EHRA
HIMSS Electronic Health Record Association

33 W Monroe, Suite 1700
Chicago, IL 60603
swillis@ehra.org
Phone: 312-915-9518
Twitter: @EHRAssociation

June 3, 2019

Donald Rucker, MD
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street SW
Washington, DC 20201

Dear Dr. Rucker,

On behalf of the Electronic Health Record (EHR) Association, we are pleased to submit our comments on the proposed rule, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," which was published in the *Federal Register* on March 4, 2019 by the Office of the National Coordinator for Health Information Technology (ONC). These comments are based on the collective perspectives and expertise of the Association's more than 30 member companies who serve the majority of hospitals and ambulatory care providers using EHRs across the United States.

The EHR Association recognizes and appreciates the extensive effort on the part of ONC and the Office of the Inspector General (OIG) to define the required exceptions to the information blocking sections of the 21st Century Cures Act (Cures). We appreciate the thoughtful work the agencies did to engage multiple stakeholders (including the Association) in gathering practical and measurable input.

Our detailed comments are included within the attached comment template provided by ONC. EHR Association members have significant concerns regarding some proposals, in particular:

Barriers to innovation
Congress intended for the Cures Act to foster innovation, but imposing price caps and compulsory licensing would override a market-based system, in which companies choose what type and when to develop solutions responsive to a market demand; and, the market, in turn, evaluates the worth of the product and which to buy.

The proposed rule risks inadvertently disrupting natural market forces, which will lead to the creation of an environment where only a handful of health IT developers survive, compelled to spend their energy on regulatory compliance, API creation, and pursuing patents. It is unlikely that possible new entrants will be interested in the healthcare space if their profits are starkly limited and their hard work in bringing emerging technologies to market is to be met with immediate exposure of their intellectual property (IP) to other interested parties; also, it will have a chilling effect within the companies already serving this market.

The proposed requirement to limit companies' ability to charge fees beyond cost recovery devalues the work of software developers, increases recordkeeping burden, and disincentivizes efforts to improve efficiency. If the goal is to reduce costs and expand interoperability, ONC must engage not only EHR developers to facilitate data exchange, but registries and other stakeholders who frequently do not use recognized standards and thus contribute measurably to the costs providers must pay to exchange information.

We note that there are implications throughout the proposed rule that EHR developers currently in the industry are incapable of innovation. That is an inaccurate characterization that trivializes the work that companies in our Association do every day to reduce clinician burden and increase patient access to and use of his/her own health information.

The breadth of the proposed rule and the complexities woven throughout--along with the numerous interdependencies and occasional conflicts with other Federal or State programs and well-intended, but confusing or not thoroughly explored implications of some of the proposals--create a regulatory burden.

Unrealistic timeline

Developing and implementing software takes time, from the time EHR developers spend in designing workflows, writing code, and performing extensive testing, to the time spent by healthcare organizations installing, customizing, and educating their users on the new workflows and expectations.

Data from a survey of EHR Association members (see development burden estimates on pgs. 5-7) shows that the proposed rule severely underestimates the development time required for its many components. Every hour spent on these projects is an hour not spent on software and usability enhancements requested by our clients.

The Association recognizes the desire to move quickly, and we don't believe it's in the interest of the healthcare industry or necessary to postpone all aspects of the proposed rule. We suggest that two proposed criteria--updates to e-prescribing and USCDI APIs--could be priority areas reasonable for the proposed timeframes. To achieve those in 24 months, other criteria will need to be deferred to a longer timeline or reprioritized in the upcoming years.

Additionally, we have concerns about how this timeframe will intersect and potentially conflict with other CMS and ONC programmatic requirements. It will be important to ensure timelines in the proposed rule remain feasible in conjunction with other priorities.

Use of ambiguous language that would challenge planning and compliance for developers and providers

ONC indicates that its goal in this rule is to be "clear, predictable, and administrable" in order to avoid undue burden on stakeholders. This is an important goal that EHR Association members strongly support. Vague or ambiguous regulatory language poses risk to affected stakeholders, especially where maximum penalties are as high as $1 million per incident.

However, much of the proposed language is drafted with room for interpretation, using words like "reasonable" and "as soon as possible" throughout the proposed rule. We make three suggestions to address this concern:

1. ONC should address as much ambiguity as possible in a final rule. To ensure this is achieved, EHR Association members suggest a second round of public comment to aid in further clarification. Because of the vague language, as well as several other elements within the Exceptions section that we anticipate will cause significant market confusion, the industry will need *many* more examples to be included in the final rule for us to have confidence in accurate interpretation. At that point, we will need an opportunity to then provide feedback on those examples before any structure is finalized.

2. After the final rule, an ongoing process for clarification needs to be established where actors can anonymously request authoritative guidance from ONC or OIG on whether a practice implicates information blocking. The guidance should be public so that all stakeholders can benefit from this information.

3. A time period of enforcement discretion should be established for this necessary guidance to be propagated and for claims to be investigated in an educational manner, without financial penalties.

While we comment below in significantly more detail, EHR Association members note that there are several components of the Exceptions section as proposed that do not seem enforceable, either because of ambiguity, difficulty tracking, or the availability of resources within ONC and OIG.

Further, we recognize that the FTC/OIG dual jurisdiction will likely cause confusion; in the main, all affected stakeholders at risk of prosecution will need much more guidance to help them understand many of the details of jurisdiction, intended processes, and more.

EHR Association members appreciate ONC's continuing efforts to move the nation's healthcare system toward improved patient care. Thank you for this opportunity to provide our input. We welcome additional opportunities to share our expertise as this initiative moves forward.

Sincerely,

Cherie Holmes-Henry

Sasha TerMaat

Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Sasha TerMaat
Vice Chair, EHR Association
Epic

HIMSS EHR Association Executive Committee

Dal J Bucciferro

David J. Bucciferro
Foothold Technology

Hans J. Buitendijk
Cerner Corporation

Barbara Hobbs

Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
Evident

Emily Richmond

Emily Richmond, MPH
Allscripts/Practice Fusion

Courtney E Tesvich

Courtney E. Tesvich, RN
Nextech

EHR Association Development Burden Estimates

Development effort: The EHR Association conducted a survey of its members (developers of certified health IT) to assess the development effort required for projects identified in the ONC Proposed Rule. Averages were calculated and are presented in the table below.

Cost savings: The EHR Association did not conduct a member survey to approximate the cost savings that ONC estimates. ONC's estimated savings seem high, based on our experience.

Development Burden Estimates

Project	ONC Estimate (hours)	EHRA Average Estimate (hours) Per Developer	EHRA Average Estimate (hours) Per Product	EHRA Project Size
USCDI updates for clinical notes	1,900-4,800	11,000	3,000	Large
USCDI updates for provenance		33,000	11,300	Massive
USCDI updates for pediatric vitals		1,300	500	Medium
USCDI patient address and phone number		1,400	400	Medium
Unique Device Identifier IG Update	Not estimated	2,500	900	Medium
Medication data request for comment	Not estimated	1,000	200	Small
EHI Export	320-3,200			
Patient Use Case		39,000	14,300	Massive
System Transition Use Case		19,000	5,900	Massive
Encrypted authentication credentials	Not estimated	300	100	Small
Multi-factor authentication	Not estimated	1,800	600	Medium
E-Prescribing Updates	Not estimated			Massive
New Rx		700	200	
New RxRequest		2,000	600	
New RxResponseDenied		2,000	600	
RxChangeRequest		400	100	
RxChangeResponse		400	100	
CancelRx		400	100	
CancelRxRseponse		400	100	
RxRenewalRequest		400	100	
RxRenewalResponse		400	100	

Development Burden Estimates

Project	ONC Estimate (hours)	EHRA Average Estimate (hours) Per Developer	EHRA Average Estimate (hours) Per Product	EHRA Project Size
RxFill		400	100	
RxFillInidcatorChange		1,600	500	
RxHistoryRequest		400	100	
RxHistoryResponse		500	100	
GetMessage		400	100	
Status		400	100	
Error		400	100	
Verify		400	100	
Resupply		2,400	500	
DrugAdministration		2,100	600	
Recertification		2,200	600	
RxTransferRequest		1,800	400	
RxTransferResponse		1,800	400	
RxTransferConfirm		1,800	400	
REMSInitiationRequest		1,800	500	
REMSInitiationResponse		1,800	500	
REMSRequest		1,800	500	
REMSResponse		1,800	500	
Include diagnosis element in DRU segment		1,400	400	
Include diagnosis element in SIG segment		2,100	700	
DS4P and Consent Management	3,000-6,000	19,000	6,100	Massive
Adopt FHIR DSTU2		1,800	500	Medium
Adopt FHIR R4		2,500	900	Medium
ARCH	1,500-3,500			Massive
AllergyIntolerance		1,300	400	
CarePlan		1,900	600	
Condition		1,300	400	

Development Burden Estimates

Project	ONC Estimate (hours)	EHRA Average Estimate (hours) Per Developer	EHRA Average Estimate (hours) Per Product	EHRA Project Size
Device		1,300	400	🟥
DiagnosticReport		1,500	500	
Goal		2,000	600	
Immunization		1,300	400	
Medication		1,300	400	🟥
MedicationOrder		1,500	500	
MedicationStatement		1,500	500	🟥
Observation		2,000	700	
Patient		1,200	400	
Procedure		1,300	400	
Provenance		2,000	600	
DocumentReference		2,000	700	🟥
OpenID Connect Core 1.0		1,700	500	
SMART Guide		1,600	500	🟥
Refresh tokens		1,400	400	
Population Level Use Cases		2,900	900	
Search Support		3,200	700	
Application Registration and Documentation	1,000-2,500	2,200	700	Medium
Real World Testing	1,140	12,000	3,400	Large

Office of the National Coordinator for Health IT
Proposed Rule Public Comment Template

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

Please Note: Sections where the EHR Association did not provide comment were removed for brevity.

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:

The EHR Association is supportive of removing the identified randomized surveillance requirements. We agree with ONC's assessment that randomized surveillance creates burden on participating providers.

Because ONC proposes that the ONC-ACBs may still conduct randomized surveillance, ONC should not remove the prohibition in (c)(6) on selecting a certified health IT module for randomized surveillance more than once during any consecutive 12 month period. Repeated randomized surveillance would continue to be burdensome.

Removal of the 2014 Edition from the Code of Federal Regulations

We propose to remove the 2014 Edition certification criteria (§ 170.314) and related standards, terms, and requirements from the rule.

Preamble FR Citation: 84 FR 7434-35 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7563-64 for estimates related to the removal of the 2014 Edition from the Code of Federal Regulations.

Public Comment Field:

The EHR Association is supportive of sunsetting the 2014 Edition criteria.

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:

The EHR Association supports removing unnecessary certification criteria and focusing certification criteria on interoperability. For example, we agree that the incorporation of problems, medications, allergies, and smoking status into USCDI means separate certification criteria are not necessary. We also agree CCDS is replaced with USCDI and is no longer necessary.

With the removal of some criteria and other changes ONC proposes to introduce to the ONC 2015 Edition, clarity of communication in requirements and on the CHPL will be critical. We suggest that it will be most clear to certification stakeholders if a separate, updated certification is introduced, rather than revising the ONC 2015 Edition. This will help our EHR customers understand the differences between the ONC 2015 Edition that they have already adopted and future requirements, for example.

Removal of Certain ONC Health IT Certification Program Requirements

We propose to remove the following ONC Health IT Certification Program requirements at § 170.523:

- Limitations disclosures
- Transparency and mandatory disclosures requirements

Preamble FR Citation: 84 FR 7437-38 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7566-67 for estimates related to this proposal.

Public Comment Field:

The EHR Association is supportive of removing these requirements.

Recognition of Food and Drug Administration Processes

We propose to establish processes that would provide health IT developers that can document successful certification under the Food and Drug Administration (FDA) Software Pre-Certification Pilot Program with exemptions to the ONC Health IT Certification Programs requirements for testing and certification of its health IT to the 2015 Edition "quality management systems" criterion and the 2015 Edition "safety-enhanced design" criterion, as these criteria are applicable to the health IT developer's health IT presented for certification. We also believe that such a "recognition" could be applicable to the functionally-based 2015 Edition ''clinical'' certification criteria.

Preamble FR Citation: 84 FR 7438-39 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The EHR Association feels that the applicability of this recognition would be limited, applying to only a very small percentage of health IT developers. If such a proposal is considered in more detail, we would be happy to consult on specifics.

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 and 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:

If such a proposal is considered in more detail, EHR Association members would be happy to consult on specifics.

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:

The EHR Association supports adopting the USCDI in place of the existing CCDS. In particular, because the USCDI data set is defined so precisely, along with mechanisms for exchanging it among cooperating entities (FHIR/ARCH), it creates a useful bright line to determine if key information has indeed been "blocked." Generally, we suggest that Conditions of Certification and Information Blocking obligations be considered as met if the USCDI data set is available or exchanged, given the challenges with broader and less clearly specified definitions such as EHI.

Providing a progressive and predictable glidepath to data in scope for APIs and documents will enable both health IT developers and providers to innovate and plan their support for that data set.

We offer the following comments, questions, and suggestions to improve on the clarity of the proposals and/or the industry's ability to achieve the objectives.

New Data Elements in USCDI
EHR supports adding the new data elements for address and phone number.

However, EHR Association members believe the pediatric vital sign data elements should be optional rather than required, as was proposed. There are a number of specialty EHRs used by providers who never see children. Including pediatric vital signs in those systems would be resource intensive for functionality that would never be used.

API Resource Collection in Health (ARCH)
ONC introduces the concept of ARCH. The EHR Association believes that the purpose of ARCH is to define the FHIR resources that would represent the USCDI, and thus the scope within HL7 ® FHIR® US

Core, with any additional implementation guidance that would not yet be in HL7 FHIR US Core. We request this be clarified in the description of ARCH.

Also, we understand that ONC intends to enable sub-regulatory updates to ARCH through the Software Version Adoption Process (SVAP). It would be helpful to provide versioning of ARCH to avoid confusion as new versions are introduced through SVAP or as a new floor is set through a certification program update.

We are concerned that ARCH did not go through typical implementation guide review processes such as HL7's ballot cycle. Given the scope, such a rigorous approach may not be necessary, but we suggest that any updates to ARCH would follow the proposed SVAP review processes, and be subject to a review opportunity.

If ARCH is not intended to follow the SVAP process, we strongly urge ONC to remove ARCH and reference FHIR US Core directly to ensure proper review can be ensured.

We appreciate the focus on read access at this stage, while considering the ability to support write at a later point. Introduction of write access would be a large scope change inappropriate for SVAP. It would require careful consideration and scoping as data integrity will become a paramount concern.

Provenance

EHR Association members suggest inclusion of provenance in USCDI be deferred until necessary implementation guidance is provided. This will avoid varying implementations and necessary re-work when standard guidance becomes available.

We do want to emphasize that we support the introduction of the provenance data class through USCDI to improve on the ability to recognize the source of the data, enable appropriate interpretation of that data, and improve trustworthiness and reliability of the data being exchanged. Additionally, provenance data can be used to disambiguate/de-duplicate data that is exchanged among various stakeholders.\

After the initial three proposed data elements of provenance have been sufficiently defined and adopted, we see value in investigating other types of provenance data, including:

- Source
- context categorization
- specialization of the author
- unique identifiers

We expect that the provenance data class will evolve over time as we gain experience on how to best use and manage the various data flows and support the intended purposes.

It will be important that ONC provide clarity around the valuation and use of provenance data to ensure consistency. HL7 started a project (https://www.hl7.org/fhir/provenance.html) to address how to best use provenance data in both C-CDA and FHIR, and we expect that the guidance will be propagated to other standards as well, considering that the source data might have been received over a different initial transmission standard. However, the guidance is not yet available.

Guidance must address critical questions such as how to identify the author and the author's organization. Author is defined as "responsible entity" and yet who the responsible entity is for each data class in USCDI is not unambiguously clear.

For example, consider a patient telling a medical assistant (MA) they are allergic to aspirin. Between the original provider who diagnosed the allergy, the patient who reported it, the MA who entered the data, and the provider who signs and bills for the visit, it is ambiguous which is the "responsible entity." Clarity must be provided on each data class to resolve such questions.

Given the variety of authors, NPI may not be enough, yet it will be important to use globally unique identifiers whenever possible to achieve the desired objective of unambiguously establishing provenance. Guidance should address cases such as unknown or multiple authors or organizations.

Given these critical questions and work in progress, we recommend that provenance data elements are not included at this time, and that USCDI adopt provenance as a data class once guidance becomes available.

USCDI Progression

The SVAP is generally proposed to enable upgrade to more current versions of a standard in an established area. However, since USCDI has not gone through the standards-creation and balloting process, it is not clear whether expansion of the USCDI would be managed through the SVAP or the Program, i.e., requiring a change to the (conditions of) certification rules. We suggest that any expansion of the USCDI over time is done through certification program updates rather than through SVAP, to synchronize updates across all stakeholders at the same time. This would align with our suggestion for ARCH above.

Encounter Data Class

HL7 CDA C-CDA documents currently contain an encounter section. To create alignment between HL7 CDA C-CDA and HL7 FHIR, we recommend an Encounter data class be added to USCDI v1 and included in ARCH. The Encounter resource should contain date and time of the encounter, the service provider (organization), location, and relevant clinicians, as is already required in the HL7 C-CDA Encounter section. Inclusion will further aid in providing encounter- and episode of care-based data exchange.

Data Stratification

As the USCDI grows to cover the entire designated record set and eventually all electronic health information, it will be increasingly common that not all health IT being certified needs to support all USCDI data classes. EHR Association members suggest clear stratification of USCDI as to what data classes should be supported based on setting, specialty, or stakeholder role (e.g., payer vs. provider).

Also, we urge ONC to work with SDOs to ensure implementation guides are aligned with and sensitive to this stratification as to not impose undue requirements on health IT that do not otherwise apply. Current examples would include pediatric vitals that not all health IT would need to capture, or implantable devices that not every setting (such as behavioral health) needs to support in full, as the current implementation guides would require.

Additionally, anticipated inclusion of claims and other financial or administrative data in USCDI may result in some data classes applicable to payers and their health IT, but not providers and their health IT.

Updated Versions of Vocabulary Standard Code Sets

We propose that the USCDI Version 1 (USCDI v1) include the newest versions of the "minimum standard" code sets included in the CCDS available at publication of a subsequent final rule. We request comment on this proposal and on whether this could result in any interoperability concerns. To note, criteria such as the 2015 Edition "family health history" criterion (§ 170.315(a)(12)), the 2015 Edition "transmission to immunization registries" criterion (§ 170.315(f)(1)), and the 2015 Edition "transmission to public health agencies—syndromic surveillance" criterion (§ 170.315(f)(2)) reference "minimum standard" code sets; however, we are considering changing the certification baseline versions of the code set for these criteria from the versions adopted in the 2015 Edition final rule to ensure complete interoperability alignment. We welcome comment on whether we should adopt such an approach.

Preamble FR Citation: 84 FR 7441 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The EHR Association is in agreement with using the upgraded version of the vocabulary code sets should the USCDI be adopted.

Unique Device Identifier (UDI) for a Patient's Implantable Devices: CDA Implementation Guide

The recently published Health Level 7 (HL7®) CDA R2 Implementation Guide: C-CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1-US Realm identifies changes needed to the C-CDA to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. We request comment on whether we should add this recently published UDI IG as a requirement for health IT in order to meet the requirements for UDI USCDI Data Class. In addition, we do not have a reliable basis on which to estimate how much it would cost to meet the requirements outlined in the UDI IG; and, therefore, we request comment on the cost and burden of complying with this proposed requirement.

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The reference to the HL7 UDI guidance document does not reflect the official name of the published document. The reference should be to the HL7 Cross Paradigm Implementation Guide: UDI Pattern, Release 1 document. This guidance covers HL7® v2, HL7 CDA®, and HL7 FHIR®, but does not cover HL7 CDA C-CDA. The guidance on how to address UDI in a C-CDA is here: HL7 CDA® R2 Implementation Guide: C-CDA Supplemental Templates for Unique Device Identifier (UDI) for Implantable Medical Devices, Release 1 - US Realm and should also be referenced in the rule for completeness.

The UDI Pattern guidance section for FHIR is based on FHIR STU 3. When FHIR R4 is referenced in the rule, as we suggest elsewhere, the upcoming UDI Pattern R2 document (recently balloted in the HL7 May 2019 ballot, now being reconciled and to be published) will need to reflect the updated guidance for FHIR R4. We urge ONC to work with HL7 to help ensure that version is available as soon as FHIR R4 is being referenced for certification purposes.

Not all health IT interested in certification may need to support documentation of implantable devices based on the targeted setting, specialty, and/or stakeholders to the extent that the current C-CDA and FHIR US Core guidance would require. For example, EHRs focused on behavioral health would not be able to fully record such data as they are not the originator of the data. At most they may have information passed to them, or from the patient some general information. The latest FHIR US Core implementation guide does not support a more general Device profile that would soften the UDI elements that must be supported.

As USCDI expands to cover more data classes that not all EHR/HIT need to support, we suggest clear stratification of USCDI as to what data class should be supported based at least on setting, specialty, or stakeholder (e.g., payer vs. provider).

Medication Data Request for Comment

The USCDI v1 "Medication" data class includes two constituent data elements within it: Medications and Medication Allergies. With respect to the latter, Medication Allergies, we request comment on an alternative approach. This alternative would result in removing the Medication Allergies data element from the Medication data class and creating a new data class titled, "Substance Reactions," which would be meant to be inclusive of "Medication Allergies." The new "Substance Reactions" data class would include the following data elements: "Substance" and "Reaction," and include SNOMED CT as an additional applicable standard for non-medication substances.

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The EHR Association supports the proposal to replace the CCDS Medication Allergy data class in USCDI V1 with a Substance Reactions data class, which then aligns through ARCH with the FHIR AllergyIntolerance resource and in C-CDA aligns with the Allergies and Intolerances section.

§ 170.205(a) Patient summary record

We propose to adopt the HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 1 C-CDA Companion Guide to support best practice implementation of USCDI v1 data classes and enhance the implementation of other 2015 Edition certification criteria that also reference Consolidated Clinical Document Architecture (C-CDA) Release 2.1 (§ 170.205(a)(4)). Those criteria include:

- "transitions of care" (§ 170.315(b)(1));
- "clinical information reconciliation and incorporation" (§ 170.315(b)(2));
- "care plan" (§ 170.315(b)(9));
- "view, download, and transmit to 3rd party" (§ 170.315(e)(1));
- "consolidated CDA creation performance" (§ 170.315(g)(6)); and
- "application access – all data request" (§ 170.315(g)(9)).

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

ONC proposes to include clinical notes as part of USCDI V1. EHR Association members note that HL7 established guidance in the C-CDA Companion Guide, while Argonaut is embarking on providing guidance on how these are to be addressed in HL7 FHIR. Additionally, Commonwell and Carequality collaborated on a set of templates for HL7 CDA C-CDA document types to improve on better capturing narrative notes/summaries for inpatient and outpatient encounters (http://www.commonwellalliance.org/wp-content/uploads/2018/07/Carequality_CommonWell_Improve_C-CDA_06-15-2018_V1.pdf), specifically an Inpatient/Hospital Summary template based on the HL7 CDA C-CDA Discharge Summary document type and an Outpatient/Ambulatory Summary template based on the HL7 CDA C-CDA Progress Notes document type.

Clinical notes in a C-CDA can be expressed in three different ways:

- As a document that includes structured and narrative data sections.
- As a document that primarily focuses on the narrative clinician notes with perhaps some accompanying structured data.
- As a section in a larger C-CDA encounter summary or other document

As the term "clinical notes" can apply to either, the term should be used with caution and the intent of what gaps in "clinical notes" are being addressed should be clearly and carefully defined.

This classification concern is made even worse in FHIR, since no published implementation guidance yet exists and resources to represent note information are not yet mature enough for adoption. The list of eight proposed clinical note types may be interpreted as HL7 C-CDA document types, while in HL7 FHIR documents they would not yet be covered through the resources listed in ARCH other than as Document Reference enabling a reference to a clinical note, which then could be a C-CDA document. Consequently, the intent is not clear. Therefore, we have the following questions.

- Is ONC proposing:
  - Option A: 8 HL7 C-CDA document types, each represented by a DocumentReference resource?
  - Option B: 8 clinical note fragments that will be added to an existing C-CDA section?
  - Option C: 8 clinical note fragments that will be added to a newly defined C-CDA section, called "Notes"?

We suggest option B or C, with notes sections included in the C-CDA document types currently within the scope of the ONC 2015 Edition and notes using FHIR resources.

- Adopting option B or C would permit the immediate use of the joint Commonwell/Carequality clinical note template definitions of types Progress Note and Discharge Summary, without requiring SVAP approval.
- The Progress Notes document type is not currently named as a required document type to support. However, to enable support for the Commonwell/Carequality Outpatient/Ambulatory Summary template, Progress Notes should be added to the list of certified document types together with the CCD, Referral Note, and Discharge Summary C-CDA document templates named in current 2015 Edition criteria.
- We note that the HL7 C-CDA CCD and Referral Note document types were not listed. We suggest ONC clarify that these document types remain part of the certification criteria.
- We are concerned with the proposed Laboratory Report Narrative, Pathology Report Narrative, and Imaging Narrative. These are not referenced in HL7 C-CDA R2.1 nor the Companion Guide R1 as either document types or note types. Only one seems to potentially be an HL7 C-CDA document type: Diagnostic Imaging Report. We seek clarification which specifications are intended to be used for a Laboratory Report Narrative and a Pathology Report Narrative. We note that the referenced wiki would be insufficient as that only represents a proposal, not a published, balloted document. We suggest that these three note types not be required for EHRs to create as they represent specialized reports that would be created by a Laboratory or Imaging Center. However, an EHR may receive and store such documents.
- ONC should clarify that only the HL7 C-CDA CCD be required to demonstrate it can include all USCDI, while any other document type only needs to be certified to the sections/entries identified in the HL7 CDA C-CDA R2.1 implementation guide for the respective document types, while any actual document generated is fit for purpose, thus may include more or less than the USCDI classes.
- We seek clarification that where the proposal indicates that clinical notes text cannot be included in an API resource as “e.g., .docx or .pdf…” that using a C-CDA representation is

permissible.

As we progress to introduce narrative notes into the appropriate documents and sections, we would like to raise the following concerns on how best to right-size documents. Communications sent in different contexts might merit different quantities of notes to be included, for example. We are concerned about how these decisions might impact C-CDA bloat and that the downstream effects of those decisions have not been fully thought out.

Therefore, EHR Association members recommend that while certification focuses on the ability to include these notes in various document types, there will not be a requirement to include all notes always. Finding the right balance and context will be a learning evolution; and, therefore, the absence of certain notes in specific documents not be grounds in itself for information blocking challenges either.

§ 170.205(b) Electronic prescribing

* * *

(1) Standard. National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 (incorporated by reference in § 170.299).

Preamble FR Citation: 84 FR 7444 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The EHR Association appreciates the inclusion of NCPDP SCRIPT 2017071 as the target for e-Prescribing, thus harmonizing with CMS' Medicare Part D rules already in effect aiming for a January 1, 2020 adoption, while eventually removing NCPDP SCRIPT 10.6. However, to allow for flexibility as CMS rolls out, we suggest that ONC define a reference to CMS' actual dates in the Medicare Part D rules and continue to keep support for SCRIPT 10.6 during the transition, but certainly until January 1, 2020, if ONC's final rule comes out before then.

We note that in prior certification testing there was a discrepancy between the NCPDP standard referenced by ONC and the implementation guide Surescripts used to certify network participants. We appreciate the work done by NCPDP to address those challenges, resulting in a complete package that everyone is working to support without developing additional, conflicting implementation guidance. The link in the proposed rule requires navigation to get to the proper page and package. We suggest that ONC work with NCPDP to include a direct URL to the right package to ensure the right set of documentation is used for implementation.

We appreciate ONC's recognition that operational deployment with Surescripts can be used toward satisfying real world testing requirements, and we ask that ONC work with Surescripts and others so that the ONC certification can be used toward those networks' certification requirements.

§ 170.315(b)(11) Electronic prescribing

Included in 2015 Edition Base EHR Definition? *No*

Electronic prescribing.

(i) Enable a user to perform all of the following prescription-related electronic transactions in accordance with the standard specified in § 170.205(b)(1) and, at a minimum, the version of the standard specified in § 170.207(d)(3) as follows:

(A) Ask mailbox (GetMessage).

(B) Relay acceptance of transaction (Status).

(C) Error response (Error).

(D) Create new prescriptions (NewRx, NewRxRequest, NewRxResponseDenied).

(E) Change prescriptions (RxChangeRequest, RxChangeResponse).

(F) Renew prescriptions (RxRenewalRequest, RxRenewalResponse).

(G) Resupply (Resupply).

(H) Return receipt (Verify)

(I) Cancel prescriptions (CancelRx, CancelRxResponse).

(J) Receive fill status notifications (RxFill, RxFillIndicatorChange).

(K) Drug administration (DrugAdministration).

(L) Transfer (RxTransferRequest, RxTransferResponse, RxTransferConfirm).

(M) Recertify (Recertification).

(N) Request and receive medication history (RxHistoryRequest, RxHistoryResponse).

(O) Complete risk evaluation and mitigation strategy transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse).

(ii) For each transaction listed in paragraph (b)(11)(i) of this section, the technology must be able to receive and transmit the reason for the prescription using the diagnosis elements in DRU Segment.

(iii) *Optional*. For each transaction listed in paragraph (b)(11)(i) of this section, the technology must be able to receive and transmit the reason for the prescription using the indication elements in the SIG Segment.

(iv) Limit a user's ability to prescribe all oral liquid medications in only metric standard units of mL (i.e., not cc).

(v) Always insert leading zeroes before the decimal point for amounts less than one and must not allow trailing zeroes after a decimal point when a user prescribes medications.

Preamble FR Citation: 84 FR 7444-45 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The EHR Association notes that the proposed rule includes 13 additional interactions, compared to those that CMS adopted in the Medicare Part D final rule to be implemented starting January 1, 2020. These are:

- NewRxRequest
- NewRxResponseDenied
- RxFillIndicatorChange
- Resupply, DrugAdministration
- RxTransferRequest
- RxTransferResponse
- RxTransferConfirm
- REMSInitiationRequest
- REMInitiationResponse
- REMSRequest
- REMSResponse

We are concerned that through this rulemaking, EHRs are required to support these new transactions, but pharmacy systems on the receiving end of these transactions are not, thus potentially leading to capabilities that are implemented but not deployed into production. We suggest removing these--or making them optional--from the certification criteria, and for ONC, CMS, and the industry to align on a future implementation once it is clear all parties would implement these and the value is established.

In addition, some of the transactions listed above would never be relevant for the scope of all health IT modules. For example, DrugAdministration is a transaction for a long term care setting and would never be needed in an ambulatory EHR. Similarly, RxTransferRequest is a pharmacy-to-pharmacy transaction that would not be needed in any EHR. ONC needs to ensure certification is flexible enough to allow health IT modules to certify only to the transactions applicable to their domains and only to include transactions that are ready for widespread adoption in the next few months.

§ 170.205(h) Clinical quality measure data import, export and reporting

* * *

(3) CMS Implementation Guide for Quality Reporting Document Architecture Category I Hospital Quality Reporting 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 EHR Association agrees with the proposal to remove the HL7 QRDA standard requirements from the 2015 Edition CQMs, but require that health IT certified to the criterion support the CMS QRDA IGs. This proposal will reduce the certification burden; however, adjustments are needed in two areas:

1. Implementation guides should only be used in certification in their intended context--i.e, hospital implementation guides for hospital quality measures and ambulatory implementation guides for ambulatory quality measures. Certifying ambulatory quality measures for QRDA I to a hospital implementation guide is not effective and will interfere with the use case of using ambulatory QRDA I to combine data between systems.

2. Products designed for only one care setting should be able to only certify to its relevant quality measures and implementation guides. For example, an ambulatory EHR should not be required to certify using the Hospital IG, and conversely, an inpatient EHR should not be required to certify using the EP/EC IG.

EHR Association members urge ONC to ensure that they put time and consideration into testing before requiring FHIR-enabled APIs to replace or complement QRDA reports for quality reporting and improvement, as well as provide a timetable for implementation.

The Association agrees with the proposal to adopt the latest CMS QRDA IGs at the time of final rule publication, as CMS updates their QRDA IGs annually to support the latest eCQM specifications and only accepts eCQM reporting to the latest version. Supporting multiple versions of IGs is inconvenient.

§ 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:

Please see comments above.

§ 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:

Please see comments above.

§ 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:

The EHR Association does not recommend that this criterion become part of the Base EHR definition. This criterion is too complex with too many unanswered questions to make certification to this criterion viable within the current timeframe expectation of 24 months from publishing of the final rule.

In light of the proposed rule indicating that new processes such as APIs could make this function obsolete, we question the importance of prioritizing the modification of this criterion. Our fear is that EHR developers will undertake significant development work to obtain certification, only for that work to later be discarded. The development for what is proposed is significant, as shown by our estimates and described below.

There is tremendous concern that the identification of all data and provision of a data dictionary to support a vendor's database will be an enormous task with variance in the amount of data provided. Expectations that this export include all maintained data could produce a volume of information that exceeds the importing system's capability. With the ever-expanding data elements required for capture in the system, the maintenance to keep this export current would be continuous. No criteria currently exists regarding administrative or billing data, so including this type of data feels like an overreach.

Instead, we propose a modification of scope that builds upon other requirements and existing standards toward ONC's envisioned future state, which we elaborate upon below. We suggest that (b)(6) Data Export be modified to include USCDI. That would expand currently available export abilities in alignment with the standards.

If this proposal moves forward, we would like to share the following considerations.

1. There is too much ambiguity over the definition of "all EHI." The effort to export data based on an entire database, which includes clinical, administrative, and claims/billing data, as well as any data stored in separate data warehouses that the system has access to, can produce, and electronically manage, cannot be overstated.

   The scope of the current proposal begins with "all data." It would be more practical to begin utilizing the USCDI. Support of interoperability would be best done by focusing on those data elements defined by the USCDI v2.

2. The EHR Association is concerned that continuing to invest in a standards-agnostic approach that would not yield any improvements in the ability to transfer data with less effort would make this essentially an orphan criterion; CEHRT would have expanded documentation, but the corresponding receive/ingest criterion could not be established given the wide range of formats to support, including still having to address client-specific variations that cannot be documented upfront. Focusing on USCDI for export will make a corresponding focus on import and eventual incorporation of data feasible, increasing the value of interoperability.

3. The phrase "near real-time" is ambiguous and unrealistic. Any specific timing expectations must be clearly defined, in both this criterion and any other certification expectations. Timely execution depends upon a number of factors which may be beyond the EHR developer's control, such as capacity of a client's hardware, volume of data, etc. Our interpretation of timeliness leaves a lot of flexibility as to account for these unpredictable factors, and we have concerns that our expectations may differ from ONC's.

   For example, this data export is significantly different than export of CQM data and, therefore, would not and should not be held to the same standards. As we have expressed to ONC in the past, we do not see the export of CQM data in near real-time as recognizing real-world constraints of hardware and system architecture either.

4. Health IT systems should be provided flexibility on how to construct exports of any required data outside of USCDI. They should not be required to permit patients to request or receive an export without provider intervention (though of course, if some systems choose to have such a feature that would be fine).

5. If assistance to third party developers for exporting or using an export is necessary beyond USCDI and the documentation requirements of certification, the health IT developer should be able to charge for this expert assistance at standard rates. The financial burden of free expert advice has not been sufficiently analyzed within the proposed rule.

6. ONC requests input on whether support for specific time-frame constraints on EHI should be required. There are existing criteria in the 2015 Edition Certification program that have timeframe elements such as "specific date" and "date range" that have proven problematic for the ONC to define in a manner to which EHR developers can appropriately code functionality. For example, natural boundaries in healthcare (such as an admission) might not align with an arbitrary selected timeframe. We are concerned that setting up similar timeframe requirements to this criterion would be just as problematic, if not more so given the volume of data.

As stated above, we are concerned with the ambiguities introduced using the terms "all EHI" and "commercially reasonable format." Based on the current 2015 Certification Edition, support is already in place using the HL7 CDA C-CDA CCD, while typical EHRs do provider data export capabilities in support of data migrations to a different EHR. The latter is frequently tailored to individual provider needs depending on the target EHR and the suitability of the data to populate the target EHR.

Considering the variety in vocabulary used, limited use of industry standard vocabulary, particular in older data sets being migrated, and the variety in data representations, this is expected to remain a labor-intensive effort until we can arrive at a standards-based migration. The proposed technical specifications would not enable another party to perform such migrations until we have arrived at a common standard for such migrations.

We suggest that a more practical approach would be that the EHI export begins to build on the USCDI using the bulk data capabilities included in HL7 FHIR R4 to enable export of multiple patients asynchronously. This will start to harmonize the data formats and vocabularies used for both export and import.

Similarly, for patient-focused EHI export, we suggest building on the USCDI FHIR based exchange where it can include a HL7 CDA C-CDA CCD for data not yet available in a FHIR-based format. Taking this approach, we can focus attention on expanding USCDI rather than on interim approaches that are expected to be replaced in the near/mid-term.

§ 170.315(d)(12) Encrypt authentication credentials

Included in 2015 Edition Base EHR Definition? *No*

Encrypt authentication credentials. Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations:

(i) "Yes." Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) "No." Health IT Module does not encrypt stored authentication credentials.

Preamble FR Citation: 84 FR 7450 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.

Public Comment Field:

The EHR Association supports ONC's efforts to encourage encryption of credentials to protect accounts with healthcare software. We have several concerns around the proposed certification criterion question, "encrypt authentication credentials."

First, we seek clarification on the definition of "authentication credentials." Authentication can be performed at multiple levels through a variety of means using several types of authentication methods. A user-level authentication can utilize individual passwords, biometric data, parameters used by multi-factor authentication (MFA) methods (such as TOTP), and certificates (such as in WebAuthn). Authentication can also occur between servers or systems using pre-shared secrets, API keys, security tokens, asymmetric keys, and certificates. The answer to whether authentication credentials are encrypted will have different meanings depending on how the respondent defines "authentication credentials." To have a fair representation of developer practices when handling authentication credentials, we recommend a more clear definition of what would be in scope. We recommend a starting scope of natural person user-level authentication credentials for introducing this criterion.

Second, while the proposed rule specifies encryption or hashing using FIPS 140-2 algorithms, it is unclear at what level those algorithms can be applied to qualify as an appropriate "yes" response to the proposed criterion. Encryption can be applied at the field level such as encrypting the field containing a user's password; database level, where all fields are encrypted whether they are authentication credentials or not; and the disk level, where all disk contents, including databases containing credentials, are encrypted at rest. The level at which data is encrypted affects the types of threats the encryption protects against. It is unclear at what levels of encryption ONC intends as meeting the proposed certification criterion. Without clarification, individual respondents may interpret differently what levels of encryption are satisfactory for a 'yes' response to the proposed certification criterion.

Additionally, the criterion question is proposed to apply to all certified versions of the software. We recommend that the proposed criterion question be required for new software going through certification and not be applied to versions already certified. Healthcare organizations looking to procure a healthcare IT solution will find the most value in using the developer's latest version of their products, as newer versions often offer additional features. Keeping software up-to-date is also important for security as older versions may not have security fixes available in newer versions.

If the criterion is applied to prior versions, it is possible that a health IT developer's answer to the criterion question might be 'no' for a prior version while being "yes" for more recent versions. Healthcare organizations using an older version of the software where credentials are not encrypted may be put at an increased security risk by publicizing the software's lack of credential encryption. Requiring this criterion for new certifications adds transparency to healthcare organizations evaluating the selection of software while still encouraging health IT developers to encrypt credentials in their software.

§ 170.315(d)(13) Multi-factor authentication

Included in 2015 Edition Base EHR Definition? *No*

Multi-factor authentication. Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations:

(i) "Yes." Health IT Module supports authentication through multiple elements the identity of the user with industry recognized standards.

(ii) "No." Health IT Module does not support authentication through multiple elements the identity of the user with industry recognized standards.

Preamble FR Citation: 84 FR 7450-51 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.

Public Comment Field:

EHRA supports ONC's effort to bring attention to multi-factor authentication, as protecting user accounts is critical to protecting patient information. Understanding a healthcare IT developer's MFA capabilities can be complex and we encourage allowing health IT developers to attest in a way that provides for clarity around what is supported.

EHRA notes that health IT developers often have suites of software products with differing authentication needs, capabilities, and audiences. Some aspects of a developer's system may not have use for MFA, such as a surgical waiting room status board display meant to be public, where display of sensitive information is limited by the application's design. Other products may be designed for use in locations where physical considerations make MFA infeasible, such as in an operating room where authentication devices may pose an infection risk. Other products within a developer's suite may have different capabilities for MFA based both on the underlying technology. A desktop application and a web application have different levels of access to hardware based authentication methods, such as biometrics, for example. Under a simple yes/no attestation criterion a health IT developer may not know how to answer the question due to this complexity.

Health IT developers may have MFA capabilities developed within their software suites, may use 3rd party solutions, or may support either or both options. Integration with 3rd party solutions can bring additional authentication capabilities and alignment with healthcare organizations' overall security stance but can also require additional cost and complexity. In a standard Identity Provider / Service Provider authentication model, a developer would not directly implement MFA since that is a function of the Identity Provider, which the healthcare organization may have selected among third- party identity provider solutions.

The EHR Association observes that detailed request for proposals are commonly used by healthcare organizations looking to select healthcare IT software. RFPs are an effective way for a healthcare organization to get detailed answers on MFA capabilities from a healthcare IT developer. An RFP allows the healthcare organization to ask the specific questions relevant to their security risk evaluation and posture. In many cases healthcare organizations have existing authentication solutions they will also apply to the health IT solution.

Because of the variation in MFA need and capability across a developer's product suite, we recommend the ONC criterion allow the developer to describe their MFA support to a level of detail that the developer determines captures the capabilities of their system. We also recommend health IT developers explain if 3rd party authentication solutions are required, optionally supported, or not supported.

We do not recommend attestation to the specific uses of MFA beyond initial user authentication. Support for MFA is a requirement for e-Prescribing of Controlled Substances (EPCS) which already has visibility to the industry through the Surescripts published list of e-prescribing certified software (https://surescripts.com/network-alliance/eprescribing-prescriber-software/). EPCS is also a key feature for healthcare it solutions in the marketplace. Including detailed information about other uses of MFA within specific workflows adds additional complexity to a health IT developer's attestation which would make the use of information by healthcare organizations more complex without adding significant value. It would be difficult for a healthcare organization to compare attestations at that level of detail and match use cases across developers.

The criterion question for MFA is proposed to apply to all certified versions of the software. Security practices evolve rapidly with significant changes occurring in the past several years including MFA techniques, their maturity, and expectations around authentication capabilities. We recommend that the proposed criterion question be required for new software going through certification and not be applied to versions already certified. Requiring this criterion for new certifications adds transparency to healthcare organizations evaluating the selection of software while still encouraging health IT developers to support MFA.

§ 170.315(b)(12) Data segmentation for privacy – send

Included in 2015 Edition Base EHR Definition? *No*

Data segmentation for privacy – send. Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

Preamble FR Citation: 84 FR 7452 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575-77 for estimates related to this proposal.

Public Comment Field:

We appreciate the need to ensure that the right data is shared with the right party based on patient consent. The proposal suggests the use of the DS4P implementation guide and the Consent2Share specifications to manage necessary data segmentation and consent management for both HL7 CDA C-CDA and HL7 FHIR based access and exchange. We have concerns with the references to the standards/implementation guides/technical specifications, as well as the practicality of the proposed approach.

Regarding the references to standards/implementation guides/technical specifications:

- Unlike as is indicated in the proposed rule and implied in the Interoperability Standards Advisory, we believe the DS4P implementation guide only focuses on data segmentation, i.e., labeling of data with certain security/privacy flags, and only applies to the HL7 CDA C-CDA documents, not to HL7 FHIR. HL7 FHIR Security Labels describes how to label resources similarly in HL7 FHIR. We suggest to clarify this distinction explicitly if ONC intended to apply data segmentation labeling to HL7 FHIR resources in support of USCDI as well.
- SAMHSA's Consent2Share is a technical specification that is based on HL7 FHIR STU 3 to record patient consent. However, we understand that SAMHSA will not continue to provide support to make any updates to the existing standard, thus the proposed technical specification effectively does not have an owner. Furthermore, the technical specification has not gone through any consensus review process, nor has it seen any substantial adoption to suggest this is a viable standard to adopt at this point. Since we suggest that HL7 FHIR R4 should be the base standard for FHIR based access/exchange of USCDI, we recommend that if Consent2Share were to be adopted, it too should require the HL7 FHIR R4 version.

Regarding the practicality of the proposal, while some adoption of document level data segmentation exists, section- or entry-level labeling of data has no real adoption in scalable clinical settings. We also note that neither USCDI, nor ARCH, nor HL7 FHIR US Core includes the FHIR Composition resource, which would be at the equivalent level of granularity as a C-CDA document. Therefore, a consistent approach of USCDI across HL7 CDA C-CDA and HL7 FHIR is not attainable at this time.

Additionally, a data segmentation approach using DS4P and presumably FHIR Security Labels would require either a user and/or an algorithm to flag the data with the appropriate security label. There is no industry level guidance available indicating for each of the policies contemplated what data should be labeled in what manner or based on what understanding of sensitive information. Such guidance would be essential to reduce user burden to properly label the data to help assure consistent semantic consents for sensitivity between sender and receiver. To the extent the user would have to label the data, labeling at a level of granularity beyond documents has not been demonstrated to be sustainable in practice. Some have even suggested that any such data segmentation quickly becomes unmanageable to explain and administer.

Based on these concerns, we suggest that the optional 2015 Certification Edition criterion maintains document level labeling and does not require section, entry, and resource level labeling until practical implementations at scale have been demonstrated at that level. This includes providing suitable guidance to developers and implementers for consistent security labeling based on agreed-to policies.

We note that the latest Carequality Query-Based Document Exchange implementation guide has further guidance on the ability to assert access policies and DS4P implementation considerations. While this guide has not yet seen significant uptake, for those opting to implement this criterion it would provide useful guidance.

While we recommend maintaining a document-level focus for the criterion, we do suggest exploring alternative approaches that have greater promise to be practically viable and scalable. For example, approaches that are provider based, similar to how data can be opted to be shared or not under 42 CFR Part II, may potentially reduce or eliminate user mediated data labeling.

Until a practical approach has solidified, we recommend continuing to rely on break-the-glass and audit mechanisms to identify where data has been inappropriately shared and disclosed. We also strongly believe that as privacy policies across 42 CFR Part II and HIPAA are harmonized, more practical approaches can emerge as well.

§ 170.315(b)(13) Data segmentation for privacy – receive

Included in 2015 Edition Base EHR Definition? *No*

Data segmentation for privacy – receive. Enable a user to:

(i) Receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1); and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Preamble FR Citation: 84 FR 7452 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575-77 for estimates related to this proposal.

Public Comment Field:

Please see comments above.

§ 170.315(g)(11) Consent management for APIs

Included in 2015 Edition Base EHR Definition? *No*

Consent management for APIs.

(i) Respond to requests for data in accordance with:

(A) The standard adopted in § 170.215(c)(1); and

(B) The implementation specification adopted in § 170.215(c)(2).

(ii) 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)(11)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7453 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.

Public Comment Field:

Please see comments above.

Note: Because this template presents comment tables in the order in which the new and revised provisions of 45 CFR parts 170 and 171 are discussed in the preamble of the proposed rule, comment tables for other new and revised certification criteria, standards, and definitions can be found in Section VII, below.

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:

The EHR Association is curious what this type of certification would look like, how it would be defined, and how consumers of health IT would be able to understand it. For example, would there be some type of indicator on the CHPL to discern which products were certified to the subset of criteria that were identified as important to the pediatric care setting?

The EHR Association is supportive of some recognition of track/pathway be given to products certified as pediatric-specific, but only if there are actual pediatric-specific criteria/requirements as part of it. Simply complying with the ability to record pediatric vital signs would be insufficient.

Also, we are concerned that there appears to be a large disconnect between the proposed recommendations and what is defined as important in the Children's Format. It is almost as though there is an attempt to retrofit the needs of pediatric patients by using adult requirements. We strongly feel that this proposal will not meet pediatricians' needs, nor their expectations.

Additionally, please note our feedback on the USCDI regarding the need for data stratification, as certain data, such as pediatrics, may not apply to all EHR/health IT.

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

EHR Association members appreciate the proposal to enable access to PDMPs at a more granular data level. That would allow systems to start enabling local data retention, which would in turn support CDS and analytics beyond the view-only access currently enabled by PDMPs (in accordance with their state law/regulations). Starting with NCPDP SCRIPT 2017071, Medication History is a reasonable start in the short term as most EHRs already support that capability.

We note that state legislation and regulation are serving as a limiting factor in any case, as many do not allow PDMPs to make data available to EHRs in this manner. The same is true of cross-state access to PDMP data, though this is critical to the value of applying PDMPs to the challenge at a more granular data level. Therefore, we anticipate that uptake will be limited, until cross-state PDMP data sharing/brokering becomes available, and PDMPs implement support for medication history access.

At the same time, we echo our comments to CMS' IPPS 2019 NPRM, where we suggest that in the short term, it may still necessitate the use of NCPDP SCRIPT standards for medication history queries from EHRs; while, long-term, we suggest convergence on the use of HL7 FHIR, such as CDS Hooks. This shift will more extensively connect EHRs with PDMPs.

We encourage ONC to work with states, PDMPs, and health IT suppliers (including PDMP and EHR developers) to further that opportunity, as well as establish a minimum data set that is expected to be accessible. With regard to the minimum data set, we note our letter dated February 8, 2019, indicating the data set represented in ASAP, currently supported by pharmacies.

We are supportive of the use of agreements for patients with opioid pain management as a means to improve opioid safety and patient engagement. However, the lack of standardization for such agreements erodes their utility in the continuum of patient care, making it impractical or impossible to exchange such agreements effectively, efficiently, and within HIPAA Security and Privacy standards and/or state privacy laws.

We would like to work with ONC, CMS, and other stakeholder groups to develop a standardized agreement and exchange protocols that would allow clinically appropriate access to these agreements and improve their effectiveness in supporting safe, effective pain management with opioids.

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:

The EHR Association agrees that specific Conditions of Certification for information blocking are unnecessary.

§ 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:

The EHR Association would like clarification on when the records retention requirement would begin; is it only certifications granted after the effective date of the final rule? EHR Association members would not be supportive of a retrospective application of this requirement; some records that are being included in this requirement may not have been retained historically, given that these communications would not fall under retention requirements related to other industry standards.

Also, we caution ONC against requiring unnecessary elements in any records retention policy, such as marketing materials. Replication of the FDA's 10K requirements is not merited and would cause unnecessary burden for companies who interact with both agencies in regulatory relationships.

Finally, the Association seeks clarification on exactly the type of information that should be kept in retained records, and we express concern that additional documentation may only compound the problem rather than helping it. We are unclear on why the documentation kept by ATLs and ACBs would be insufficient.

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:

The NPRM proposes that IT developers would be required to participate in a framework or network to provide certain assurances to their consumers. The EHR Association observes that IT developers do not normally directly "participate" in networks on their own, but instead provide the technology to enable participation by others. Examples would be eHealth Exchange and various HIEs serving different regions through different technology and governance models. In other cases, IT developers are members for the purpose of establishing the network, e.g., Commonwell HealthAlliance, but the provider remains the participant in that network; the IT developer cannot share data they manage for a client with other providers without the provider's direct permission. On the other hand, other networks may be mixed where developers and providers are eligible to join, such as Carequality. Therefore, we suggest careful consideration of the interpretation of "participation" and thus measurement requirements. Examples may be where:

- Membership is not the same as participation, as it may indicate those IT suppliers who actively enable their clients to participate in a network.
- Health IT developers act as enablers for Direct-based exchange through virtual networks.

The EHR Association suggests that the primary focus should be on ONC collaborating with CMS to encourage providers to participate in networks as an assurance for consumers, payers, and other providers that they are not engaged in information blocking and to publicize all the addresses by which they can be reached and for what purpose. We believe this, in turn, will strongly encourage IT developers to support their clients to be connected.

Given an IT developer's operational participation in some networks, as well as enabling clients to participate in networks, it should be recognized that those networks deploy standards-based access and exchange within and across networks when assessing information blocking claims. For example, when a health IT developer satisfies TEF participation, either by direct network participation or enabling provider network participation in a manner that meets the same end, then an unmet request to access and exchange data through another means cannot be considered an act of information blocking.

The notion of a framework or network should not presume that all data in question will always be routed through such a network, i.e., brokered and/or physically flowing through that network's hardware infrastructure. Rather, different models are emerging where the framework/network enables discovery of endpoints and capabilities, yet the data requester connects directly with the endpoint(s) to interact. Neither model should receive preferential treatment under regulation where they achieve the same end result of data access and exchange. Thus, we suggest that ONC use concepts such as "routing" carefully to avoid prescriptive interpretations or confusion/ambiguity on what is required.

We note that references to EHI in this section may give the impression that all EHI is expected to be accessible/exchanged using C-CDA documents and FHIR resources. Thus, when referencing use of C-CDA and FHIR, we suggest that the dataset is USCDI as a subset of EHI.

§ 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—

(q) Making a disclosure required by law;

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

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

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

(u) 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.

(i) 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

(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:

As EHR developers, patient safety and its relationship to the user experience is of utmost importance to us. In fact, members of the EHR Association already encourage participation in patient safety organizations, and many developers already have established forums specifically for the discussion of system design, feature, implementation decisions, and more. The importance of building a collaborative system focused on the safety of the patient also imbues the EHR Developer Code of Conduct. Subsequently, we find problems in ONC's proposal, which goes beyond the goal of data sharing for the purposes of patient safety and system improvement; and, instead, it appears to open the door to unprecedented access to intellectual property. We are very concerned about this approach.

The proposal is especially concerning as the scope exceeds beyond the technology a developer presents for certification and seems to apply to all of the developer's products, such as a billing system. This introduces a regulatory imbalance between developers of billing systems who also offer certified health IT and developers of billing systems who do not. We suggest the proposal only apply to certified health IT communications.

The proposal in the rule only addresses copyrighted intellectual property with the acknowledgement of fair use. However, other intellectual property protections--trade secrets, patents, confidential and proprietary information--are unaddressed. ONC will need to revise with these other types of intellectual property protections in mind.

When combined with the API availability requirements proposed in the information blocking provision, an unscrupulous actor could create a "knockoff" version of any EHR. In fact, at least one of our member companies has already experienced this challenge, being forced to deploy resources to fight a pirating actor. We see no way to protect against that given the current language and exceptions as proposed.

The EHR Association is generally supportive of the two-part test. However, there is no provision for addressing claims that are patently untrue or specifically doctored screenshots. We need the ability to refute such claims. We also have concerns about individuals who may post anonymous comments with no way to verify the validity of those statements, as this removes the developer's ability to help mitigate the problem and solve it. This is especially concerning regarding ONC's comment related to social media posts and online forums.

We appreciate the recognition that software in the Alpha and Beta stages of development are not addressed by this proposal.

EHRA is concerned by the proposed requirement to review and revise contracts, as the timeframe provided is incredibly short given the high volume of contracts held by larger developers. Reworking contracts where language exists that could be interpreted as limiting transparency of information related to patient safety or usability concerns could be untenable. Several of our member companies have tens of thousands of clients and have estimated this process would cost tens of millions of dollars and take many, many years to complete.

Instead, we suggest that if contract language must be amended, an alternative means of completing this must be made allowable, such as posting revised language specific to the "communications" issues on the company's website, making clear that the posted language supplants any pre-existing contractual language. Generally, should the proposed language be adopted, we struggle to see how the regulation achieves its proposed goal of increasing innovation or reducing burden.

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:

The EHR Association appreciated the flexibility provided in the 2015 Certification Edition where there was not immediately a standard defined to support the consumer focused APIs. Based on the experience to date, we believe the industry is ready to name a minimum standard in the Certification Program that must be used to support APIs enabling consumer, provider, payer, and other user focused Apps to get consistent access to the APIs, as well as enable business-to-business interactions using these APIs.

We strongly suggest that HL7 FHIR R4 with the soon-to-be-published US Core implementation guide provides that minimum standard that the Standards Version Adoption Process can evolve until the bar can be raised to a new minimum standard. While we recognize that most implementations that use HL7 FHIR use DSTU 2, we believe the following rationale supports our recommendation:

- The progress made in the development and deployment of HL7 FHIR in general.
- Various capabilities being contemplated cannot be achieved using that version, e.g., Provenance, Clinical Notes, bulk data transfer.

- The specifications are more robust where the foundation and an initial set of resources, including Patient and Observation, are now normative and have benefited from increased use and refinement.
- Vocabularies have improved alignment with HL7 CDA C-CDA.
- Adoption of HL7 FHIR DSTU 2 or HL7 FHIR STU 3 would quickly yield introduction of HL7 FHIR R4. That in turn would unnecessarily require support for multiple versions to enable interoperability between any two parties. Those developing toward FHIR for the first time have to develop both rather than one to start. Those who are on a later version would have to also implement STU 2 if that option is chosen. Many of those supporting FHIR DSTU 2 or FHIR STU 3 are ready to move on to FHIR R4.

We urge ONC to work with other agencies wherever possible to encourage any health IT holding USCDI to adopt these standards. CMS' Interoperability and Patient Access NPRM already indicates that payers are encouraged to use the standards identified in ONC's rule and that payers are actively engaged through Da Vinci to operationalize that. Also, we believe that it would be of tremendous value in furthering the payer-to-provider sharing of patient data that the payer may already have, but the provider does not. However, that leaves ambiguity for laboratories, pharmacies, PDMPs, registries, public health agencies, and others that have patient identifiable USCDI.

With the expansion of those who share data and consequently how data can flow through the health system, Provenance is an important capability. We urge ONC to not only focus on HL7 FHIR and HL7 CDA C-CDA based data access and exchange, but also other interoperability formats that actually may yield the original data set that ends up populating the FHIR and C-CDA formats.

We support the use of OpenID Connect Core 1.0 incorporating errata set 1 as well as SMART Application Launch Framework Implementation Guide Release 1.0.0. However, we note that standalone launches of provider-focused Apps should not be a requirement, as they typically operate within the context of the EHR and may therefore be launched in a variety of ways.

The various standards referenced above and in the proposed rule are essential to expanding the value of interoperability, but are not enough. In particular, in relation with TEF and the initiatives currently in flight of various networks to expand the ability to not only exchange documents, but also "data elements" based on FHIR (whether small or large data sets in bulk), that standards such as back-end service authentication will play an important role to enable business-to-business, not just Apps to access and exchange data. We suggest that ONC work closely with those initiatives to foster collaboration, e.g., align the FAST initiative with efforts already in flight with Carequality, Commonwell, and others.

We support the proposal that refresh tokens should have a three month minimum expiration period for consumer Apps only. Business-to-business and other interactions using FHIR-based web services may use different techniques where this minimum may not apply. We also suggest that revocation of refresh tokens is permissible within the confines of the information blocking exceptions related to security.

§ 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.

Public Comment Field:

We appreciate that ONC is addressing concerns raised around the ability to validate the authenticity of an app developer. However, we remain concerned that while one can address security and performance issues reactively, as they occur, through the information blocking exceptions, pre-deployment testing/validation can only be offered through value-add services. This limitation, which is placed on private/public providers and their health IT suppliers but not on government agencies operating under the Privacy Act and FISMA, remains a concern. We urge ONC to consider allowing for fundamental security and performance testing that apps and business-to-business interactions can be required to be performed before they can be connected to a provider's infrastructure.

The industry has had some discussion about the creation of a "seal of approval" for safety and security related to apps available to consumers, and we are cautiously supportive of this concept. It might offer a level of assurance or indemnification, and it also allows for more reliability. We suggest this be further explored by ONC.

We support the proposal that refresh tokens should have a three-month minimum expiration period, but it must be recognized that this is primarily focused on consumer apps. Business-to-business interactions using FHIR-based web services may use different techniques where this minimum may not apply.

We request clarification on provision of refresh tokens to public/non-confidential apps, which is not recommended in the implementation guide. Does ONC intend to require this?

§ 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

(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

(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

(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.

(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.

(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:

At a high level, we agree that providing APIs that are "standardized," "transparent," and "pro-competitive" is the right direction to promote interoperability. However, the definitions of each attribute listed here are too vague to objectively certify against. Given the clear emphasis on APIs as an emerging mechanism for information access and exchange within ONC communications and regulations, this is a very important section.

Cost Limitations

With APIs increasingly used across the industry and more and more use cases being explored in various collaborative environments, efforts by ONC, within this NPRM, to limit the costs that can be charged and to whom they can be charged have a potentially outsized importance in the information blocking conversation.

We find the section on API Policy and Pricing to be unnecessarily disorienting, as the proposals are split between the Conditions of Certification and the information Blocking exceptions. We suggest that the approach could be simplified by addressing the topic in one consolidated section. Similarly, there are quite a large number of carve outs, as well as different terms with differing restrictions regarding what can be charged for and who can be charged, depending on the purpose of use.

It is proposed that the cost for development be distributed among those who will use it. This is problematic in many ways. There seems to be a belief, for example, that when a new API is developed, an invoice for that work is separately sent just for that work to those that are buying it separately from their other purchases, which would allow the proposed model of cost distributive invoicing to work. This is not how development is done and charged for today.

Further, if costs are to be divided among clients, it presents several challenges: What happens if you have divided the costs and been paid, but then a new customer decides they want to purchase the same API? Do you need to refund other clients because their cost should then come down? The intent is to track every minute of work being done to justify prices charged to customers, but the implementation of this concept seems impractical and burdensome.

Small companies could be disadvantaged because the development cost would be divided among a smaller base of clients, thereby increasing the costs charged and creating a disincentive for purchasers to choose to work with small companies. Conversely, large companies would be disadvantaged through the inherent profit reduction that would come from being forced to divide development costs among a very large base of clients and thus charge significantly less than the market is willing to support in a natural market-based economy.

Also, we see several issues and request reconsideration of the proposed prohibitions on charges. First, the prohibition against health IT developers charging for work to update our code structure is unreasonable; this is important work that is necessary for companies to be able to modernize their solutions as broader technologies evolve, and the work is something that should be able to be included in what we charge our clients where the market supports it.

Under the proposal, in fact, there would be a lot of work conducted by our member companies that they could not charge for: EHRs can't charge the third party, but the third party can charge the patient. EHRs can't charge for the use of the APIs, but can charge providers for the development of the APIs. Providers, in turn, can charge third parties for the use of the APIs. As you can see, this is confusing, and we request clarification through a chart that lists all actors, all types of costs and who can charge whom.

Finally, we are concerned that while these changes are intended to advance innovation, they will have the opposite effect. Health IT companies unable to price their products and services at market rates will not be incentivized to invest further in research and development or offer new products and services. This is particularly true if other parties can benefit from their development and are not restricted to cost-based pricing. We request clarification on two pricing concepts here:

- Are the prohibitions related only to development, with services and ongoing support not covered?
- Can an EHR developer charge for the use of sandboxes by app developers?

We urge reconsideration of the cost-based approach. Instead, ONC can acknowledge the value of market-based pricing to drive innovation and competition, while identifying pricing behavior that is specifically in play to block information flow--such as those intended to limit communication with a competitor--while continuing efforts to standardize interoperability that will create a transparent and level playing field that enables identification and correction of outliers.

Documentation
EHRA is requesting a time allowance on this criterion to allow documentation and all other websites to come into alignment with regards to documentation before this is considered a violation of the Condition of Certification.

Recordkeeping Burden
In regards to the Permitted Fees, EHRA is troubled by the level of granularity that would introduce unreasonable burden into the process. The enormity of recordkeeping for this purpose would far exceed any documentation we are doing for any other purpose. Instead, we would like to suggest focusing on what's most important, which is encouraging interoperability and innovation. We suggest that ONC simply allow patients the ability to access their EHI without charge; focus on a good conduct approach rather than overly prescriptive requirements about fees.

FHIR Endpoint Transparency
We are concerned with the proposed requirement that health IT developers publish their clients' FHIR endpoints. We recognize that one of the reasons to require health IT developers to publish this data is to enable App developers a single point of access and ease the registration process across providers using the same health IT developer. However, we strongly support the statement, "The API approach also supports health care providers having the sole authority and autonomy to unilaterally permit connections to their health IT through certified API technology the health care providers have acquired.

Thus, an App developer would have to contact the relevant data holder directly, unless the data holder is part of a network in which the App developer participates, and therefore can connect to all data holders in that network based on their participation level. Considering this, and that a health IT developer cannot publish client information without their express consent through the applicable Business Associate agreement, we cannot support this proposal.

Rather, we urge ONC to work with CMS and data holders to make such information available through the Provider Digital Information Index called for in the 21st Century Cures Act. Such a directory, in combination with directories maintained by the networks that operationalize many of the necessary infrastructures to connect, can support look-ups by authorized parties, while still being able to contact the data holder for this information. CMS may consider, perhaps as a condition of participation, that a data holder publishes their endpoint information either on their website, and/or their organizations' entry in the NPPES.

We recognize that FHIR-based access/exchange is not widely available for networks, but expect this to be ramping up quickly in the near-term, providing a scalable solution that recognizes the data holder's responsibility and choice for external Apps and other data holders to be connected.

We note that the term "endpoint" is ambiguous. In various architectures the actual information needed is an endpoint plus site ID, as multiple sites may be serviced by the same endpoint. We suggest the term be clarified.

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.

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

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

(viii) 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:

The EHR Association is supportive of limiting the criteria on which real world testing focuses, such as only measuring care coordination criteria, or measuring whether public health immunization records are sent/received, as we believe the focus should be on clients being able to use the system and get the results they want. If a larger scope of testing is expected, EHR developers would need a two-year cycle instead of a one-year cycle in order to adequately demonstrate compliance.

Also, the Association would like ONC to provide an optional template and guidance, similar to what has been provided for usability testing, so that there is more cohesiveness in the way the test plans are written by the various developers.

We have concerns about the additional resource burden this will put on clinicians, and the misalignment with ONC's purported goal of decreasing burden. Most clinicians expect to be paid to participate in testing such as this. That makes testing more expensive or infeasible. We do not feel that EHR developers should be penalized for clinicians declining to participate--similar to in-the-field surveillance conducted by ACBs. However, EHRA also recommends that ONC find some way to incentivize clinicians to participate; without their participation, this becomes an untenable requirement. Finally, ONC should incorporate provider time spent in testing into the burden analysis.

The EHR Association is recommending that ONC limit real world testing to *substantive* updates to functionality related to certified criteria. For example, leverage the existing quarterly update attestation process and ask developers to conduct real world testing on those items identified as major changes. This recommendation helps support ONC's goal of reduced provider burden associated with repeated testing when no significant changes have been made to the CEHRT.

We seek confirmation that a test server could be used for real world testing instead of a production environment, given the permissible use of synthetic data. Also, we seek confirmation that a product serving multiple care settings could complete a single test relevant to all settings. Furthermore, we ask ONC to provide a list of eligible care settings for reference.

We do not support developers being required to submit testing results for a minimum "core" set of general metrics primarily because not all metrics will be available to all systems uniformly. Many metrics are retained in the client's system itself and are not available to the vendor without development and considerable time to retrieve the data and post them to the vendors' records. Due to this complexity, we believe developers would prefer to create their own metrics, though we are definitely interested in ONC providing examples of the types of metrics they would like to review, as this may be helpful when developers create their own metrics.

The EHR Association is supportive of 2020 being treated as a pilot year, with no penalties and with education and feedback provided to EHR developers in a timely manner. We suggest that 2021 should also be a pilot year, particularly if the final rule is published late in 2019.

Additionally, EHR Association members seek clarification on how using existing networks and tools (e.g. Surescripts, public health testing, etc.) might count toward real world testing efforts.

We seek clarification on what definitions and interpretations of "received by" and in particular "used" in "Electronic health information is received by and used in the certified health IT" are, in order to understand what is actually being measured.

Meaningful interoperability testing involves health IT from different vendors. Where efforts connecting with networks can satisfy real world testing, coordination and alignment of timelines are already part of those efforts and generally work well. However, for any interoperability without a coordinating network in the middle, we must be sensitive to the challenges that may arise when needing to line up multiple health IT vendors and a provider.

We appreciate the flexibility to use real data, synthetic data, parallel environments, and other configurations enumerated.

§ 170.555 Certification to newer versions of certain standards

(b) * * *

(1) ONC-ACBs are not required to certify Complete EHRs and/or Health IT Module(s) according to newer versions of standards adopted and named in subpart B of this part, unless:

(i) The National Coordinator identifies a new version through the Standards Version Advancement Process and a health IT developer voluntarily elects to update its certified health IT to the new version in accordance with § 170.405(b)(5); or

(ii) The new version is incorporated by reference in § 170.299.

Preamble FR Citation: 84 FR 7497-501 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The EHR Association is generally supportive of this requirement.

ONC requests feedback as to how much time is appropriate for notifying customers of a new standard. We would recommend two months as a reasonable minimum time prior to implementation of an updated standard for our customers to be notified.

We seek clarification on whether multiple versions of a test tool would be maintained to accommodate all these versions of standards when a new system is presented for certification. If not, EHRA is supportive of allowing self-declaration to a new version if the testing tool is unavailable. Within six months of the test tool being updated to the new standard, we recommend that the developer would run the file(s) through the tool and submit the file(s) and validation results to the ACB during the next quarterly product update process (or sooner) to serve as documentation of compliance.

We appreciate and support the introduction of the Standards Version Advancement Process (SVAP) to create flexibility to advance to more current versions of a standard, not only for vocabulary standards as is currently permissible, but other standards as well. We underscore the need for a clear and transparent process to consider when a newer version is deemed permissible for use as part of a certified product.

We note some areas that require further consideration.

The proposed rule is not clear on whether it is permissible to only support the version referenced in the SVAP, or whether one must always be certified at a minimum to the version referenced in the Certification Program then current finalized rule. Different use cases seem to have different needs. In some cases, support for a minimum version is not necessary; in other cases it might have value.

For example, if CMS expects submission according to the most recent implementation guide, it would not make sense to certify products to older versions of the implementation guide. Similarly, if CDC permits submission of healthcare surveys according to an updated version of the standard, it would not make sense to certify products to older versions of the standard.

However, in other cases, there are advantages to all certified software able to communicate using a common standard version. While certain backwards compatibility is aimed for, it is frequently unlikely that a solution using standard Rn can fully and reliably interact with a solution using standard Rn+1, requiring transformation tools while still having a potential incompatibilities. For example, if two health IT systems are exchanging data with each other, they should be able to rely on support for at least the minimum common standard version, even if additional standards are also supported..

Therefore, we suggest clarification from ONC on cases where certification to a floor is not necessary and cases where certification to a floor is expected. We recognize that, for a new entry introducing a solution for certification when the SVAP includes a more current permissible version and wanting to use that version, that might mean needing to certify against two versions around the same time. However, interoperability compatibility is critical to the success of the program, providing providers and other stakeholders with predictable, lowest effort, connections.

The proposed rule is not clear whether the USCDI is expected to be versioned through the SVAP or the Certification Program. Considering the implications and fundamental purpose of the USCDI, we suggest clarifying that the USCDI will be versioned through the Certification Program.

Lastly we note that the proposed rule indicates that an expanded section of the Interoperability Standards Advisory is expected to be used to facilitate the public transparency and engagement process. We note that such a section should be very clearly delineated and distinct from the ISA to avoid any confusion whether a standard/implementation guide version referenced in the ISA implies that it is permissible for use under SVAP.

VII.B.6 Attestations

§ 170.406 Attestations

(a) Condition of Certification. A health IT developer must provide the Secretary with an attestation of compliance with the Conditions and Maintenance of Certification requirements specified in §§ 170.401 through 170.405 at the time of certification. Specifically, a health IT developer must attest to:

(1) Having not taken any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103;

(2) Having provided assurances satisfactory to the Secretary that they 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;

(3) Not prohibiting or restricting the communications 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; and

(4) Having published application programming interfaces (APIs) and allowing health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces 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;

(5) Ensuring that its health IT allows for health information to be exchanged, accessed, and used, in the manner described in paragraph (a)(4) of this section; and

(6) Having undertaken real world testing of its Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9)) in the type of setting in which such Health IT Module(s) will be/is marketed.

(b) Maintenance of Certification.

(1) A health IT developer must attest to compliance with §§ 170.401 through 170.405 at the time of certification.

(2) A health IT developer must attest semiannually to compliance with §§ 170.401 through 170.405 for all its health IT that had an active certification at any time under the ONC Health IT Certification Program during the prior six months.

Preamble FR Citation: 84 FR 7501-02 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7582-38 for estimates related to this proposal.

Public Comment Field:

EHRA is concerned that the conditions of certification expect health IT developers to attest to statements that are subject to interpretation and ambiguous. Developers should be able to articulate how their software and businesses meet the expectations to avoid ambiguity or confusion.

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:

The EHR Association appreciates the opportunity to comment on the exceptions proposed and have included feedback on each of them below.

Overall, we are concerned that the proposed information blocking provisions will have detrimental consequences to the industry given the breadth of the definitions, ambiguity of the expectations, and narrowness of proposed exceptions.

We note that inherent to the concept of information blocking is the element of intent and knowledge. It is not clear how the intent and knowledge element of an information blocking action will be determined. ONC should clarify.

In this work, we suggest a focus on standards-based interoperability and reciprocity. Lack of standardization disadvantages all actors, but in particular it leaves those without access to sophisticated technology, such as those who are economically disadvantaged, without the ability to meaningfully use their data. A thriving environment of free flowing information will require the participation of all actors; allowing information blocking or information hoarding from certain actors, such as data aggregators, but not others will not achieve the desired results.

§ 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.

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.

(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:

Important definitions such as "interoperability elements," "Health Information Network," and "Electronic Health Information" (EHI) have been drafted very broadly, going well beyond Congressional intent, which was to enable patient data access and patient care coordination. Instead, the proposed rule is so broad and so inclusive that it envelops every stakeholder and product that may have access to elements of patient data. Particularly, EHI being broader than PHI and the designated record set introduces challenges when actors have focused efforts historically on PHI and HIPAA.

The EHR Association recommends that the definitions be re-drafted to more narrowly focus on Congressional intent in the 21st Century Cures Act, ensuring that patients have access to their own data; that the data is able to move between care providers; and that appropriate data is available for research. Any drafted definition should be checked against those criteria and narrowed if it goes beyond those goals.

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:

The EHR Association notes that including price transparency information in information blocking would have broad implications for other types of health IT products and actors (for example, practice management products, claims clearinghouses). We suggest extensive further research be done on the implications and on alternative methods to advance price transparency.

Request for comment regarding price information (Department of Health and Human Services)

The overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

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

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Medication price information is already widely available using standards such as NCPDP and e-prescribing networks; however, wider adoption is limited due to the availability of such information. For example, if a network only has price information available for a portion of the drugs on covered plans of a patient panel, it may make sense to defer implementation until a larger data set is present.

The following domains for pricing are going to be much harder to make available. Labs, imaging, procedures, and other treatments are not services that can be compared, apples to apples, in the same way as medication pricing. Standards to compare data in those categories are not widely adopted.

In order to make meaningful strides in price transparency to help patients make more informed decisions about their care and to avoid surprise billing, it is critical that standards be developed for identifying, categorizing, and comparing those services. To date, the lab industry has resisted broader adoption of consistent standards. , and the difficulty of procedure price comparison with the challenge of the chargemaster is well-known, given the entirely different ways that hospitals and physician practices describe and charge for their services.

Request for comment regarding practices that may implicate the information blocking provision

We request comment regarding our proposals about practices that may implicate the information blocking provision. Specifically, we seek comment on:

- Our proposed approach regarding observational health information and encourage commenters to identify potential practices related to non-observational health information that could raise information blocking concerns.
- The circumstances described and other circumstances that may present an especially high likelihood that a practice will interfere with access, exchange, or use of EHI within the meaning of the information blocking provision.

Preamble FR Citation: 84 FR 7515-21 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

ONC has indicated that use of non-standard means for interoperability could implicate information blocking. However, the 21st Century Cures Act includes the use of non-standard-based interoperability. We recommend that the rule clarify when non-standard based interoperability is permissible. We suggest that for an interoperability capability not referenced in the Certification Edition with a specific standard attached to it, use of non-standard solutions would not be considered information blocking.

§ 171.200 Availability and effect of exceptions

A practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision by meeting all applicable requirements and conditions of the exception at all relevant times.

Preamble FR Citation: 84 FR 7522 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The EHR Association recognizes and appreciates the effort on the part of ONC and OIG to define the required exceptions to the information blocking sections of the 21st Century Cures Act. While the proposed rule took some time to be propagated, we believe there is value in the work that the agencies did to engage multiple stakeholders (including the Association) in gathering practical and measurable input. We strongly encourage ONC to take the same paced approach with the final rule, thoughtfully considering the substantive input being returned by the industry.

The broad definitional scope has direct bearing on the Exceptions and how proposals there should be interpreted, and there are other areas where further exceptions will likely be appropriate. We make the following recommendations:

1. ONC should address as much ambiguity and as many unanticipated exception cases as possible in a final rule. A second round of public comment would aid in even further clarification.
2. After the final rule, an ongoing process for clarification needs to be established where actors can anonymously request authoritative guidance from ONC or OIG on whether a practice implicates information blocking. The guidance should be public so that others can benefit from this information.
3. A time period of enforcement discretion should be established for this necessary guidance to be propagated and for claims to be investigated in an educational manner, without financial penalties.

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 healthcare 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:

The EHR Association believes the Preventing Harm exception is a relevant and fairly well-articulated one. It is very well-intended, and we appreciate the thoughtfulness. We support the cited use cases, and it is, of course, aligned with the Hippocratic oath to "do no harm" so will resonate with affected healthcare professionals.

While we appreciate the appropriateness of sharing information, we fear that ambiguity in the Preventing Harm exception will cause providers to err on the side of sharing *too* much. Ideally, all providers would be thoroughly educated on their responsibilities under HIPAA, the information blocking provisions, and the crisscrossing patchwork of state and local regulations and organizational policy. However, in reality, a small provider practice facing the threat of a referral to OIG for investigation might take what they see as the simpler path, sharing information indiscriminately and with less regard for patient safety than ONC likely intended.

This exception should be simplified for purposes of ensuring greater understanding by those affected, and the balance between HIPAA and Information Blocking regulations should be explicitly explained in more detail and plain language.

As stated, we support this exception, and we appreciate that there may be instances in which sharing information could be problematic. Following are some areas we believe need additional thought before any version is finalized:

- In the instance that a clinician decided that sharing a patient's information would or could cause harm, what documentation do they need to preserve to justify (upon further investigation) why the record wasn't shared? The NPRM suggests that policies will be developed in response to this rule to guide clinicians in their decision-making, and we suspect that to be true. However, even with a policy in place, the clinician may not remember a year later why that record wasn't shared in that instance. What information are they expected to capture to explain that? Where is that to be captured? How long must they keep that justification document? What burden will it place on clinicians to cover themselves in this scenario? Those are the types of details that must be considered and included in any further regulation.
- Further detail is necessary in clarifying how "harm" is to be defined, as well as who must be at risk of harm to fulfill the Exception criteria. Physical, emotional and mental harm could all be a factor in different situations. We recommend that each clinician be allowed the discretion to determine if "harm" is a risk, rather than forcing the application of a series of tests to determine whether it qualifies. We note that this seems to align with OCR's thinking related to updating HIPAA regulations soon to come, and consistency in allowing clinician discretion would be appreciated.

- The proposal that a record be sent as wholly as possible while withholding any portion of the record that is corrupt or inaccurate is technically problematic. Further, the NPRM suggests that the clinician should not have to take multiple steps or spend a lot of time wading through what portions of the record to send, but the idea that a provider is responsible for knowing if there is any portion of the record that is corrupted or inaccurate for a reason out of their control on any given day *and* how to filter the problematic areas while sending the rest seems to conflict with that guidance.

We suggest that the provider should definitely be excused from exchanging the patient's data while any issue with corruption or inaccuracy is being dealt with, rather than expecting them to differentiate and withhold some but not all information. Otherwise, it could very quickly become burdensome and confusing.

§ 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 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:

The imperative to protect the privacy of patients and treat their data as a priority consideration is well-recognized within ONC's proposed rule. While the issue of privacy and how to navigate it within the context of a connected healthcare system touches on several of the other Exception categories, EHR Association members applaud the consideration of the topic as its own area worthy of in-depth conversation.

Health-related privacy is a very complex area where most people already don't understand the law. It is well-known that healthcare providers across the country frequently make well-intended but ill-informed decisions about information exchange in attempts to comply with the HIPAA law, and efforts to educate and address those misunderstandings have not done as much as was hoped to change behaviors. In fact, we recommend ONC review and consider using the API Task Force Recommendation around coordinating and improving "privacy literacy."

Our concern with the Promoting Privacy section of this NPRM is that where there is already tremendous industry confusion, there are complex new concepts about privacy and information exchange being put forward that seem to create possible areas of conflict between HIPAA and the Information Blocking rules in practicality. In particular, we believe there will be a lot of confusion and concern among average clinicians, working in independent physician practices without budgets to hire advanced legal guidance to help them understand. Frankly we, as experts in reading and analyzing regulatory language related to privacy, found the proposals puzzling. It needs to be simplified.

In addition, we do not see data segmentation as solving the challenges identified here. Please see our concerns about data segmentation elsewhere in the document. Instead, we suggest that the provision of machine-readable state and local privacy policies would aid in consistent implementation by health IT and healthcare providers.

Therefore, we strongly encourage ONC to include less in the final rule that would require providers to research the varying and sometimes conflicting laws that govern them (and thus concluding for themselves which to follow). Further, we request explicit guidance from ONC, OCR and SAMHSA outlining the interactions between HIPAA, 42 CFR Part 2, and Information Blocking rules; this guidance would need to be reissued and clarified upon any further promulgation of regulations amending any of those programs, which we understand to be expected later this year.

We note as well that there will always be unforeseen circumstances that regulators and practices didn't account for in drafting regulation and writing internal organization policies. We suggest that ONC work with OCR where appropriate to craft simpler regulatory language; specifically, we suggest that a "case-by-case" exception with documented justification should be used in those instances when information is withheld due to privacy concerns, and this should not be considered information blocking. A provider should never be in a position where they believe they are "forced" to compromise patient privacy because their policy and practices did not cover a given scenario that has emerged through interaction with a patient.

We encourage a risk-based approach, particularly in circumstances where HIPAA or state law may not provide a specific exception. For example, there are instances wherein alerts are issued about fraud schemes involving malicious threat actors, or it becomes known that compromised credentials have been listed on the dark web, thereby creating opportunities for exchange with falsified actors. Providers should be allowed to use their discretion not to exchange information with affected providers in their network until those issues are resolved.

We agree that multi-state organizations need the ability to apply high-water mark policies.

We recommend using a less tailored approach in the consent exception; consent management in the API era is still so nascent, any approach outlined now would be quickly outdated. We would prefer ONC monitor this area and issue guidance in the future.

We appreciate the inclusion of the requirement for the clinician or provider organization to respect an individual's request not to share information. Individuals should also have an easy way to check their current privacy elections at any point.

There are several areas in which we request clarification and more specificity to ensure appropriate implementation:

- Does the record need to capture the patient's preference for non-exchange (i.e. don't send my record to that one practice down the street)? Where is it expected that this preference would be recorded, and for how long does that preference need to be retained? How should a changed preference be captured so as not to replace the initial preference that led the provider not to exchange information?
- Given the issue of cross-state patient flow, does the law derive from where the care is delivered to the patient vs. the state in which the patient lives? We request guidance to the states from ONC/OCR to match how this rule specifically interacts with and/or conflicts with each state's own regulations.

§ 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:

Again, the EHR Association applauds the creation of the Promoting Security Exception. We support this exception, and we add that there is never a minimum standard in security; security technology is ever evolving as new threats emerge. This exception is vital to allow those on the forefront of security technology a means to stop the flow of data when new threats emerge, and the only course is to not share information until a new secure method of sharing is identified.

Clearly, in the age of daily cybersecurity threats and the increasing number of bad actors, as well as the ongoing challenges with patient identification and matching, this is an area where the industry must continue to respond to security as an impediment to information flow. We are supportive of ONC's use of consensus-based standards, and the guidance provides an appropriate reference point for the development of security policies.

We applaud the clear effort to maintain flexibility in the approach to this Exception. Generally, we agree the Exception must revolve around security viewed as an incident or threat; best practices in security mitigation are to take a proactive approach as opposed to a reactive approach, which could be viewed as discriminatory.

Certain elements of the proposed language seem to reflect a lack of awareness of the practicality of managing security practices for a base of clients. Specifically, the use case in which a security threat or attack is identified and in which an instantaneous response -- possibly including taking down a system -- is required, the concept of needing to seek client permission or place phone calls to all clients is simply untenable. It would not be advisable to use up valuable time to place a call to a single client, much less an entire group in the case of a cross-base risk. This must be addressed in the final rule.

We have identified several areas where we need clarification and where the answers could affect the optimal path forward in implementing support for this Exception:

- Does a past issue with another organization where security or patient identification caused an issue qualify for this Exception? For example, HIEs occasionally have security breaches -- does that mean someone has the right to block them? For how long do they have such authorization? What do entities have to do to show they are trustworthy and remove the cover for someone to refuse exchange?
- Does the burden of patient identity verification fall on the provider? That is implied within the proposed regulatory language because concerns about identity are a security exception, but this assumes that consideration of patient matching challenges should go into the decision to respond to a request for a patient's record. We think this is unreasonable and burdensome to the average clinician.
- In the statement, "Disagreement with the individual about the worthiness of the third party as a recipient of EHI, or even concerns about what the third party might do with the EHI, except for reasons such as those listed in the 'preventing harm' exception, are not acceptable reasons to deny an individual's request," is ONC referring to an individual as an individual as defined under HIPAA? If yes, we agree with this statement; if "individual" included any third party claiming to provide treatment, payment and healthcare operations or claiming to represent an individual on whose behalf they want to access that individual's data, then we have serious concerns with this proposal as it relates to the security of EHI.
- Does the FTC have a role here (security, business practices, privacy, etc.)? The FTC is already going to be processing complaints in this space related to consumer-directed apps, so why not set clear expectations ahead of time through promulgation of pre-identified standards? It seems reasonable that just as health IT companies are held to standards, other apps being developed in other sectors of the healthcare industry should be as well.

Lastly, we ask ONC to consider how the increased transparency about security issues as a reason for limited exchange of a patient's data could inadvertently hurt the health IT ecosystem. We are concerned that we may ultimately see less trust in the health IT infrastructure being built in this country as an unintended consequence, which is something to avoid.

§ 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.

(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:

While the EHR Association appreciates the ability to recoup the costs of investing in technologies above and beyond the exchange of data for patient care, and especially appreciate ONC's acknowledgement that it is appropriate to pay software developers for the work they do as we invest in our companies' futures, we have a number of noteworthy concerns with this section.

Effect on Innovation

Limiting or excluding the ability to profit will lead to an unintended consequence of discouraging investment and innovation in the industry. While acknowledging in this rule concerns about the relationship between costs and the flow of information, ONC is not sufficiently addressing several factors that are recognized as contributing to those costs, but is instead focusing on price-capping models that undermine market-based pricing structures. In particular, the slew of entities (such as lab companies and state-based or small registries) who do not follow nationally-recognized standards in how they connect to others, thus driving up costs unnecessarily, will have little reason to change their approach.

A challenge of pricing being based on cost-recovery, too, is that it removes the incentive to innovate and offer products or services more efficiently. If a company figures out a method to be more efficient, they would not be rewarded by making a greater profit on that product or service. Instead, they must lower their price. This seems counter to the overall goals of greater efficiency in the healthcare space.

Variability of Cost

In addition to the variability of costs discussed in the section entitled "*Requirement that costs be reasonably incurred,*" we note that labor incurs different costs depending on where it is performed. Further, the rate of compensation for software development staff may be heavily influenced by the individual's experience, the quality of the development they produce, the language in which they are coding, and more.

Challenges of Dividing Costs

As we addressed in our earlier comments on API-related pricing, the notion that costs can be evenly divided among clients is flawed. The number of anticipated clients who will want to purchase a software module cannot be known with certainty, which presents several scenarios:

- Customers will delay in purchasing hoping that others will become interested and lower the cost, thus delaying adoption of interoperability.
- Developers will overestimate how many customers will purchase the module and end up losing money because they didn't charge enough.
- Developers will underestimate how many customers will purchase the module and be at risk of

information blocking because they inadvertently overcharged or need to find some method to refund money with increased recordkeeping and administrative overhead.

- Fear of overestimation or underestimation will cause developers to be reluctant to invest in creating new modules with uncertain financial returns.

Further, the nature of investment is such that certain investments will succeed and others will fail. Without perfect knowledge at the time of investment which ones will be successful, developers need to be able to use profits from successful investments to fund those that will not be successful. We are concerned that the limitation to "reasonable profit" on a specific project or investment would preclude vendors from earning enough to explore investments that ultimately may not be successful, further discouraging investment and innovation.

The intent to evenly divide costs may result in differences by an order of magnitude between a customer using software from a company with five clients and one who purchased software from a company with 500 clients.

Additionally, larger companies would seem to be at risk of losing significant revenue if they are dividing their costs across a large client base from whom they have traditionally collected market-based prices; is ONC prepared to have a significant impact on the financial soundness of companies in the industry? We recommend that ONC and OIG keep these circumstances in mind when determining if an observed price discrepancy is valid.

Architectural Changes and Charging
ONC specifically prohibits charging extra to account for architectural designs and decisions that might add to the overall time spent developing APIs. While the EHR Association endorses API-first and contract-first development patterns, we note that some software in use was written before modern software architecture principles were established. In addition, software architected to maximize internal extensibility, performance, or scalability might not be equally optimized for public APIs. Such architectural decisions are reasonable and prevalent, and the inability to fund the rearchitecting of the software for use cases for which it was not envisioned may be insurmountable for some smaller developers.

Recordkeeping Burden
Finally, we note that the requirement to track costs discretely to the level of detail envisioned by this Exception may, in and of itself, introduce more cost, reduce the timeliness of enhancement delivery, and just generally add unreasonable burden to the software development community. We suggest ONC keep such costs in mind when balancing the overall benefits and costs of this method of tracking the Exception.

Finally, similar to other sections within the information blocking provisions, we request explicit clarification on areas of ambiguity, such as who is allowed to charge whom for what, and what "reasonable" means in this context. We note that this exception is especially confusing when combined with the API Policy and Pricing condition of certification, and there is language here that seems to conflict with the Preamble in terms of allowing for profit vs. only allowing for cost recovery. We suggest that the final rule clarify explicitly in the regulatory text that profit is permitted.

Limiting the profit a business can make is a disincentive to invest and innovate. Profits are often put back into the business to fund innovation efforts, are returned to employees through rewarding salaries and benefits packages, and provide value to shareholders. Other tech spaces do not face such cost limitations, and neither should the health IT space.

§ 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

(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:

The EHR Association agrees that an inability to do something, if it is truly infeasible, should not be penalized as information blocking. Overall, we anticipate that health IT developers will frequently need to use this exception to justify why they are not able to accommodate all stakeholders' development requests and need to prioritize their work. Given our anticipated reliance on this exception, we have several concerns about its language and underlying assumptions.

Size of Organization and Capability to Respond to Requests

In this exception, ONC differentiates between a large provider organization--which ONC appears to presume has large numbers of technical resources and staff--and a smaller one, which presumably has none. While such a presumption is common, in practice it leads to erroneous and problematic conclusions.

For example, consider a large, multi-site integrated delivery network. The network has hundreds of small, two-doctor practices referring patients to it. Any one practice makes up about 1% of the network's referral traffic, but each practice refers 80% of its patients to the network. In this scenario, each practice considers the delivery network to be its first priority in establishing connectivity. Does ONC expect that the delivery network will hire some number of extra temporary staff to arrange, set up, test, and validate the hundreds of connection requests, or is the delivery network permitted to prioritize the list of requestors? Should prioritization take into account the needs of the requester, or only the needs of the organization servicing the request? Is there an expected period of time in which a request must be served? Even if the healthcare delivery network was already an active member of a thriving exchange community, the process of providing each requester with "a detailed written explanation of the reasons why the actor could not accommodate the request" imposes a heavy burden.

On the other hand, we believe this exception, as worded, disincentivizes taking steps to support data exchange, especially by small organizations. Consider ONC's example of a small practice that does not have the technical or staffing capacity to support requests to interoperate--because the practice is small and has not chosen to invest in the necessary connectivity capability, they would qualify for this

Exception, and they have no motivation to ever address the gap in interoperability.

Custom Development
Similarly, the preamble suggests that health IT developers, exchanges, and networks whose "business it is to develop and provide technological solutions" do not take on substantial burden in supporting custom development when it is requested. On the contrary, custom development that is created for one user introduces a much higher burden than standard development that can be used by that developer's entire user community. Development, whether it is custom or not, incorporates design work, requirements analysis, writing code, reviewing code, testing the new code, testing any old code related to the new code to ensure it continues to function as expected, running usability tests, packaging code, updating documentation, creating training materials, potentially resubmitting the finished product for certification, and then maintaining the code over the lifetime of the release, including accounting for support staff who may be less familiar with the functionality because only one site is using it. Additionally, prioritization of custom development comes at the cost of disadvantaging the rest of the developer's users.

Therefore, "custom" does not always mean a small amount of work, while it eliminates the economies of scale that are achieved through more standard development.

Imbalance of Requestor versus Requestee
Regardless of size, this exception seems imbalanced, favoring the requester who wants to exchange data over the actor they approach. Indeed, a first-to-request mentality seems most advantageous, as the original requester bears no obligation for response, can set the terms of the technology, etc. Rather, the burden sits with the requestee who is at risk of being reported for information blocking if their response does not satisfy the arbitrary preferences of the requestor.

The EHR Association seeks more information as to the explicit expectations of both the actor and the requester; and, specifically, we recommend an approach that more fairly balances the concerns and judgement of burden between the two. ONC should include in the final rule more detailed guidance as to what would be considered "reasonable," and create a mechanism through which industry stakeholders can seek and receive clarification from ONC and/or OIG on detailed examples.

Overall, we support the acknowledgement that unreasonable requests to exchange data should be treated as such, but this exception is worded so generically that we fear there will be significant variability in how it is interpreted. Rather than attempting to define what is unreasonable, we suggest that an explicit safe harbor be granted--for example, if the actor accused of information blocking is a member of a widely used exchange network, it should be sufficient that the actor advertises this route to all parties wanting to exchange clinical information, without providing a detailed list of reasons why a standards-based open network is more scalable than a one-off custom connection.

Enforceability and Administrability
Also, EHR Association members have serious concerns about the enforceability and administrability of this provision and the resources of OIG to do so. We foresee this being a very commonly claimed Exception, and a timely and clear response to any filed complaint is going to be very important to the

implicated bodies.

§ 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.

(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.

(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:

The EHR Association appreciates the recognition that health IT includes intellectual property or other products which might need to be licensed for use. However, the breadth of interoperability elements subject to this provision give us grave concerns about its detrimental effect on innovation in the industry.

Also, we are concerned that the proposal lacks an important voluntary aspect, critical to use of RAND.

RAND License Terms

ONC proposes that offering RAND license terms would be a way to avoid other licensing practices which might implicate information blocking. First, the penalties associated with information blocking seem to make this RAND license effectively required. Second, this is inconsistent with the usual use of RAND or FRAND terms, which rely on a voluntary decision by the property holder to license with the expectation of their property being accepted as a standard and thus achieving more widespread use and licensure than it would otherwise. The effective compulsory licensing of health IT on RAND terms is a significant overstep.

The difference between the standards development world ONC cites as an example and the proposed mandates in our sector of the software industry is that of volunteership. Normally, in a standard-setting context, we choose whether to contribute our technology to a project and make it part of a standard. If adopted, the quid pro quo is that we will offer Fair RAND (FRAND) terms. Here, however, the proposal is that a large portion of our technology (given the broad definition of "interoperability elements") is subject to FRAND on a compulsory basis. The approach ONC proposes here is very different from that taken in other IT and computing sectors.

Patents, copyrights, trade secrets and other intellectual property are property; property that cannot be taken without due process. Compulsory licensing has happened in the past in very specific situations, but always via an act of Congress. Congress, in drafting the 21st Century Cures Act, did not choose to take that extreme step, and we believe this proposal exceeds Congressional intent.

ONC's justification for this approach refers to the "power dynamics" that exist in the health IT market, though what those power dynamics are is not clearly defined. We strongly believe the approach is problematic and far beyond Congressional intent within the 21st Century Cures Act.

Negative Effect on Innovation

Further, EHR Association members suggest that the proposal would actually provide severe disincentives for established companies to develop new, forward-leaning solutions. We strongly encourage ONC to refer to the history of such an approach within the pharmaceutical industry: when mandatory IP donation and caps on pricing were enforced, development of new drugs within the sectors placed under limitation virtually stopped overnight. The pipeline of new medications in those areas slowed significantly, and Wall Street's valuation of associated companies dropped, having measurable impact on the company's status as stable employers. It is clear that this overly-severe approach, as proposed, would have a chilling effect on investment in innovation.

Along those lines, ONC seems to imply in several places throughout the rule that it is only small, emerging companies outside of our current space that innovate. This is false. Innovation emerges from a variety of places within the industry and in companies of all sizes, and there is also an innovation ecosystem that relies on strong partnerships between companies of all sizes and tenures. Few entrepreneurs or companies evaluating expansion into health IT would be interested in pursuing it if they were aware that their IP would be no longer controlled by them and that their opportunities for profit would be wholly limited. Simply, we risk the progress we wish to see in healthcare by putting a lid on innovation.

The proposal minimizes the role of intellectual property in innovation, and the role they play in inciting interest in investment in new technologies. For instance, the NPRM states,

> *"Similar concerns arise when actors who control proprietary interoperability elements demand royalties or license terms from competitors or other persons who are technologically dependent on the use of those interoperability elements. As discussed in section VIII.C.5 of this preamble, to the extent that the interoperability elements are essential to enable the efficient access, exchange, or use of EHI by particular persons or for particular purposes, any practice by the actor that could impede the use of the interoperability elements for that purpose —or that could unnecessarily increase the cost or other burden of using the elements for that purpose— would give rise to an obvious risk of interference with access, exchange, or use of EHI under the information blocking provision."*

When you consider that "interoperability elements," as defined in the NPRM, refers to "any means by which EHI can be accessed, exchanged, or used," this amounts to virtually any piece of technology that engages EHI on some level. Conversely, the "purpose" for which a competitor may wish to access those "elements" is not reined in at all. This is imbalanced and unfair. The natural result of these proposals moving forward would be lawsuits contesting the validity and arguing the overreach of the regulation. This would not be beneficial to the industry.

ONC's stated concern is that a third party might see its costs increase if it has to license the intellectual property from a competitor or another developer. Intellectual property protections such as patents are, by their very nature, supposed to provide protection to the investing entity by allowing them to charge for the use of their differentiated technology, and this is clearly a model followed by countless companies around the world. ONC has suggested that any cost charged should be "reasonable." As already included in our comments, we ask, what is "reasonable?" Does "reasonable" (or the acceptable profit) change based on the overall profit of the company? If a company hits hard financial times and needs to make more money, would their "reasonable" be different from that of a company that has experienced great financial success? The arbitrary and undefined elements here, again, cause us concern.

Looking past our sizable concerns about the overall approach, we offer feedback and seek information on several elements of the proposal.

EHR Association members appreciate the supplied example of an app store charging fees based on RAND terms to access and use APIs. We note, however, that the text of this Exception is long and written so generically that we struggle to interpret how it would apply in other scenarios, and we request that ONC provide several more examples of behaviors that would qualify for the exception.

We request clarification as to whether this Exception would require RAND licensing of the following:

- Standards-based APIs related to ARCH resources
- Standards-based APIs generally
- Existing developer-specific and/or commercially available APIs
- COM APIs or other, non web-service based APIs
- APIs used for elements outside of specific certified health IT
- Use of the software outside of APIs

We are concerned ONC's proposal (and example) leaves open practices, which other parties could take, that would run counter to the goals of information sharing. For example, a health IT developer could not charge more in their app store for an application that acts as a passthrough to the other applications and disintermediates the app store itself, while not being subject to the same regulatory overhead or restrictions.
We specifically point out that there is little incentive for EHR developers to provide APIs or other interoperability elements above and beyond what is specifically required, given the barriers that ONC has placed to making those APIs financially viable.

Lastly, we are aware that ONC has come to the conclusion that because there is no exception specifically for IP protection under Section 4004 of the 21st Century Cures Act that the approach taken in the NPRM is the only option. We are confident that is not an accurate interpretation; ONC has regulatory authority to interpret the appropriate balance between Congressional intent--which was not so extreme--and the regulatory levers to be applied to the industry. We believe a middle ground exists that is not as severe an approach; for example, focusing open licensing of IP where the use of the IP is *necessary* (i.e., no commercially reasonable alternatives exist) to exchange patient data (and not broader use of all inclusive "EHI") would be more aligned with the goals of the Cures Act.

§ 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:

The EHR Association appreciates the inclusion of this Exception, as it allows for the necessary system maintenance and improvements. It is positive that ONC recognizes that throttling is a reasonable approach to maintain access to mission-critical and safety-critical functionality, and we support the concept of agreed-upon, client-by-client setups according to their best interest.

We ask that ONC explicitly reflect in the final regulation allowances for the fact that downtime is tied not only to the technologies directly under the jurisdiction of this proposed rule but others: cloud services, network lines, Microsoft Windows, AIX patches, etc. Further, it is possible that a provider organization causes an issue within its own configuration--such as through a forgotten patch or inappropriate configuration--which then affects the performance of their EHR. ONC should clarify that those affected by downtime, but not responsible, are not information blocking.

Also, we strongly encourage there to be an explicitly-clarified association between the Security and Performance Exceptions for instances such as a malware attack (or suspected malware attack). Health IT vendors or others hosting HIT must be allowed to take down a system in question without providing advanced notification to end users. In these situations, every second counts.

Additionally, we seek clarification to understand what "as soon as possible" means. There are various timeframes for which a system may be down, depending on the exact maintenance activity or urgent need for a fix. A quick update could take only minutes, whereas an on-premise upgrade could be multiple days. If a maintenance period is planned for a certain timeframe and is completed a few minutes early, it does not seem appropriate to consider sticking to the published schedule to bring the system back online information blocking. Without more guidance on the meaning of "as soon as possible," it would encourage a conservative, self-protective approach that could slow down the ability to respond to threats. We request guidance prior to OIG action.

Also, we do not believe adjudication of any complaint should be the first place that more detail is put behind the included terms. A significant hole in this proposed rule is the total lack of information as to how complaints will be investigated, determined worthy of prosecution, adjudicated, and resolved.

Lastly, we note that the Exception as drafted contains no provision for mistakes. It is possible that a client or software developer may make a mistake in loading a new version of software, for example, that would require the system to be down for some period of time. In this example, there is no intent, but the information would not be available and could be construed as "blocked." We recommend including the specific allowance for accidental down-time.

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

Public Comment Field:

Congress, through the Cures Act, directed the National Coordinator, in collaboration with NIST and other HHS agencies, to convene public-private and public-public partnerships to build consensus to develop or support a trusted framework, including a common agreement, as an intentionally *voluntary* agreement to facilitate the sharing of data among different healthcare information networks. As proposed, requiring developer participation in the Trusted Exchange Framework and Common Agreement (TEFCA) to demonstrate a lack of information blocking would deviate from the original Congressional intent.

While the EHR Association generally acknowledges the positive benefits of connecting networks under a common agreement, we note that the framework should be reexamined with significantly more scrutiny if participation is required (which, as stated, we do not support), as the terms and conditions would essentially act as regulation incorporated by reference. Voluntary programs can reasonably push faster and further because there is the opportunity not to participate should a company or organization find themselves unable to comply without undue burden. For now, without more specific technical information on the nature of a developer's participation, we cannot endorse required participation.

We note that already, even without TEFCA, exchange is occurring by all measures, including ONC's own measures. This is partially due to the rise of existing frameworks, such as Carequality and CommonWell, and we recommend ONC focus on supporting, encouraging, and increasing participation in already existing successful networks as permissible, and considered desirable under the Cures Act, rather than developing a new framework. Taking a new approach and mandating participation would inadvertently undo years of progress and stamp out innovative solutions that are already achieving success at scale.

Also, in some networks, health IT developers are not the primary participants in a network but rather enable and support their clients to be the primary participants. In other networks, the health IT developers are among the primary participants or are the only primary participants. All network forms are demonstrating they can effectively achieve the intended intra- and inter-HIN data exchange and access.

If ONC wishes to encourage vendor participation in TEFCA or chooses to require developer participation against this advice, it could be considered that participation would connote satisfaction of other Information Blocking requirements. Participation could be called out specifically as a safe harbor for developers and providers alike in regards to other information blocking provisions. For example, an organization could indicate publicly their participation in a participating HIN rather than needing to respond to individual requests to connect.

Request for information on new exceptions

We welcome comment on any potential new exceptions we should consider for future rulemaking. Commenters should consider the policy goals and structure of the proposed exceptions in this proposed rule when providing comment. We ask that commenters provide rationale for any proffered exceptions to the information blocking provisions and any conditions an actor would need to meet to qualify for the proffered exception.

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

Regulatory Impact Analysis: Not applicable

Public Comment Field:

With so many of the rule's expectations and definitions unclear, and without guidelines from the HHS Office of the Inspector General on when an information-blocking investigation or prosecution would be triggered, stakeholders will be understandably anxious and bewildered.

Because the penalty for information-blocking is so significant, it is imperative that ONC and OIG provide specific guidance on what is and is not acceptable. EHR Association members propose a grace period, during which time organizations could anonymously submit questions about the application of such terms to practical, real-world examples, which would be answered publicly to further educate stakeholders.

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:

ONC indicates that its goal in this rule is to be "clear, predictable, and administrable" in order to avoid undue burden on stakeholders. This is an important goal that EHR Association members strongly support. However, the ambiguous language throughout the proposal jeopardizes this goal and will unnecessarily complicate the complaint process. We make three suggestions to address this concern:

1. ONC should address as much ambiguity as possible in a final rule. To ensure this is achieved, EHR Association members suggest a second round of public comment to aid in further clarification. Because of the vague language, as well as several other elements within the Exceptions section that we anticipate will cause significant market confusion, the industry will need *many* more examples to be included in the final rule for us to have confidence in accurate interpretation. At that point, we will need an opportunity to then provide feedback on those examples before any structure is finalized.

2. After the final rule, an ongoing process for clarification needs to be established where actors can anonymously request authoritative guidance from ONC or OIG on whether a practice implicates information blocking. The guidance should be public so that all stakeholders can benefit from this information.

3. A time period of enforcement discretion should be established for this necessary guidance to be propagated and for claims to be investigated in an educational manner, without financial

penalties.

Consistent with these recommendations, initial complaints should be provided a time period for education and corrective action plans.

Additionally, to avoid trivial complaints wasting the time of investigators and actors, we suggest that complainants be required to collect sufficient evidence of intentional information blocking action.

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: It is unclear where a penalty under the information blocking regulations duplicates any penalty under other programs which requires that a provider not information block.	

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	

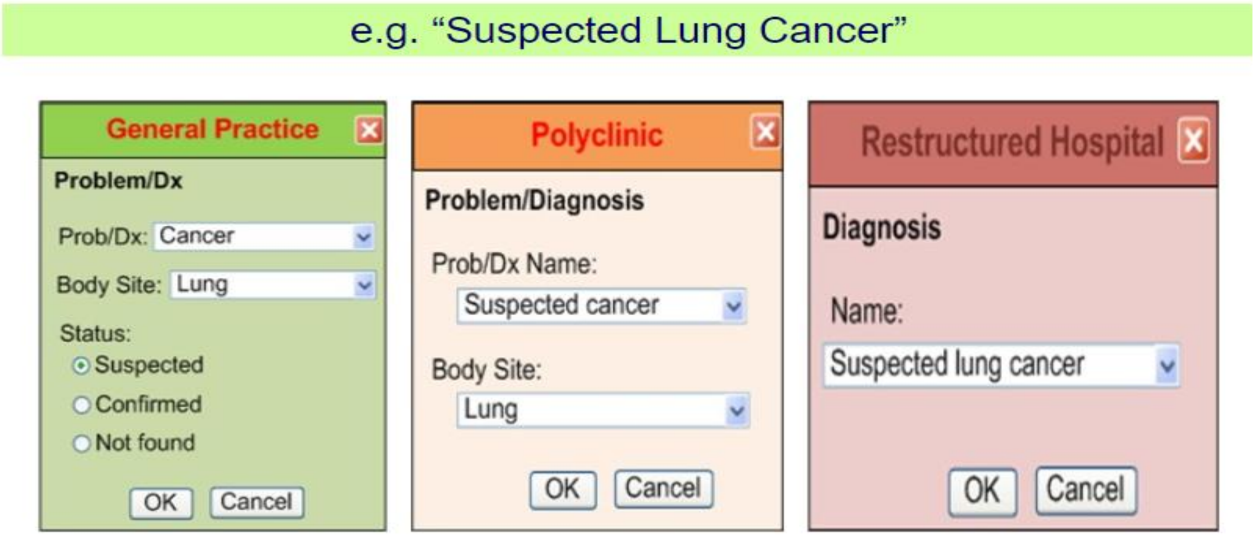
Public Comment Field:

The EHR Association agrees that having a standards-based approach will be very beneficial for connecting to all other registries. It will help to reduce the burden on both EHRs and registries.

However, whether FHIR R4, plus associated implementation guides, is the appropriate standard to use is not as relevant as focusing on what is necessary to reduce friction and burden when supporting registry data requirements. Regardless of format, the fundamental issue to address is the variation in data definitions and formats, plus additional documentation requirements, to satisfy the registries' data needs.

While EHR developers are increasingly adding support for FHIR, we remind ONC that the EHR developer is only one half of the registry puzzle. If registries do not add support for FHIR, it negates the point of EHRs to invest significant development resources in doing so. Converting existing registries to the use of new standards is a process that takes political capital, time, and development investment that many registries do not have. We urge ONC to survey the state landscape more completely before committing to a move that registries may not support and would not solve the core challenges. Also, we point out that while states may be forced via regulatory pressure to update their registries, no such carrot-and-stick arrangement exists with registries created by specialty societies.

Secondly, registries often need bespoke implementations; not because their underlying technical standards are necessarily different, but their data models are inconsistent, both in definition and in granularity across registries. This example from Dr. Linda Bird (retrieved from https://slideplayer.com/slide/10958717/) illustrates one common problem in describing a common finding such as "suspected lung cancer:"



e.g. "Suspected Lung Cancer"

General Practice

Problem/Dx

Prob/Dx: Cancer

Body Site: Lung

Status:

● Suspected

○ Confirmed

○ Not found

OK Cancel

Polyclinic

Problem/Diagnosis

Prob/Dx Name: Suspected cancer

Body Site: Lung

OK Cancel

Restructured Hospital

Diagnosis

Name: Suspected lung cancer

OK Cancel

Similarly, registries also take different approaches to how much preprocessing is required of the data source. Consider this example of a registry asking for a patient's age at the date of an event:

- Approach 1 (simple, modular, preferred): Patient DOB, Event Date
- Approach 2: Patient age at event
- Approach 3 (requires mapping and re-coding): Patient is > N years old at date of event

If ONC wishes to solve the problem of registry-specific solutions, it should focus on first gathering a list of standard data elements across all programs and then encourage reuse of those standard data definitions, similar to the work CMS is attempting with the Data Element Library.

In addition to the data model challenges that require reimplementation for each registry, we point out the challenges faced by providers and developers alike when similar registries require different or even contradictory processes. EHR Association members recently completed a state-by-state landscape of the many different policies, procedures, and mandates for prescription drug monitoring programs. The differing requirements for who must enroll in PDMPs, the requirements for queries, the data that must be reported, and the included drugs results in a patchwork approach that is complicated, confusing, and prone to mistakes.

There is already significant support and live use of successful registry implementations, including bi-directional interfaces. It would be tremendously wasteful to throw away these achievements in order to support a new technical standard that is not yet proven in the space. A small, well-defined use case, perhaps with a net new registry that includes FHIR R4 and also addresses the challenges of varying data models, policies, and procedures, would be much more appropriate.

We recommend that registries be encouraged to find common ground, sharing data definitions for common concepts and aligning those with documentation requirements already in place for providers. We recognize that for certain research objectives, new data may need to be collected in the context of specific participating providers (who then presumably would not object to collecting that extra data) and specific patient cohorts.

Further definition of those criteria could enable EHR developers to improve upon tailored and focused data collection, while building on existing common datasets wherever possible.

If ONC moves to requiring FHIR R4 without addressing these underlying challenges, we will have added significant development work to the industry without the promise of real gain. Again, we support the transition to R4 in the right timeframe and are engaging many resources within our own companies and industry standards development work; we simply point out the critical need to address - in parallel - the other issues that cause disconnection with registries.

Finally, we point out that the price limitations proposed in the rule remove incentives for efficiency and efforts to lower cost for registries, as interoperability actors, just as they do software developers.

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 seek input on the potential effect that data collection standards may have on the quality of health data that is captured and stored and the impact that such standards may have on accurate patient matching.

In general, standardized data collection and formatting makes it easier to match patients across systems; formatting differences such as "100 South First Street" and "100 S 1st St" can confuse a matching algorithm. The EHR Association supports efforts to define more standard data elements and to constrain the formatting for those elements to aid in consistency.

We seek input on what additional data elements could be defined to assist in patient matching as well as input on a required minimum set of elements that need to be collected and exchanged.

The EHR Association supports the inclusion of phone number and address elements in the USCDI demographic dataset. However, we caution ONC that, especially as demographic elements are added, it becomes less likely that any one patient will have all of those elements: certain populations do not have a phone, an email address, or even a physical address. Therefore, any discussion of a minimum dataset should consider how to account for these populations. Additionally, ONC should balance the need for a minimum data set with the documentation burden that could be introduced by requiring it. No minimum should be required without specific evidence supporting that minimum.

Also, we suggest that ONC work with providers to educate them--specifically within the context of patient identification and matching--on the value of collecting as much as possible of this data, as it cuts down on back-end data cleanup, incomplete data sets, etc. There are several recent studies (from Intermountain, The Sequoia Project, The Pew Foundation, and RAND) that demonstrate that improved data collection for standardized fields and key fields, wherever possible (such as validated cell phone numbers), substantially improves matching. Sharing this information with clinicians and users documenting patient demographics would help them better understand the return for what they consider to be unnecessary work.

We seek input on whether and what requirements for electronic health records could be established to

assure data used for patient matching is collected accurately and completely for every patient.

The EHR Association reminds ONC that data collection is a process owned by the healthcare delivery organizations, as is the data itself, not the electronic health record developer. Developers can facilitate the collection and use of this information; but, in most instances, we do not own or control the data.

We seek comment on potential solutions that include patients through a variety of methods and technical platforms in the capture, update and maintenance of their own demographic and health data.

The EHR Association, too, is interested in exploring solutions that include patients. If ONC pursues the use of data held outside organizations for the purposes of patient-driven matching, we believe ONC should provide guidance to those data sources about the need to protect such data and support patient privacy and consent.

We seek input on transparent patient matching indicators such as database duplicate rate, duplicate creation rate, and true match rate, for example, that are necessary for assessment and reporting.

While the EHR Association generally supports more standardized metrics for patient matching, we question the necessity of requiring organizations to go through the bookkeeping exercise of defining, collecting, publishing, and updating these metrics, especially given the overall value of these metrics compared to other metrics more directly tied to clinical outcomes.

Also, we note that certain settings may lead to performance that are not easily generalizable when compared across other settings. For example, an extremely busy emergency department might routinely create temporary records for new arrivals that are later merged back into existing patient records once the patient is stabilized and more information can be collected. Such a setting would have inflated duplicate creation rates, compared to a specialty setting that only takes referrals; similarly, an EHR that supports this workflow would have higher duplicate creation rates comparatively.

Appendix: Pediatric Technical Worksheets

The appendix is published in the *Federal Register* at 84 FR 7605-10 but (as noted at 84 FR 7610) will not appear in the Code of Federal Regulations. The appendix is included in the unofficial copy of the proposed rule is also available in Microsoft Word format on ONC's website at https://www.healthit.gov/sites/default/files/page/2019-03/ONCCuresActProposedRule.docx to help enhance the commenting experience.

As noted in the proposed rule (at 84 FR 7461), additional information on prior ONC initiatives related to health IT for pediatric settings as available from the ONC website at https://www.healthit.gov/pediatrics.

Recommendation 1: Use of biometric-specific norms for growth curves

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association agrees that the proposed USCDI aligns with the prerequisite data collection in this proposal, but not the "calculate" and "display" parts.

The Demographics and CDS criteria do not seem aligned with this proposal. The API criterion is tangentially related.

Recommendation 2: Compute weight-based drug dosage

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association agrees that the proposed USCDI criterion captures relevant data elements to support this requirement.

We do not agree that the electronic prescribing criterion aligns with the ability to compute weight-based drug dosing. The electronic prescribing criterion is used to ensure transmission of medication order information, not the ability to compute the dose in the first place.

Recommendation 3: Ability to document all guardians and caregivers

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The Care Plan, Transitions of Care, and Demographics criteria listed may be related to this requirement, but they do not meet it. They do not require the system to capture or store information about a patient's guardians and caregivers in a standard way.

The USCDI includes "history" as a note type and "care team," but it does not include information about guardians and caregivers. While this information could be captured in a note, it is not clear how requiring the USCDI criteria adds value toward meeting this requirement. It would be more valuable if the data was captured in a standard manner.

EHR Association members request clarification on how the API or DS4P criteria are more than tangentially applicable to this requirement.

Please see our concerns about data segmentation elsewhere in the document.

Supplemental Children's EHR Format Requirements for Recommendation 3

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association agrees that the recommendations seem to be aligned with the requirement.

Recommendation 4: Segmented access to information

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association suggests prioritizing electronic consent prior to adopting this recommendation. Please see our concerns about data segmentation elsewhere in the document.

Public Comment Field:

The EHR Association agrees that the existing criteria appear to align with the Requirement. However, we believe that including the API criteria seems problematic. For example, how would we restrict certain data elements if a parent has access to the API?

We are similarly concerned with this inclusion in the USCDI, as the specific data elements listed within requirement 4, do not appear to be covered in USCDI. We find that the data segmentation criterion seems to be relevant.

Please see our concerns about data segmentation elsewhere in the document.

Supplemental Children's EHR Format Requirement for Recommendation 4

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

EHRs are not well positioned to provide access to local, legal guidelines on consent. Instead, this content should be managed by a central group, such as ONC, so that every EHR or health system is not attempting to keep the same materials current. Ideally, machine-readable versions of the privacy and consent policies of state and local jurisdictions would be available for health IT developers and providers to use in consistent interpretation and implementation.

Recommendation 5: Synchronize immunization histories with registries

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association agrees that the existing and proposed criteria are relevant to the recommendation.

Supplemental Children's EHR Format Requirement for Recommendation 5

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The identified relevant criteria of View, Download, and Transmit and the API criteria do not have a requirement associated with the ability to produce immunization history reports.

Recommendation 6: Age- and weight-specific single-dose range checking

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association believes that the existing criteria alignment with clinical decision support seems appropriate. However, we question the alignment of the API criteria.

Additionally, EHRA finds that the proposed criteria related to USCDI seem misaligned.

Recommendation 7: Transferrable access authority

Public Comment Field:

The EHR Association does not believe the existing criteria align, as this recommendation deals more with security functions. The proposed criteria related to data segmentation align; however, we see no alignment with the cited API criteria. Please see our concerns about data segmentation elsewhere in the document.

Supplemental Children's EHR Format Requirement for Recommendation 7

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association agrees with the supplemental requirements. However, we would like to point out that it does not align with the demographics criteria, since the current criteria have no requirement to record a patient's emancipated minor status.

Recommendation 8: Associate maternal health information and demographics with newborn

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association finds that none of the existing criteria are representative of Recommendation 8, as none of the criteria require the functionality specified by Recommendation 8.

Recommendation 9: Track incomplete preventative care opportunities

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association does not see alignment of any of the existing or proposed criteria, particularly with the Bright Futures recommendations, since no certification requirement currently cover these capabilities.

Recommendation 10: Flag special health care needs

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

The EHR Association finds alignment with the existing criteria related to clinical decision support and problem list, but no alignment with clinical quality measures. We could not identify a single CQM that aligned.