-party rights), if a developer does not prohibit the communication of screenshots of the health IT developer's health IT, subject to limited restrictions. Some of these restrictions include not altering screenshots, except to annotate, resize, or redact.

The proposed regulation also allows developers to put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because the reproduction would infringe the third-party's IP rights. However, specific HIT products may feature proprietary protocols and/or algorithms that are embedded in user interfaces, where nearly all of a specific user interfaces are considered IP. Developers do not want this IP broadly published or shared, but it would be extremely difficult to "put all potential communicators on sufficient written notice of those parts of the screen display that contain trade secrets or Intellectual Property Restrictions (IPRs)and cannot be communicated," without preventing a communication about the entire user interface.

It is also important to note the possibility exists of "bad actors" receiving screen shots and then using that information to develop malware or other harmful IT that could be incorporated into the healthcare ecosystem. We see the permitted user sharing of screens to be opening up a situation where developers could be forced to monitor all user forums as much as possible to prevent IP from being stolen, and/or malware from being introduced.

VII.B.4 Application Programming Interfaces

Key Terms Relevant to §170.404 API Conditions (Proposed for Adoption at § 170.102)

* * * * *

API Data Provider refers to the organization that deploys the API technology created by the "API Technology Supplier" and provides access via the API technology to data it produces and electronically manages. In some cases, the API Data Provider may contract with the API Technology Supplier to perform the API deployment service on its behalf. However, in such circumstances, the API Data Provider retains control of what and how information is disclosed and so for the purposes of this definition is considered to be the entity that deploys the API technology.

API Technology Supplier refers to a health IT developer that creates the API technology that is presented for testing and certification to any of the certification criteria adopted or proposed for adoption at § 170.315(g)(7) through (g)(11).

API User refers to persons and entities that use or create software applications that interact with the APIs developed by the "API Technology Supplier" and deployed by the "API Data Provider." An API User includes, but is not limited to, third-party software developers, developers of software applications used by API Data Providers, and patients and health care providers that use apps that connect to API technology on their behalf.

* * * * *

Preamble FR Citation: 84 FR 7477 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS encourages ONC to divide the definition of "API User" into two separate categories: "Software Developers" and "End Users." There should be a standardized process established to evaluate software developers that use APIs and verify that they meet certain minimum criteria, including protection of data in transit, at rest, and at death (when the data is no longer being used).

§ 170.215(a)(2) API Resource Collection in Health

Implementation specifications. API Resource Collection in Health (ARCH) Version 1.

Preamble FR Citation: 84 FR 7479-80 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to our proposals regarding APIs.

Public Comment Field:
HIMSS supports ONC’s establishment of the API Resource Collection in Health (ARCH) to align the proposed USCDI standard. HIMSS requests that ONC recognize the important role of standards and profiling organizations, and ensure that the ARCH and USCDI include data classes and data elements that have SDO-developed implementation guides and integration profiles.

§ 170.315(g)(10) Standardized API for patient and population services (Certification Criterion)

Included in 2015 Edition Base EHR Definition? *Yes*

Standardized API for patient and population services. The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) Data response. Respond to requests for data (based on an ID or other token) for each of the resources referenced by the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a)(2) and (3).

(ii) Search support. Respond to search requests for data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) App registration. Enable an application to register with the technology's "authorization server."

(iv) Secure connection. Establish a secure and trusted connection with an application that requests data in accordance with the standard adopted in § 170.215(a)(5).

(v) Authentication and app authorization – 1st time connection. The first time an application connects to request data the technology:

(A) Authentication. Demonstrates that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the standard adopted in § 170.215(b).

(B) App authorization. Demonstrates that a user can authorize applications to access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) and issue a refresh token that is valid for a period of at least 3 months.

(vi) Authentication and app authorization – Subsequent connections. Demonstrates that an application can access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months.

(vii) Documentation.

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

(B) The documentation used to meet paragraph (g)(10)(vii)(A) of this section must be available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7481-84 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to our proposals regarding APIs.

§ 170.315(g)(10) Standardized API for patient and population services (Certification Criterion)

Public Comment Field:

HIMSS supports the updated criterion for Standardized API for patient and population services, and the use of HL7 FHIR standards and the additional named implementation specifications. HIMSS recognizes and supports the importance of ONC's approach to promoting open APIs and the directional signal that ONC is sending the community by specifying HL7 FHIR. HIMSS strongly encourages the selection of FHIR Release 4, the latest balloted and normative version of FHIR, over any previous versions. HIMSS also supports ONC's establishment of the API Resource Collection in Health (ARCH) to align the proposed USCDI. HIMSS requests that ONC recognize the important role of standards and profiling organizations, and ensure that the ARCH and USCDI include data classes and data elements that have SDO-developed implementation guides and integration profiles.

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

The following Condition of Certification applies to developers of Health IT Modules certified to any of the certification criteria adopted in § 170.315(g)(7) through (11).

(a) Condition of Certification.

(1) General. An API Technology Supplier must publish APIs and must 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, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) Transparency conditions.

(i) General. The business and technical documentation published by an API Technology Supplier must be complete. All documentation published pursuant to paragraph (a)(2)(ii) of this section must be published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(ii) Terms and conditions.

(A) Material information. The API Technology Supplier must publish all terms and conditions for its API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

(1) Develop software applications to interact with the API technology;

(2) Distribute, deploy, and enable the use of software applications in production environments that use the API technology;

(3) Use software applications, including to access, exchange, and use electronic health information by means of the API technology;

(4) Use any electronic health information obtained by means of the API technology; and

(5) Register software applications.

(B) API fees. Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(1) The persons or classes of persons to whom the fee applies;

(2) The circumstances in which the fee applies; and

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

(3) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

(C) Application developer verification. An API Technology Supplier is 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.

(3) Permitted fees conditions.

(i) General conditions.

(A) All fees related to API technology not otherwise permitted by this section are prohibited from being imposed by an API Technology Supplier.

(B) For all permitted fees, an API Technology Supplier must:

(1) Ensure that fees are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(2) Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting API technology to, or at the request of, the API Data Provider to whom the fee is charged.

(3) Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers to whom the API technology is supplied, or for whom the API technology is supported.

(4) Ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

(ii) Permitted fee – Development, deployment, and upgrades. An API Technology Supplier is 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.

(iii) Permitted fee – Supporting API uses for purposes other than patient access. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider. This permitted fee does not include:

(A) 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;

(B) Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or

(C) Opportunity costs, except for the reasonable forward-looking cost of capital.

(iv) Permitted fee – Value-added services. An API Technology Supplier is 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.

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

(v) Record-keeping requirements. An API Technology Supplier must keep for inspection detailed records of any fees charged with respect to the API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(4) Openness and pro-competitive conditions. General condition. An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

(i) Non-discrimination.

(A) An API Technology Suppler must 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.

(B) The terms on which an API Technology Supplier provides API technology must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(C) An API Technology Supplier must not offer different terms or service on the basis of:

(1) Whether the API User with whom an API Data Provider has a relationship is a competitor, potential competitor, or will be using electronic health information obtained via the API technology in a way that facilitates competition with the API Technology Supplier.

(2) 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.

(ii) Rights to access and use API technology.

(A) An API Technology Supplier must have and, upon request, must grant 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, including:

(1) For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier’s health information technology or with health information technology under the API Technology Supplier’s control;

(2) 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

(3) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(B) An API Technology Supplier must not condition any of the rights described in paragraph (a)(4)(ii)(A) of this section on the requirement that the recipient of the rights do, or agree to do, any of the following:

(1) Pay a fee to license such rights, including but not limited to a license fee, royalty, or revenue-sharing arrangement.

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

(2) Not compete with the API Technology Supplier in any product, service, or market.

(3) Deal exclusively with the API Technology Supplier in any product, service, or market.

(4) Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.

(5) License, grant, assign, or transfer any intellectual property to the API Technology Supplier.

(6) Meet additional developer or product certification requirements.

(7) Provide the API Technology Supplier or its technology with reciprocal access to application data.

(iii) Service and support obligations. An API Technology Supplier must 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.

(A) Changes and updates to API technology. An API Technology Supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.

(B) 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 thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API 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.

(b) Maintenance of Certification.

(1) Registration for production use. An API Technology Supplier with health IT certified to the certification criterion adopted in § 170.315(g)(10) must register and enable all applications for production use within 1 business day of completing its verification of an application developer's authenticity, pursuant to paragraph (a)(2)(ii)(C) of this section.

(2) Service Base URL publication. API Technology Supplier must support the publication of Service Base URLs for all of 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.

(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) must provide all API Data Providers with such API technology deployed with API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of this final rule's effective date.

Preamble FR Citation: 84 FR 7485-95 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to this proposal.

Public Comment Field:

HIMSS supports the idea from the 21st Century Cures Act that health IT developers publish APIs and allow health information from such technology "to be accessed, exchanged, and used without special effort." This phrase of "without special effort" requires that APIs, and the health care ecosystem in which they are deployed, have three attributes: standardized, transparent, and procompetitive.

The questions in this proposed regulation center around whether the permitted fees tied to APIs include effective guardrails to ensure that fees do not prevent EHI from being accessed, exchanged, and used through the use of APIs without special effort. Overall, HIMSS supports the creation of the API Technology Suppliers' Development, Deployment, and Upgrade Fees as well as Value-Added Services Fees. We appreciate the proposed regulation's prohibition on any fees, except those expressly permitted, and support the idea that Technology Suppliers should not engage in pricing practices that create barriers to entry and competition for apps that health care providers seek to use.

However, we note that the complexities created in this proposed fee structure may lead to less innovation, more administrative burden, and a focus on cost recovery rather than creation of novel ways to improve data access.

As ONC evaluates comments on the proposed regulation, HIMSS encourages the agency to look for approaches that address these complexities and seeks to minimize them to ensure that health system stakeholders have the opportunity to continue to innovate and integrate the use of newer technologies into their solutions. HIMSS also seeks to ensure that a complaint process to any fees be instituted that is clearly articulated and well-publicized, especially if fees are used in a way that is perceived to restrict access. Examples include published and widely disseminated pricing structures so that end users can plan and budget appropriately.

The proposed regulation discusses how permitted fees are intended to recognize that suppliers need to recover costs and earn a reasonable return for providing certified API technology.   HIMSS appreciates ONC's emphasis on the fact that fees could not be used 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.

From the proposed regulation, HIMSS recommends changes to the parameters around API Usage-Based Fees. We support the use of these fees, but ask that volume thresholds be included in any contractual language related to these fees, to ensure that any incremental costs attributable to supporting API interactions at increasing volumes and scale are addressed appropriately. If a technology supplier is receiving fees to develop, deploy, and upgrade API technology, it is unlikely that they would also need to charge for usage of the APIs, as long as their usage remains under a pre-determined volume threshold. Without these specified thresholds, a new barrier to innovation and startups as well as registries may be established. Usage fees could potentially block data and negatively affect patient safety.

HIMSS also encourages ONC to divide the definition of "API User" into two separate categories: "Software Developers" and "End Users." There should be a standardized process established to evaluate software developers that use APIs and verify that they meet certain minimum criteria, including protection of data in transit, at rest, and at death (when the data is no longer being used). Additional criteria should include proper identity management, including identity proofing; authorization, authentication, and authorization; and, ensuring software developers do not act in a way that could inhibit patient control of their data (such as storing user passwords). This certification process should look similar to the health IT certification process, but with far fewer steps, and might possibly be automated. This process would also help to protect patients, but it would also protect API Data Providers from claims of being irresponsible with patient data.

A centralized and standardized assessment process would ensure that each entity would not have to run their own assessment process. Using such a standard process would be less expensive and more consistent as well as provide better legal protection because the healthcare entity would not have to take the legal risk itself, as the certifying entity would be responsible.

In addition, HIMSS endorses the read-only access to data for APIs in the proposed regulation for the present state. We encourage the community to move toward a position where APIs have the ability for write access for patients and their authorized family members. ONC should work across the entire community to develop a process and a timeline on implementing write access and integrating this information into EHRs. We suggest a pilot phase, but recommend a somewhat condensed 2-3 year period until full implementation.

VII.B.5 Real World Testing

§ 170.405 Real world testing

(a) Condition of Certification. A health IT developer with Health IT Modules to be certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (11), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b) Maintenance of Certification.

(1) Real world testing plan submission. A health IT developer must submit an annual real world testing plan to its ONC-ACB via a publicly accessible hyperlink no later than December 15 of each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section.

(i) The plan must be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information.

(ii) The plan must include all health IT certified to the 2015 Edition through August 31st of the preceding year.

(ii) The plan must address the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

(A) The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability and conformance to the certification criteria's requirements, including scenario- and use case-focused testing;

(B) The care setting(s) that will be tested for real world interoperability and an explanation for the health IT developer's choice of care setting(s) to test;

(C) 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.

(D) A schedule of key real world testing milestones;

(E) A description of the expected outcomes of real world testing;

(F) At least one measurement/metric associated with the real world testing; and

(G) A justification for the health IT developer's real world testing approach.

(2) Real world testing results reporting. A health IT developer must submit real world testing results to its ONC-ACB via a publicly accessible hyperlink no later than January 31 each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section. The real world testing results must report the following for each of the certification criteria identified in paragraph (a)of this section that are included in the Health IT Module's scope of certification:

(i) The method(s) that was used to demonstrate real world interoperability;

(ii) The care setting(s) that was tested for real world interoperability;

(iii) The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

§ 170.405 Real world testing

(iv) A list of the key milestones met during real world testing;

(v) The outcomes of real world testing including a description of any challenges encountered during real world testing; and

(vi) At least one measurement/metric associated with the real world testing.

(3) USCDI Updates for C-CDA. A health IT developer with health IT certified to § 170.315(b)(1), (e)(1), (g)(6), (f)(5), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(3)(i) of this section within 24 months of the effective date of this final rule.

(4) C-CDA Companion Guide Updates. A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (b)(9), (e)(1), (g)(6), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(4)(i) of this section within 24 months of the effective date of this final rule.

(5) Voluntary standards and implementation specifications updates. A health IT developer subject to paragraph (a) of this section that voluntary updates its certified health IT to a new version of an adopted standard that is approved by the National Coordinator through the Standards Version Advancement Process must:

(i) Provide advance notice to all affected customers and its ONC-ACB –

(A) Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator;

(B) The developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world;

(C) Whether the developer intends to continue to support the certificate for the existing certified Health IT Module version for some period of time and how long or if the existing certified Health IT Module version will be deprecated; and

(ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in applicable 2015 Edition certification criterion specified in paragraph (a) of this section.

Preamble FR Citation: 84 FR 7495-97 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7578-82 for estimates related to this proposal.

Public Comment Field:

HIMSS strongly supports the concept of real world testing, and the Standards Version Advancement Process. Tools to test conformance in healthcare settings are often a limiting factor, and HIMSS recognizes ONC's vision to advance standards in the absence of robust conformance testing tools, however HIMSS encourages ONC to invest along with the private sector to help develop more advanced conformance test tools and require conformance testing once tools become available.

On October 6, 2017, the HIMSS North America Board of Directors approved the Interoperability Call to Action. This document was originally developed and championed by the HIMSS Interoperability and HIE Committee, which focuses on the advancement of semantic interoperability and standards based health information systems that lead to meaningful health information exchange. As the health information exchange landscape continues to evolve, interoperability is a key driver towards achieving secure, lower cost and higher quality patient care when and where it is needed. Real world testing that focuses on standards based, interoperable health IT aligns with the goals of the HIMSS Interoperability Call to Action.

HIMSS applauds ONC's focus on enhancing the state of testing health information technologies and examining the testing continuum, especially with regards to how systems and products function once implemented. HIMSS has long championed many of the industry's various interoperability initiatives such as IHE USA, the Personal Connected Health Alliance, and also supports increasingly robust testing of health IT to ensure that the technology functions as intended in venues like the North American Connectathon and programs like the Immunization Interoperability Program.

Real world testing of health information technology addresses a component that is missing in the current health IT testing continuum. The regulatory environment and the current state of the health IT landscape signal the need for having a ready mechanism to robustly test health IT *in situ* in order to assess its efficacy in real-world environments and to further advance rapid progress in technology development and interoperability. To date, there has not been a network of organizations developed and aligned with the scope, authority, resources, and makeup to carry out such an initiative. HIMSS feels this is a helpful first step to developing more robust capabilities allow for real world testing at scale.

VII.D Enforcement

§ 170.580 ONC review of certified health IT or a health IT developer’s actions

(a) * * *

(1) Purpose. ONC may directly review certified health IT or a health IT developer’s actions or practices to determine whether either conform to the requirements of the ONC Health IT Certification Program.

(2) * * *

(i) Certified health IT causing or contributing to unsafe conditions. * * *

* * * * *

(ii) Impediments to ONC-ACB oversight of certified health IT. * * *

* * * * *

(iii) Noncompliance with Conditions and Maintenance of Certification. ONC may initiate direct review under this section if it has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement under subpart D of this part.

(3) * * *

(i) ONC's review of certified health IT or a health IT developer’s actions or practices is independent of, and may be in addition to, any surveillance of certified health IT conducted by an ONC-ACB.

(4) Coordination with the Office of Inspector General.

(i) ONC may coordinate its review of a claim of information blocking with the Office of Inspector General or defer to the Office of Inspector General to lead a review of a claim of information blocking.

(ii) ONC may rely on Office of Inspector General findings to form the basis of a direct review action.

* * * * *

(iv) An ONC-ACB and ONC-ATL shall provide ONC with any available information that ONC deems relevant to its review of certified health IT or a health IT developer’s actions or practices.

(v) ONC may end all or any part of its review of certified health IT or a health IT developer’s actions or practices under this section at any time and refer the applicable part of the review to the relevant ONC-ACB(s) if ONC determines that doing so would serve the effective administration or oversight of the ONC Health IT Certification Program.

(b) * * *

(1) * * *

§ 170.580 ONC review of certified health IT or a health IT developer’s actions

(i) Circumstances that may trigger notice of potential non-conformity. At any time during its review of certified health IT or a health IT developer’s actions or practices under paragraph (a) of this section, ONC may send a notice of potential non-conformity if it has a reasonable belief that certified health IT or a health IT developer may not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(iii) * * *

(D) Issue a notice of proposed termination if the health IT is under review in accordance with paragraphs (a)(2)(i) or (ii) of this section.

(2) * * *

(i) Circumstances that may trigger notice non-conformity. At any time during its review of certified health IT or a health IT developer’s actions or practices under paragraph (a) of this section, ONC may send a notice of non-conformity to the health IT developer if it determines that certified health IT or a health IT developer’s actions or practices does not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(3) * * *

(i) All records related to the development, testing, certification, implementation, maintenance and use of its certified health IT;

(ii) Any complaint records related to the certified health IT;

(iii) All records related to the Condition(s) and Maintenance of Certification requirements, including marketing and distribution records, communications, and contracts; and

(iv) Any other relevant information.

(c) * * *

(1) Applicability. If ONC determines that certified health IT or a health IT developer’s action or practice does not conform to requirements of the ONC Health IT Certification Program, ONC shall notify the health IT developer of its determination and require the health IT developer to submit a proposed corrective action plan.

* * * * *

(e) * * *

(1) Applicability. Excluding situations of noncompliance with a Condition or Maintenance of Certification requirement under subpart D of this part, ONC may propose to terminate a certification issued to a Health IT Module if:

* * * * *

(f) * * *

(1) Applicability. The National Coordinator may terminate a certification if:

(i) A determination is made that termination is appropriate after considering the information provided

§ 170.580 ONC review of certified health IT or a health IT developer’s actions

by the health IT developer in response to the proposed termination notice;

(ii) The health IT developer does not respond in writing to a proposed termination notice within the timeframe specified in paragraph (e)(3) of this section; or

(iii) A determination is made that the health IT developer is noncompliant with a Condition or Maintenance of Certification requirement under subpart D of this part or for the following circumstances when ONC exercises direct review under paragraph (a)(2)(iii) of this section:

(A) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

(1) Fact-finding;

(2) A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(3) of this section; or

(3) A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(3) of this section.

(B) The information or access provided by the health IT developer in response to any ONC communication, including, but not limited to: fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete;

(C) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(D) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(E) The health IT developer fails to timely submit a corrective action plan that adequately addresses the elements required by ONC as described in paragraph (c) of this section;

(F) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(G) ONC concludes that the non-conformity(ies) cannot be cured.

* * * * *

(g) * * *

(1) Basis for appeal. A health IT developer may appeal an ONC determination to suspend or terminate a certification issued to a Health IT Module and/or an ONC determination to issue a certification ban under § 170.581(a)(2) if the health IT developer asserts:

(i) ONC incorrectly applied ONC Health IT Certification Program requirements for a

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2); or

* * * * *

(2) Method and place for filing an appeal. A statement of intent to appeal followed by a request for appeal must be submitted to ONC in writing by an authorized representative of the health IT developer subject to the determination being appealed. The statement of intent to appeal and request for appeal must be filed in accordance with the requirements specified in the notice of:

§ 170.580 ONC review of certified health IT or a health IT developer’s actions

(i) Termination;

(ii) Suspension; or

(iii) Certification ban under § 170.581(a)(2).

(3) * * *

(i) A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

* * * * *

(4) Effect of appeal.

(i) A request for appeal stays the termination of a certification issued to a Health IT Module, but the Health IT Module is prohibited from being marketed, licensed, or sold as “certified” during the stay.

(ii) A request for appeal does not stay the suspension of a Health IT Module.

(iii) A request for appeal stays a certification ban issued under § 170.581(a)(2).

(5) * * *

(i) The hearing officer may not review an appeal in which he or she participated in the initial suspension, termination, or certification ban determination or has a conflict of interest in the pending matter.

* * * * *

(6) * * *

(v) ONC will have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf that clarifies, as necessary, its determination to suspend or terminate the certification or issue a certification ban.

* * * * *

Preamble FR Citation: 84 FR 7503-07 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7583-84 for estimates related to this proposal.

Public Comment Field:

Given that 21st Century Cures affirms ONC’s role in using certification to improve health IT’s capabilities for the access, use, and exchange of electronic health information, HIMSS supports the expanded certification authority for ONC to establish Conditions and Maintenance of Certification requirements for health IT developers that go beyond the certified health IT itself. This additional focus is placed on the actions and business practices of health IT developers as well as technical interoperability.

We endorse the general enforcement approach outlined in the proposed regulation that calls for 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, including the requirement for a health IT developer to attest to meeting the Conditions and Maintenance of Certification.

Section VIII – Information Blocking

§ 171.100 Statutory basis and purpose

(a) Basis. This part implements section 3022 of the Public Health Service Act, 42 U.S.C. 300jj-52.

(b) Purpose. The purpose of this part is to establish exceptions for reasonable and necessary activities that do not constitute "information blocking," as defined by section 3022(a)(1) of the Public Health Service Act, 42 U.S.C. 300jj-52.

Preamble FR Citation: 84 FR 7508 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports, at a high level, the Information Blocking Exceptions in the proposed regulation, as they identify the appropriate categories that will help inform the community as well as define sharing boundaries and expectations that will lead to greater information exchange. In addition, we support advancing the aims of this regulation that focus on promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI, protecting patient safety, and promoting competition and innovation in health IT and its use to provide health care services to consumers.

ONC's attempts to level the playing field for data exchange are also positive. Themes from the Information Blocking Exceptions all bolster ONC's approach: implemented in a consistent and non-discriminatory manner; reasonably related and uniformly applied; and, based on objective and verifiable criteria.

Although we support the exception categories identified, under each of the identified exceptions, we recommend specific refinements and clarifications for inclusion in the regulatory text. Each of the exceptions needs to have clearer definitions and requirements with more examples of what a valid exception in each of the seven categories would look like. If there is ambiguous regulatory text on what is and what is not information blocking, as well as the circumstances when a designated actor could make an information blocking claim, it will be exceedingly difficult for a developer, provider, or a network/exchange to do its part to support the free flow of information across the healthcare ecosystem.

The inclusion of terms such as "reasonable" and "as soon as possible" and not properly defining these terms will only make applicability and enforcement of the exceptions more challenging. The addition of many more detailed examples around the exceptions in the final regulation will help provide more confidence in the accurate interpretations of when the exceptions apply and the peace of mind that the actors will need to proceed with appropriately sharing information.

In addition, we ask ONC to ensure that the depth of the examples included in the final regulation match the requirements included in regulatory text. Many of the current examples in the proposed regulation clearly illustrate what is reasonable and what is not reasonable in terms of the application of the information blocking exceptions. However, the corresponding regulatory text often does not define that information in the same straightforward way. ONC needs to coordinate the substance of the text with what is included in the examples, as enforcement of the information blocking exceptions will be wholly dependent on what is stated in the regulatory text as well as the clarity around those points. The criteria and language in the examples often put limits on what is information blocking by making a clearer case than the text that the interference may be unreasonable. However, the text typically reserves broader definitions of information blocking without the criteria that would separate what may be unreasonable from what may be reasonable. In sum, the text should not be worded in such a way that it is overly broad.

HIMSS also requests that ONC recognize and accommodate the inherent complexities around the exceptions and seek to streamline the processes around claiming an exception, compliance with all the applicable terms and conditions of the exceptions, the burden of proof to demonstrate compliance, and enforcement from ONC, HHS Office of Inspector General (OIG), HHS Office for Civil Rights (OCR), and Federal Trade Commission (FTC). The burden placed on all health system stakeholders will be extensive, and could contribute to the clinician burden issues that ONC and CMS have been working to try to address over the last two years.

This burden will also present a hurdle for the new market entrants and innovative developers that ONC would like to see enter this space and contribute to facilitating more access, exchange, and use of EHI. Moreover, investment in new, emerging technologies to promote broader data exchange by certified developers could also suffer if reporting and compliance burden is not minimized.

Also, the requirement in the proposed regulation that to “qualify for any of these exceptions, an individual or entity would, for each relevant practice and at all relevant times, must satisfy all applicable conditions of the exception,” sets a very high bar for compliance. HIMSS recommends that ONC seek to relax this standard, especially given the inherent intricacies of a broader nationwide exchange enterprise. ONC could look at scaling up to the “all applicable conditions of the exception” standard beginning in year 2 or possibly year 3 of this regulation’s implementation, and create a smaller set of requirements that have to be met in year 1 as the actors figure out how to implement the regulation and ensure their internal processes are established.

Although the 21st Century Cures Act mandates a focus on identifying the reasonable and necessary activities and practices that do not constitute information blocking, we also ask ONC to promulgate a list of best practices for broadly sharing more information, consistent with these exceptions. Such a list could serve to reinforce the positive behaviors expected of the regulated actors, establishing “safe lanes” for specific use cases and reducing compliance costs and risks. These best practices could also help define more detailed information around the intended roles and expectations for each of the actors.

Collecting and disseminating this type of information would help to frame the Information

Blocking requirements differently, enabling better interpretation across the community as well as relieve some of the administrative and regulatory burden associated with implementing this regulation. Moreover, such information should also include baseline expectations that can be consistently applied and measured to ensure that expectations are explicitly communicated to the actors as well as demonstrated by those actors in the course of facilitating more data exchange.

Adding a list of best practices to the Information Blocking section of the final regulation and in subsequent sub-regulatory guidance would support ONC's idea to promote policies that are clear, predictable, and administrable as well as help to minimize compliance and other burdens for stakeholders. It would also contribute to ONC's adherence to Congress's plainly expressed intent to provide a comprehensive response to the information blocking problem.

§ 171.102 Definitions

For purposes of this part:

Access means the ability or means necessary to make electronic health information available for use, including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained.

Actor means a health care provider, health IT developer of certified health IT, health information exchange, or health information network.

API Data Provider is defined as it is in § 170.102.

API Technology Supplier is defined as it is in § 170.102.

Electronic Health Information (EHI) means—

(1) Electronic protected health information; and

(2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that 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.

Electronic media is defined as it is in 45 CFR 160.103.

Electronic protected health information (ePHI) is defined as it is in 45 CFR 160.103.

§ 171.102 Definitions

Exchange means the ability for electronic health information to be transmitted securely and efficiently between and among different technologies, systems, platforms, or networks in a manner that allows the information to be accessed and used.Fee means any present or future obligation to pay money or provide any other thing of value.

Health care provider has the same meaning as ‘‘health care provider’’ at 42 U.S.C. 300jj.

Health Information Exchange or HIE means an individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes.

Health Information Network or HIN means an individual or entity that satisfies one or both of the following—

(1) 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 electronic health information between or among two or more unaffiliated individuals or entities.

(2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

Health IT developer of certified health IT means an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program.

Information blocking is defined as it is in § 171.103 and 42 U.S.C. 300jj-52(a).

Interfere with means to prevent, materially discourage, or otherwise inhibit access, exchange, or use of electronic health information.

Interoperability element means—

(1) Any functional element of a health information technology, whether hardware or software, that could be used to access, exchange, or use electronic health information for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.

(2) 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.

(3) Any technology or service that may be required to enable the use of a compatible technology in production environments, including but not limited to any system resource, technical infrastructure, or health information exchange or health information network element.

(4) 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.

§ 171.102 Definitions

(5) Any other means by which electronic health information may be accessed, exchanged, or used.

Permissible purpose means a purpose for which a person is authorized, permitted, or required to access, exchange, or use electronic health information under applicable law.

Person is defined as it is in 45 CFR 160.103.

Protected health information is defined as it is in 45 CFR 160.103.

Practice means one or more related acts or omissions by an actor.

Use means the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.

Preamble FR Citation: 84 FR 7509-15 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Access Definition

HIMSS questions the expansive definition of “access” in the proposed regulation focused on:

“the ability or means necessary to make electronic health information available *for use*, including the ability to securely and efficiently locate and *retrieve information from any and all source systems* in which the information may be recorded or maintained.”

We fear that this proposed definition could be interpreted to allow access to a provider’s health information systems, and locate and retrieve information from their EHR, patient accounting systems, picture archiving and communication system (PACS), laboratory information system (LIS), etc. This access would be much broader than portal access or transmission to patient, third party, or API, as it would essentially permit every patient, their agent(s), and every treatment provider (as well as their business associates) to gain entry to a provider’s networks and browse through their systems.

These actions are materially different than transmitting data and enabling APIs, and would be extremely challenging to implement given the current state of technical privacy and security safeguards for patient identity matching and data segmentation embedded in certified EHRs, and even more taxing in source systems such as patient accounting systems, PACS, LIS, as well as other systems.

HIMSS recommends that the definition be scaled back to more closely align with the HIPAA definition of access, which is essentially to gain an electronic copy of one’s PHI. That definition would ensure that data could be transmitted as directed by the patient without weakening any of the API provisions in the proposed regulation. In addition, it is important to note that providers would need to continue to provide a portal, and extract as well as download an individual’s information into standard formats to be considered successful under the regulations included in the CMS

Promoting Interoperability Program.

EHI Definition

ONC proposes to define EHI as electronic protected health information (ePHI) that 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. The focus of the proposed definition casts an enormous net across the healthcare ecosystem to collect as much information as possible about an individual.

HIMSS supports a scaled-back definition of EHI in the final regulation that focuses on using the US Core Data for Interoperability (USCDI) data classes in the near-term as the requirement for being interoperable nationwide. This scaled-back approach would concentrate on exchanging the most clinically relevant, actionable information for an individual that could be used to improve their health outcomes (with or without a consultation with a healthcare practitioner). Facilitating the sharing of more targeted data will help address any concerns arising from a clinician burden perspective and help ensure that the receiver of the data is able to "consume" and use the data in a clinical setting.

In the future, HIMSS would like to see USCDI expanded to include additional data classes that encompass more information streams. As ONC discusses in the proposed regulation, the USCDI data classes (including structured data fields) are designed to be expanded in an iterative and predictable way over time. Within the next two years, HIMSS recommends that ONC consider the addition of several data classes to USCDI, including: social determinants of health data, patient-generated health data, wearables data, genomics data, and healthcare cost and price information, including attributes to ONC's Interoperability Standards Advisory.

ONC should work with the community to develop parameters and definitive implementation timeframes for these data classes as well other HIPAA-compliant data that should be considered for inclusion in USCDI. Ultimately, HIMSS wants the community to move beyond simply facilitating the exchange of the data typically stored in an EHR—more innovation and new market entrants could accompany the establishment of these additional data classes, leading to more novel ways to deliver on the promises of healthcare transformation.

HIN/HIE Definitions

HIMSS requests that ONC revise and hone the definitions for HIE and HIN in the proposed regulation to ensure that only the organizations intended to be in these categories are included in this regulation. The 21st Century Cures Act draws a distinction between these two terms in statute and ONC attempts to define each separately. We recommend that ONC seek greater alignment with the common use of each term from across the community as well as with Congressional intent at the time the law was enacted.

One significant change that we are also recommending is that the ONC merge the two terms into a single category. With the information blocking exceptions, definitions, and penalties applying exactly the same to both kinds of entities, it is not materially relevant for these terms to remain in separate categories.

However, it is critically important that the merged terms do not remain defined as expansively as they currently are structured. For example, Congress created "health care provider" as a separate category; however, the broad definition of HIN in the proposed regulation could possibly encompass a healthcare organization with very limited exchange capabilities that is directing its own exchange processes. HIMSS recommends that ONC formalize the definition of this new merged category and clearly detail the entities that would and would not be considered an HIE or an HIN in the final regulation.

In addition, state public health agencies, public health interface engines, as well many SDOs likely fall into the current HIN definition, but, based on congressional intent, our read is that none of these entities should be placed in that category. Payers, middleware developers, and clearinghouses also fall into the proposed regulation's broader HIE/HIN definition, but were never intended to be during enactment.   Clearly defining which organizations are included in the HIE/HIN category provides the entire community with the clarity that they need to implement this regulation and facilitate greater levels of exchange.

Request for comment regarding the definition of "health care provider"

The term "health care provider" is defined in Public Health Service Act section 3000(3) (42 U.S.C. 300jj(3)). We propose to adopt this definition for purposes of section 3022 of the PHSA when defining "health care provider" in § 171.102. We note that this definition is different from the definition of "health care provider" under the HIPAA Privacy and Security Rules. We are considering adjusting the information blocking definition of "health care provider" to cover all individuals and entities covered by the HIPAA "health care provider" definition. We seek comment on whether this approach would be justified, and commenters are encouraged to specify reasons why doing so might be necessary to ensure that the information blocking provision applies to all health care providers that might engage in information blocking.

Preamble FR Citation: 84 FR 7510 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

ONC asks the question about how it should define "health care provider" in the proposed regulation. HIMSS supports the "provider" definition from section 3000(3) of the Public Health Service Act (PHSA). We prefer this definition because it is clear by provider type and specifically enumerates the types of providers to whom the information blocking provisions apply. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) "health care provider" definition is too broadly construed as a provider of medical or health services and "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." The specificity inherent in the PHSA definition is what the community needs to appropriately implement a final regulation.

Request for comment regarding price information (ONC)

We seek comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking.

Preamble FR Citation: 84 FR 7513-14 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS agrees with ONC’s characterization in the proposed regulation around the fragmented and complex nature of pricing within the health care system and the negative impact that it has had on the efficiency of the health care system and all health system stakeholders. Transparency issues and anticipating as well as planning for costs is challenging, and there are few objective means for patients and providers to measure the quality of the care or coverage received relative to the price paid. Moreover, in order for price transparency to be truly useful for patients, price information must be paired with meaningful quality data.

HIMSS supports the idea of including price information in EHI, but cautions about attempting to include this information in the rollout of this initial final regulation. As previously described, HIMSS envisions that the EHI definition would comport with USCDI, and we propose that the data classes evolve over time to eventually include healthcare price information. We recommend that ONC look at adding data classes within the next two years.

In the meantime, HIMSS recommends that ONC work with CMS to support and enhance the efforts currently underway to improve access to price information. Earlier this year, CMS began requiring hospitals to post their standard charge information online in a machine-readable format. CMS is also facilitating action at the state level to hold insurers accountable. For example, CMS is providing grants to states to develop and upgrade existing technology to streamline data sharing and put information in the hands of consumers more quickly. These efforts can help to inform the future expansion of the data classes under USCDI to include price information. HIMSS wants to help ONC work towards developing a practical framework that prevents the blocking of price information.

VIII.D Proposed Exceptions to the Information Blocking Provision

§ 171.201 Exception – Preventing harm

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) 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—

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; or

(3) Disclosure of a patient's electronic health information 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, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be—

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; and

(4) No broader than necessary to mitigate the risk of harm.

(c) 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.

Preamble FR Citation: 84 FR 7523-26 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Preventing Harm is a critical exception to include in the regulation. HIMSS requests that the focus of this exception expand from preventing physical harm by not broadly sharing data to include psychological, psychosocial, and mental harm. Ultimately, it should be up to the regulated actor to determine what patient-related harm they are trying to prevent by claiming this exception, and document how they reached this decision to restrict access, use, or exchange of EHI. As ONC moves to a final regulation, more examples and use cases could better define the parameters around use of this exception. Also useful for ensuring consistency would be an inclusion of issues that do not qualify for such an exception, e.g., applying this exception to all patients because of an inaccurate belief that not sharing data is safer than sharing data.

The Proposed Regulation is thoughtful around describing the idea that 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. However, it is often a challenge for an actor to determine all the instances of corruption or inaccuracies in a patient’s record. If an issue is identified, as a regulated actor works to determine the extent of these issues, ONC should provide clear guidance that the record in question can meet the requirements around the exception—this patient data should not be shared while this evaluation is taking place.

ONC needs to be cognizant of the significant burden placed on an actor to do their best that data quality and that data integrity is preserved in a specific record in order to share it. ONC needs to allow the actor to err on the side of caution as it looks to determine the extent of potential distortions in the record before sharing it. Furthermore, ONC should consider that data coming from new actors will mean that records will include differences of opinions—perhaps with different data points or differing concepts in one party’s determination—and questions about accuracy in others. ONC should impose a time limit on how long this evaluation could last, but the final regulation needs to recognize and address this issue.

In addition, when developing policies to guide actors in how to claim as well as fully justify this exception, we encourage ONC to define the level of documentation that should be preserved and a length of time that information needs to be accessible in order to make a claim determination.

§ 171.202 Exception – Promoting the privacy of electronic health information

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) Meaning of “individual” in this section. The term “individual” as used in this section means one or more of the following—

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual’s estate under State or other law.

(b) Precondition not satisfied. If the actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information, the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that—

(1) The actor’s practice—

(i) Conforms to the actor’s organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; and

(C) Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; or

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor’s practice is—

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

c) Health IT developer of certified health IT not covered by HIPAA. If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the actor may choose not to

§ 171.202 Exception – Promoting the privacy of electronic health information

provide access, exchange, or use of electronic health information provided that the actor's practice—

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

Preamble FR Citation: 84 FR 7526-35 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports the inclusion of the promoting privacy exception and the four sub-exceptions defined in the proposed regulation. HIMSS is very supportive of the proposed expansive definition in this exception to protect information about all individuals, not just individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates. In addition, HIMSS also appreciates that ONC is permitting an actor not to provide access, exchange, or use of EHI if an individual has specifically requested that the actor not do so.

ONC clearly states that any privacy protection practice must be consistent with applicable laws related to health information privacy, such as the HIPAA Privacy Regulation, HITECH Act, 42 CFR Part 2, and state privacy laws. However, given the extensive uncertainty that still exists across the community around these requirements and how they intersect with individual rights, it is critical that ONC work with OCR and other federal and state entities to create clear guidance on when this exception applies to patient privacy rights as well as information sharing, including additional guidance related to data which is *outside* of the domain of HIPAA.

ONC should also clarify issues surrounding control over the exchange of an individual's EHI in public health contexts (for example, data about HIV status and individuals' engagements in HIV-related medical care). Uses of data by health departments are generally subjected to a much different sets of regulations (federal and state) than EHI generated by HIPAA CEs. Overall, these guidance documents will help to simplify what is a complex information blocking exception.

Unfortunately, HIPAA is still often used as an excuse to not share information with or on behalf of patients. HIMSS wants to ensure that the community more clearly understands the pertinent privacy-related laws and how they could potentially conflict with information blocking exceptions, as this regulation may require actors to provide access, exchange, or use EHI in situations that are inconsistent with HIPAA requirements.

In one of the sub-exceptions, ONC proposes to protect actors who do not provide access, exchange, or use EHI because a necessary precondition imposed under law for that disclosure was not met. If the legal precondition relies on consent or authorization from an individual, the actor must do all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide that consent or authorization.

We agree with ONC that the final regulation should provide further guidance on what “reasonably necessary” and “within its control” mean, and provide more detailed examples and use cases. This sub-exception could apply differently to each regulated actor, as they may have varying levels of control over the generation of an individual’s health information as well as different levels of contact with individuals in order to secure consent and authorization.

Finally, it is important for ONC to recognize that exceptions such as this one must not be used to justify failure to perform public health reporting.

§ 171.203 Exception – Promoting the security of electronic health information

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; and

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

Preamble FR Citation: 84 FR 7535-38 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports this exception and ONC's work to encourage actors to implement appropriate security protocols and safeguard the confidentiality, integrity, and availability of EHI. HIMSS also appreciates that ONC mandates that an actor's documented security policy must be informed by a security risk assessment and be aligned with applicable consensus-based standards as well as best practice guidance. Such alignment will provide actors of different sizes and with various levels of resources the flexibility they need to apply the right security controls, to the right information systems, at the right time to address risk adequately.

HIMSS recommends that ONC work with OCR to develop further guidance around this exception, including any additional legal liability that could come from the intersection of this exception and HIPAA, state privacy laws, or other agreements. In particular, the recent OCR guidance requiring Covered Entities (CEs) to share data with anyone the patient designates may lead to patient harm.

OCR should revisit this guidance to allow CEs to prohibit sharing with developers who fail to meet a standard level of security during this time of transition. In these early days, patients will have no resources to evaluate the third parties who would be acting on their behalf, so in order to avoid patient harm, it behooves ONC and OCR to coordinate how a transparency requirement for communicating data sharing policies with patients is enforced. It is likely that CEs will need to be the gatekeepers in order for this transparency to occur.

In addition, we ask ONC to clearly define several terms to help regulated actors appropriately understand the parameters of this exception. For example, as ONC discusses the conditions that an actor must meet in order to qualify for this exception, and states that, “the practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information,” and “the practice must be tailored to the specific security risk being addressed.” Further clarity around the terms “directly related” and “tailored” is required for actors to determine their status in relation to this exception.

Moreover, we applaud ONC for including the contingency for practices that do not implement an organizational security policy and recognizing that this issue will likely arise under exigent circumstances. However, the possibility that an actor in these kind of situations can consider “reasonable and appropriate alternatives that could have reduced the likelihood of interference with access, exchange, or use of EHI,” is unlikely. ONC should provide actors with more flexibility when they encounter these extreme exigent circumstances and the often urgent nature of the security threats in question. Further documentation and notification requirements after an incident is resolved may be a better approach, instead of expectations around consideration of reasonable and appropriate alternatives.

§ 171.204 Exception – Recovering costs reasonably incurred

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Types of costs to which this exception applies. This exception is limited to the actor's costs reasonably incurred to provide access, exchange, or use of electronic health information.

(b) Method for recovering costs. The method by which the actor recovers its costs—

(1) Must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests;

(2) Must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged;

(3) Must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported;

(4) Must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor; and

(5) Must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information.

(c) Costs specifically excluded. This exception does not apply to—

(1) Costs that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using electronic health information;

(2) Costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets;

(3) Opportunity costs, except for the reasonable forward-looking cost of capital;

(4) A fee prohibited by 45 CFR 164.524(c)(4);

(5) A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's electronic health information;

(6) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; or

(7) 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.

(d) Compliance with the Conditions of Certification.

§ 171.204 Exception – Recovering costs reasonably incurred

(1) Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4) or § 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(2) If the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404 of this subchapter.

Preamble FR Citation: 84 FR 7538-41 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports this exception and the ability of regulated actors to be able to recover the costs they incur to develop technologies and provide services that enhance interoperability. ONC is justified in its approach as excessive fees could interfere with the access, exchange, or use of EHI.

This exception will allow actors to recover costs that they reasonably incur to develop technologies and provide services that enhance interoperability, and bolster the ultimate goals of the information blocking provision by incentivizing investment, development, and dissemination of interoperable technologies and services that enable more robust EHI exchange. It is important that ONC clarify the situations when this exception would apply compared to the pricing aspects of the reasonable and non-discriminatory contracting exception. It would benefit the community if ONC could provide relevant examples to illustrate the distinctions between the applicability of the two exceptions.

Regulation established under HIPAA provides guidance that permissible fees should be nominal and not exorbitant. ONC should take a similar approach regarding rights to access and should provide guidance that seeks to avoid costly volume based API transactions that directly penalize data consumers. This approach should also be harmonized with any final guidance in order to maintain the spirit across all interoperable mechanisms, along with input and guidance from OCR.

HIMSS also supports the provisions that focus on the costs that are excluded from protection under this exception, such as costs due to non-standard design or implementation, as they increase the complexity, difficulty, or burden of accessing, exchanging, or using EHI. In addition, we endorse the exclusion of any fee associated with an individual electronically accessing their EHI. HIMSS also applauds the alignment of this exception with compliance under the Conditions of Certification provisions for health IT developers, although it notes that the cost documentation requirements for certification appear even more substantial than those for the exception.

We also ask ONC to recognize that basing pricing on client or partner size or revenue, which is very common in the non-profit community, can be a reasonable and cost-effective proxy on which to base fees and allocate costs. However, as new actors participate in information exchange, new pricing models will emerge. ONC should also recognize that certain agreements that share revenues can be economically warranted if entered into freely (and not implicate information blocking), as long as patients' individual access is not prevented by exorbitant pricing practices.

Although HIMSS supports the approach of this exception, more specifics will be needed by regulated actors in order to ensure compliance with these regulations. HIMSS is also very concerned with the overall complexity and burden that these requirements will impose on the community, and the infrastructure that will need to be created and maintained in order to capture and document all the fee information charged by actors in the course of access, exchange, and use of EHI. We recommend that ONC seek to simplify these requirements, especially around the cost accounting that will be required of the actors. We also ask the ONC retain and clarify the notion of a "reasonable profit," which is referenced in the preamble but not actual regulatory language.

How each actor allocates its costs among different projects will be unique, and ONC will need to provide more specifics around its expectations for capturing and recording costs, including the length of time that actors need to retain this cost information. It may be challenging for an actor to allocate its core costs around a specific technology that was developed to be supplied to multiple customers with minimal tailoring. If the cost accounting infrastructure called for in this exception is not significantly simplified, it could lead to the perverse effect of raising an actor's costs to develop and deliver technologies that lead to more information exchange.

We understand ONC's justification for inclusion of this exception is the practices identified in the Report to Congress on Information Blocking. However, there is a need for more specifics as well as a reduction of some requirements, to ensure that this new infrastructure does not have the unintended consequence of raising an actor's costs to produce new exchange-related technologies.

§ 171.205 Exception – Responding to requests that are infeasible

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Request is infeasible.

(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—

(i) The type of electronic health information and the purposes for which it may be needed;

(ii) The cost to the actor of complying with the request in the manner requested;

(iii) The financial, technical, and other resources available to the actor;

(iv) 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;

(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

(vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and

§ 171.205 Exception – Responding to requests that are infeasible

(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.

(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.

(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(b) Responding to requests. The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.

(c) Written explanation. The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(d) 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 electronic health information.

Preamble FR Citation: 84 FR 7542-44 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS agrees with this exception and supports the idea that in certain circumstances there are legitimate practical challenges beyond an actor's control that limit its ability to comply with requests for access, exchange, or use of EHI. In some cases, the actor may not have the necessary technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, or because the actor would incur costs or other burdens that are clearly unreasonable under the circumstances.

However, this exception could place significantly more burden on the organization receiving the request than the actual requestor. ONC should work across the Department to devise a simpler, streamlined framework that could guide actors when considering whether they are eligible to claim this exception. HIMSS supports the fact-specific approach that ONC is planning to undertake as well as its consideration of an actor's particular circumstances and the financial, technical, and other resources and expertise at its disposal.

Given our expectations around the use of this exception in practice, HIMSS also wants to ensure that all health system participants are appropriately incentivized to broadly share information across organizational and regional boundaries. Over the next several years, ONC should try to determine if the same actors are consistently claiming this exception, and whether those actors are making the necessary investments in IT infrastructure and personnel in order to do their part to fulfill requests for access, exchange, or use of EHI.

In addition, ONC should reduce its expectations around what an actor should do to facilitate other means of accessing, exchanging, and using the EHI if it cannot carry out the request. An actor that receives a request should not necessarily have to shoulder the burden of finding a reasonable alternative means of accessing, exchanging, or using the EHI. Often, there will be a straightforward means that an actor can recommend to the requestor about how best to obtain the information that they are seeking, but the actor should not be required to work with the requestor—HIMSS would favor language stating that the actor is encouraged to work with the requestor if feasible. In particular, if the actor can provide the data requested in a standard format that meets the requirements of this regulation, any other format being requested should be based on a negotiated discussion between the parties that is outside of this regulation.

HIMSS appreciates the inclusion of language about how an actor could seek coverage under this exception if it is unable to provide access, exchange, or use of EHI due to a natural disaster (such as a hurricane, tornado, or earthquake). HIMSS strongly encourages ONC to expand the list of disasters to include man-made situations, such as an accident, active shooter, terrorism, or cybersecurity incident. These types of situations would most likely be outside of the actor's control and should be noted under this exception.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) 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 by:

(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and

(2) Offering an appropriate license with reasonable and non-discriminatory terms.

(b) Reasonable and non-discriminatory terms. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

(1) Scope of rights. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.

(i) 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.

(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.

(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(2) Reasonable royalty. If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor’s technology to the licensee’s products, not on any strategic value stemming from the actor’s control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards development organization in accordance with such organization’s policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies.

(3) Non-discriminatory terms. The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements.

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on—

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

(4) Collateral terms. The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

(5) Non-disclosure agreement. The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided—

(i) The agreement states with particularity all information the actor claims as trade secrets; and

(ii) Such information meets the definition of a trade secret under applicable law.

(c) Additional requirements relating to the provision of interoperability elements. The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

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

(d) Compliance with conditions of certification. Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the conditions of certification in §§ 170.402, 170.403, or 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

Preamble FR Citation: 84 FR 7544-50 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS appreciates the procompetitive stance in this exception for developers of interoperable technologies and services, as well as innovators and new market entrants. We support the push to eliminate practices that limit access, exchange, and use of EHI and stifle competition and innovation in the health IT sector. Contractual language or intellectual property rights should not be used to extract rents for access to EHI—such actions would undermine the fundamental objectives of the Information Blocking regulation.

Also, as previously mentioned, it is important that ONC clarify the situations when this exception would apply compared to the recovering costs reasonably incurred exception. It would benefit the community if ONC could provide relevant examples to illustrate the distinctions between the applicability of the two exceptions and ensure that there are not intended incentives to use or not use licensing models.

ONC's standard guiding this exception permits actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms that do not impose collateral terms or otherwise impede use of interoperability elements.   We ask ONC to clarify whether this exception applies to all software-relate licenses, which are ubiquitous in health IT, or only specific licenses for certain types of IP (e.g., use of patented technology, code sets, etc.).

The 10 business days that ONC provides an actor to respond to a request to license or use interoperability elements is acceptable. It is also important to note that ONC is not requiring actors to grant a license to a requestor under all circumstances—as long as the negotiations are conducted under RAND terms and an offer pursuant to those negotiations is made, the actor is meeting the terms of the exception.

Moreover, HIMSS appreciates that actors do not have to apply the same terms and conditions for all persons requesting a license, although any differences are based on actual, legitimate differences in costs that actors incur, or on other non-discriminatory criteria that are objectively verifiable. More examples on this topic from ONC would be helpful, but an actor could provide more favorable terms under a co-marketing agreement or joint venture than for a transaction with a new partner.

HIMSS is also supportive of ONC's proposal to allow an actor to require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets. The agreement would have to specify all information the actor claims as trade secrets, with the information meeting the definition of a trade secret under applicable law. We also endorse the idea that actors should be held accountable when they license interoperability elements on RAND terms that they will not engage in separate practices that impede the use of those interoperability elements or otherwise undermine the intent of this exception.

§ 171.207 Exception – Maintaining and improving health IT performance

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) 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, provided that the actor's practice is—

(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

(b) Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(c) Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

Preamble FR Citation: 84 FR 7550-52 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports this exception for identifying practices that are reasonable and necessary to maintain and improve the overall performance of health IT, including both planned and unplanned instances when health IT needs to be temporarily taken offline for maintenance and improvement purposes.

We appreciate that ONC acknowledges that health IT performance service agreements need to continue to be able to provide flexibility to ensure that system availability is balanced with essential maintenance and improvements. When health IT is taken offline for maintenance or improvement that has been agreed to by the customer, HIMSS supports ONC's proposal that the agreement or resultant actions would not constitute information blocking.

We also endorse the inclusion of more specifics around when health IT must be taken offline on an urgent basis that is not expressly permitted in a contract. ONC proposes that this action would not necessarily be considered information blocking if the actor provides oral notice to the recipient. However, HIMSS wants ONC to clarify this issue, and ensure that the recipient/client would need to provide permission, which could be problematic if there is an urgent need to take a system down, especially in a cloud environment.

In addition, HIMSS is supportive of this exception applying when a customer initiates unavailability and no agreement was previously established, although this unavailability would still need to satisfy the other conditions of this exception.

We also appreciate that ONC aligns the “maintenance and improvement of health IT performance” exception with other relevant exceptions in the regulation. If the unavailability of health IT is initiated by an actor in response to a risk of harm to a patient, that actor would not need to satisfy the requirements of this exception, but they would need to comply with all the requirements for the “preventing harm” exception. Moreover, if the unavailability of health IT is in response to an EHI security risk, the actor would have to comply with all the requirements for the “promoting the security of EHI” exception.

Request for information on a potential additional information blocking exception for complying with the Common Agreement for Trusted Exchange

We are considering whether we would should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement. Such an exception may support adoption of the Common Agreement and encourage other entities to participate in trusted exchange through HINs that enter into the Common Agreement. We ask commenters to provide feedback on this potential exception to the information blocking provision to be considered for inclusion in future rulemaking.

Preamble FR Citation: 84 FR 7552 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Request for information on a potential additional information blocking exception for complying with the Common Agreement for Trusted Exchange
Public Comment Field: HIMSS supports the work undertaken by ONC to develop TEFCA. As previously discussed, we are still completing a full analysis of TEFCA Draft 2, and will be submitting public comments on that guidance document in the next several weeks. The underlying concept and goals of TEFCA are forward-looking: to provide a single on-ramp to nationwide connectivity and enable EHI to securely follow the patient when and where it is needed. Moreover, the idea of potentially providing an information blocking exception that drives more health system stakeholders toward participation in TEFCA is compelling. Given the scope of the other seven exceptions identified in the proposed regulation, an exception in this area is necessary. However, without a final Common Agreement released for production, it is difficult to say whether health system stakeholders will adopt the voluntary Framework and if an information blocking exception should be structured around it. TEFCA has no firm infrastructure yet in place, the proposed implementation timelines are challenging, and the draft exchange standards are not very mature. In the broadest sense, HIMSS sees the value of providing protections to practices that are expressly required by the Common Agreement, or that are necessary to implement such requirements, that might implicate the information blocking provision and would not qualify for another exception. But, without a final Common Agreement, we cannot commit to adding a narrow exception in this area.

VIII.F Complaint Process

Information blocking complaint process
ONC requests comment on the current complaint process approach and any alternative approaches that would best effectuate this aspect of the Cures Act. In addition to any other comments that the public may wish to submit, we specifically request comment on a list of specific issues related to the complaint process.
Preamble FR Citation: 84 FR 7552-53 Specific questions in preamble? *Yes*
Regulatory Impact Analysis: Not applicable
Public Comment Field: HIMSS supports the development of a reconfigured complaint process that builds on existing mechanisms for the public to submit reports of claims of health information blocking, including the

complaint process currently available at https://www.healthit.gov/healthit-feedback.

We encourage ONC to reformat this program to ensure that the reporting and administrative burden requirements for the public as well as the regulated actors is minimized. ONC should also look to try to leverage data that is already captured in health IT platforms and use it to help inform the complaint process. In addition, given the amount of patient-level data that CMS already collects from providers, we encourage the agencies to work together to determine if it is possible to repurpose collected information to replace documentation requirements and eliminate additional reporting.

The Cures Act provides for the collection of such information as the originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information. ONC should capitalize on these information sources, but as the process evolves, the agency should look at determining the information that is absolutely critical to have in order to render an information blocking decision and only request those data points in the next iteration of the complaint process.

VIII.G Disincentives for Health Care Providers – Request for Information

Request for information on disincentives for health care providers

We request information on disincentives or if modifying disincentives already available under existing HHS programs and regulations would provide for more effective deterrents to information blocking. We also seek information on the implementation of section 3022(d)(4) of the PHSA, which provides that in carrying out section 3022(d) of the PHSA, the Secretary shall, to the extent possible, not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved as of the day before December 13, 2016 – enactment of the Cures Act.

Preamble FR Citation: 84 FR 7553 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

ONC should develop disincentives for health care providers that will act as an effective deterrant to information blocking-related actions. Given the Civil Monetary Penalties in place for the other regulated actors in this proposed regulation, disincentives for providers must be on par with the other actors. We recommend that ONC work with CMS to use its payment programs as policy levers to encourage compliance with the provisions of this regulation. Building in further disincentives to the Promoting Interoperability Program as well as other payment policies will encourage behaviors that facilitate greater information sharing and hold those accountable that do not meet expectations.

ONC should also explore holding back other federal funding streams that typically flow to providers as possible disincentives for repeated, purposeful information blocking. Funding from other Department of Health and Human Services agencies, such as the National Institutes of Health, Centers for Disease Control and Prevention, as well as the Department of Veterans Affairs and Department of Defense could also be suitable levers for those providers that are repeatedly non-compliant. Any disincentives structure that ONC is considering should be put through a public notice and comment process, and the agency should leverage the work and expertise of its Health IT Advisory Committee to help determine an appropriate disincentives framework.

Section IX – Registries Request for Information

Health IT Solutions Aiding in Bidirectional Exchange with Registries

We believe it is appropriate to explore multiple approaches to advancing health IT interoperability for bidirectional exchange with registries in order to mitigate risks based on factors like feasibility and readiness, potential unintended burden on health care providers, and the need to focus on priority clinical use cases. ONC is therefore seeking information on how health IT solutions and the proposals throughout this rule can aid bidirectional exchange with registries for a wide range public health, quality reporting, and clinical quality improvement initiatives.

We also welcome any other comments stakeholders may have on implementation of the registries provisions under § 4005 of the Cures Act.

Preamble FR Citation: 84 FR 7553-54 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

HIMSS supports ONC's work on facilitating interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. We agree with ONC about the myriad public reporting requirements for registries where a lack of standardization has contributed to slow adoption of health IT systems.

We highlight for ONC that there are real limitations around any version of FHIR that can adequately support registry reporting and activities. Additional work needs to be undertaken to ensure that FHIR R4 builds in these capabilities and that the community understands how to take advantage of these technological advances.

HIMSS encourages ONC to continue to emphasize the areas where the use of standards could significantly improve bidirectional exchange with registries for a whole host of topics, including: public health, quality reporting, and quality improvement. In addition, ONC should build on the promise of FHIR R4 in reducing the burden associated with implementing multiple solutions and the expanded capabilities to collect detailed, standardized data.

Section X – Patient Matching Request for Information

Opportunities to Improve Patient Matching
We seek comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. ONC is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability.
Preamble FR Citation: 84 FR 7554-55 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: NA

Public Comment Field:

We are pleased that ONC (along with CMS) is considering more action on patient matching by seeking comment in this proposed regulation. As we scale towards nationwide exchange, patient matching accuracy will only degrade further as more enterprises contribute errors and these errors compound, unless more action is taken on this critical patient safety issue. Poor patient matching can easily lead to patients receiving erroneous care or not receiving care they need. Whether matching errors lead to duplicate records or record overlays, patients who are not correctly matched to their records within and across healthcare systems and providers will ultimately not receive optimal care.

It is clear to HIMSS, as well as other stakeholders, that patient identification and matching remains a paramount challenge to information exchange and optimized patient care. HIMSS has long been involved in leading private sector efforts to improve patient matching, including funding an Innovator-in-Residence at HHS who worked on this topic. It was the work of the HIMSS Innovator-in-Residence that led to the ONC Patient Matching Algorithm Challenge in 2017.

This effort helped to bring greater transparency and data on the performance of existing patient matching algorithms, and spur the adoption of performance metrics for patient data matching algorithm vendors, as well as positively affect other aspects of patient matching such as de-duplication and linking to clinical data. Given that ONC has an infrastructure created by this challenge, it is important that HHS use the infrastructure for continued analysis and work on matching, potentially even with an updated challenge. Consideration should also be given to evaluating and expanded set of identifiers for use in the matching challenges, ranging from things like biometrics to height to less commonly used demographics, such as mother’s first name, which is already being used in the California Medicaid Program. It is critical that this work continue to be led by the private sector in coordination with our federal partners.

Across the healthcare sector, there is a broad range of patient matching solutions commercially available. Some are stand-alone component products that focus just on patient matching, while others can be found embedded within the EHR platforms. Since there is no recognized authority or measure for patient matching capability, no organization can make a fact-based decision about which technologies work well and which do not. Many health organizations do not realize that there are differences in performance, and, ultimately, that they have a serious patient matching problem until it is too late.

Improving patient matching by standardizing demographic data means the benefits will mostly be realized by those organizations using the less sophisticated patient matching tools. Today, the higher performing technologies already accommodate “dynamic standardization” which formats demographic attributes consistently prior to any match algorithms being applied.

HIMSS strongly supports the use of matching algorithms as part of an overall patient matching strategy. However, we think that an explicit mandate of a specific patient matching algorithm at this time is premature, especially considering there is no current way to benchmark the accuracy of those algorithms. HHS should work with the private sector to create a benchmark measurement for algorithms that have been and will be developed. This benchmark would help providers, organizations, and potentially ONC decide which algorithm to use moving forward.

These patient matching algorithms could be improved with more standardized data elements. HIMSS offers these additional data elements as a suggestion to improve patient matching: maiden name, multiple birth indicator, birth order, telephone number types (specifically mobile), and email address. More generally, data collection standards and their consistent application by health plans, providers, and exchange organizations are a critical determinant to matching accuracy. HIMSS believes the biggest opportunity to immediately enhance matching rates is standardized formats for demographic data among data sharing participants.