Detailed Comments of the Connected Health Initiative on the Office of the National Coordinator for Health IT's

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

Section III – Deregulatory Actions for Previous Rulemakings

Removal of Randomized Surveillance Requirements
We propose to revise § 170.556(c) by changing the requirement that ONC-Authorized Certification Bodies (ONC-ACBs) must conduct in-the-field, randomized surveillance to specify that ONC-ACBs may conduct in-the-field, randomized surveillance. We further propose to remove the following: • The specification that ONC-ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year. • Requirements regarding the exclusion and exhaustion of selected locations for randomized surveillance. • Requirements regarding the consecutive selection of certified health IT for randomized surveillance. Without these regulatory requirements, ONC-ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, using the methodology identified by ONC with respect to scope and selection method, and the number and types of locations for in-the-field surveillance.
Preamble FR Citation: 84 FR 7434 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Please see 84 FR 7562-63 for estimates related to the removal of randomized surveillance requirements.
Public Comment Field: CHI supports the removal of randomized surveillance because new and more detailed conditions and maintenance of certification requirements have been proposed. We highlight that removal may increase physician responsibility to flag certification issues. ONC should develop additional education and guidance to help physicians know what would be considered in and out of conformance with certification. We also worry that, since ONC has not chosen to implement Cures' Electronic Health Record (EHR) Reporting Program provision, physicians will not have a "go-to" resource to report or learn about EHR issues. We recommend that ONC direct ONC-ACBs to engage in reactive surveillance when users report usability, safety, security, privacy, or interoperability concerns openly (e.g., as described by Cures § 4002. Transparent reporting on usability, security, and functionality).

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:

CHI supports removal of the identified criteria and standards from 2015 Edition criteria for the reasons articulated by ONC and because CMS removed requirements to use some of these listed criteria.

We disagree with ONC reasoning to not propose a new Edition designation. We question why ONC proposed to modify the 2015 Edition as opposed to creating a new Edition. ONC is proposing broad-sweeping changes to the 2015 Edition. By not updating to a new Edition, users of the Certified Health IT Product List (CHPL) will be confused about which version of 2015 Edition is being referenced. ONC should release a new Edition given the substantial changes being proposed. We recommend a 2020 Edition or the corresponding year in which this rule is finalized. HHS should direct its agencies to update regulations to reflect the new Edition.

Removal of the ONC-Approved Accreditor from the Program

We propose to remove the ONC-Approved Accreditor (ONC-AA) from the Program, including definitions, processes, and references to ONC-AA throughout the rule. This proposal also includes removing the final rule titled "Permanent Certification Program for Health Information Technology; Revisions to ONC-Approved Accreditor Processes" (76 FR 72636). Because this prior final rule relates solely to the role and removal of the ONC-AA, we propose removing § 170.575, which codified the final rule in the CFR.

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

Regulatory Impact Analysis: Please see 85 FR 7564-65 for estimates related to this proposal.

Public Comment Field:

No comment.

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:

CHI disagrees with ONC's proposal to remove from the 2015 Edition Criteria the problem list, medication list, medication allergy list, drug formulary, and smoking status requirements. EHR vendors must be required continue to support these requirements especially with the Tobacco Use: Screening and Cessation Intervention measure. This measure has recently changed from recording all patients screened regardless of tobacco use to just patients who screen positive for smoking and measuring cessation intervention at each patient encounter. Measure 226 is the second most commonly reported measure in the Merit-based Incentive Payment System (MIPS) by eligible clinicians across all quality reporting mechanisms including CMS Web Interface. Based on the 2017 Quality Payment Program (QPP) Experience Report, close to 500,000 eligible clinicians selected this measure in the first performance year.

Moreover, CHI recommends ONC remove barriers limiting Systematized Nomenclature of Medicine (SNOMED) categories for smoking status. We note that documentation mechanisms in EHRs do not account for length and duration of smoking and that any simplification of the current SNOMED codes could have unforeseen consequences and impacts. We believe addressing SNOMED code limitations will improve EHR usability and help reduce smoking.

Furthermore, ONC should coordinate with measure stewards, including national medical societies, on the development of future quality measures. Medical specialties should not be required to dilute measure development due to delinquencies in EHR data capture.

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:

CHI supports ONC's proposal to, as a complementary Condition of Certification, prohibit developers from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification.

We do not support ONC's proposal to remove Principles of Proper Conduct (PoPC) in § 170.523(k)(2), which requires health IT developers to submit an attestation validating compliance with mandatory disclosure requirements (ONC reasons it is no longer necessary since health IT developers are readily complying with the requirements). However, our experience is that PoPC requirements are themselves the motivating factor and therefore should continue to be enforced. We recognize the need to reduce burden, but an attestation (which ties a developer to their actions) is not burdensome. Additionally, ONC should refrain from actions that reduce transparency. At a time when the Administration is calling for more transparency across the health care continuum, we find it perplexing that ONC is proposing to remove a key transparency requirement from EHR vendors.

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 FDA's Pre-Certification Program is a risk-based regulatory framework to facilitate software as a medical device (SaMD). We understand the volume and rapid-cycle iterative improvements in SaMD dictate a new approach that would allow the FDA to streamline oversight for lower risk products while allocating scarce resources to the highest risk regulated digital health tools. CHI notes that a confluence of factors is driving the need to develop alternative options for regulatory oversight of SaMD, including the rapid iterations in SaMD, the capability of SaMD supporting technologies to track post-market impact, and the proliferation of SaMD which is outpacing regulatory agency capacity to review and surveil.

However, we note that health IT development and use should not be conflated with SaMD. Congress specifically carved many health IT components out of FDA's jurisdiction (e.g., EHRs). The FDA has pivoted from what most would consider "traditional health IT" to other aspects of digital health (e.g., SaMD, Artificial Intelligence (AI), digital therapeutics). This is not to say EHR development will not eventually incorporate AI or other technologies that intersect with the FDA. However, the Pre-Certification Program is still early in its first full year of operation, having received SaMD technology applications by way of its pilot participants. We note that none of the pilot participants are considered EHR vendors. As such, we do not believe the FDA has contemplated the full picture of EHR user needs in Pre-Certification, nor has the Pre-Certification Program experienced applicants representing EHR vendors or their users' interests.

We also have concerns with the potential for entities to get "certified" to ONC health IT requirements when they have not first had experience going through ONC's certification testing process. FDA's Pre-Certification Program specifies that a business unit or business center—not the actual product or application—is granted precertification status. Organizations that have not successfully deployed certified EHR products (CEHRT) should first demonstrate that they are able to deploy such software safely through ONC's existing oversight process. Circumventing this process would degrade trust in ONC's oversight and would fail to provide a documented track record of performance or accountability.

We do not agree that the FDA's Pre-Certification Program sufficiently aligns with ONC's Program. We further do not believe ONC could properly operationalize an ONC/FDA-hybrid approach and ensure certifications indicate which criteria have been "deemed certified" by ONC, but still subject to ONC-ACB surveillance. We believe focusing on whether a company or organization excels in software design, development, and validation (testing) are important components. We also believe that the track record of the developer's products is equally important; thus, post-market active sentinel capabilities with organized feedback loops—easily captured by regulators as well as developers—are essential. ONC's current program and proposed changes to Conditions of Certification and Maintenance of Certification, while not perfect, are better facilitators of real-world use, feedback, and iterative design.

An additional concern regarding the application of the pre-certification program to health IT developers is the impact on the viability of any potential false claims act cases. A large deterrent in making false statements to the federal government is the false claims act. However, under a "recognition" program, no false statement as to the capability of a CEHRT is actually made. Thus, as it relates to false statements, cases like eClinicalworks and Greenway would not be viable under the false claims act because no statement was made regarding the capability of a CEHRT. Instead, the business reputation is evaluated. For example, in Greenway, the Department of Justice alleged that Greenway falsely represented to the certifying entity performing the testing and certification that its software met the required certification criteria. If, however, Greenway or any other health IT developer participated in the "recognition" program, it would not make any certification or statement as to whether its products meet the certification requirements.

We recognize that some EHR vendors (e.g., eClinicalWorks, Greenway Health) were accused of falsifying ONC certification, which included product testing. However, we view this as an additional reason why health IT developers, and entities new to the EHR space, should not be provided a less stringent path to certification than is currently available. If anything, ONC should intensify its testing and validation of health IT products.

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 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: CHI notes its comments above regarding the potential cross-walking of the FDA Pre-Certification Program (and evaluating of an organization's process as opposed to each individual module/product produced in that process). We support the concept of a streamlined approval approach that would consider organizational trustworthiness through quality assurance and interoperability "by design" practices, but believe that such a process requires further thought and input before being put into place; therefore, we request that the development of such a "similar independent program" be addressed in a future ONC rulemaking.

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:

CHI supports the use of the USCDI in place of the Common Clinical Data Set, and further supports the proposed additions of address and phone number, pediatric vital signs, clinical notes, and provenance. Our specific comments include:

- Regarding address, CHI urges for the utilization of the U.S. Postal Service standard, and for addresses to be noted by type (home, office, etc.). Regarding phone number, we similarly urge that type be noted (home, mobile, etc.). CHI also suggests that ONC consider including patient email. Such information is typically provided in FHIR APIs today.
- CHI urges ONC to support clinical notes being made available to patients through APIs using the HL7 Argonaut Project's implementation guidelines, but to also support notes being made available in other formats.
- CHI supports the addition of provenance. In the future, provenance should likely be aligned with relevant HL7 Argonaut Project guidelines.
- CHI urges ONC to add the Encounter data type from USCDI 1.0, which will assist in bringing clinic visit data to the patient in detailing procedures performed within that visit. Encounter data type is likely to be included in the next HL7 Argonaut guidelines to support FHIR R4.

CHI notes its support for ONC's USCDI expansion process proposed in the draft USCDI, which would occur annually based on stakeholder input. We also support the ONC-proposed "glide path" for additions to the USCDI which should reflect technology and competitive neutrality principles as it incrementally expands data classes.

CHI urges ONC to prioritize its effort to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. The accelerated addition of data classes and elements—along with additional context around these data (i.e., metadata)—is vital to meeting the goals of the 21st Century Cures Act. It is also logical to include pricing, cost, and administrative transaction standards in the USCDI version expansion.

This will support the Administration's goal to bolster a health care market economy, facilitate price transparency, and vastly expand the number of ways in which a beneficiary can access and utilize such information. Additionally, coding and terminologies that support a patient's use of his or her health information will become increasingly vital. Descriptors are available that supports the translation of medical jargon into consumer-friendly information. Immediately following the publication of its final rule, ONC should establish a formal USCDI submission, review, and validation process to ensure clinician perspectives are considered. As ONC considers the structure and processes necessary to expand the USCDI, CHI recommends ONC adopt the Health Information Technology Advisory Committee (HITAC) USCDI Task Force's recommendations dated April 18, 2018. This is a critical need to build consensus across the health care system.

We do not support requiring both health IT developers and users of certified health IT to concurrently develop, test, implement, train, and use EHRs with these updates within a 24-month timeline. Health IT development requires a separate timeline than the adoption and use of products by physicians. We suggest ONC continue to allow CMS to designate the update timeline for CEHRT. ONC should clarify that its proposed timeline does not include the 12+ months needed for physicians and other health care providers to schedule product updates/installations, test deployments, train staff, and safely use new EHRs.

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 USCDI v1 includes new data elements for "address" and "phone number". The inclusion of "address" (to represent the postal location for the patient) and "phone number" (to represent the patient's telephone number) would improve the comprehensiveness of health information for patient care. CHI strongly supports inclusion of these new data classes and data types. We recommend ONC point towards established standards for address, such as the USPS standard.

The USCDI v1 also includes a new data class "provenance." Provenance has been identified by stakeholders as valuable for interoperable exchange. ONC proposes to further delineate the provenance data class into three data elements: "the author", which represents the person(s) who is responsible for the information; "the author's time stamp", which indicates the time the information was recorded; and "the author's organization", which would be the organization the author is associated with at the time they interacted with the data. ONC requests comment on the inclusion of these three data elements and whether any other provenance data elements—such as the identity of the individual or entity the data was obtained from or sent by (sometimes referred to as data's "last hop")—would be essential to include as part of the USCDI v1 standard. CHI supports this new data class and data elements. However, we anticipate that more granularity will be needed for Provenance Data Elements, such as "role of the individual", (e.g., ordering/verifying/supervisor author) and "patient identification". Patient identification would be useful to include in provenance to track usage and ensure governance and consented use aligns with patient preference. CHI recommends ONC make "Provenance" a functional requirement, rather than a named standard given that more work needs to be done before an industry consensus standard is available.

As ONC considers the structure and processes necessary to expand the USCDI, CHI recommends ONC adopt the Health Information Technology Advisory Committee (HITAC) USCDI Task Force's recommendations dated April 18, 2018. These recommendations include:

- Establishing a six-stage maturation process through which data classes would be promoted, each with objective characteristics for promotion;
- Expanding the USCDI as each data class completes stages 1-4 without a predetermined timeline;
- Establishing an annual publishing cycle for the USCDI with periodic bulletins as data objects/data classes progress from one stage to the next;
- Incorporating public feedback in each stage;
- Testing USCDI process by addressing critical trusted exchange framework requirements;
- Ensuring the voice of the patient is represented and heard;
- Supporting the process of data object harmonization as a condition for data class advancement
- Establishing a process for data class management; and
- Establishing a governance structure for the USCDI.

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:

CHI supports requiring the new UDI IG as a requirement for health IT. The UDI for medical devices aims to improve post-market surveillance and patient safety. While we strongly support the incorporation of the UDI on medical devices, there is some debate about the most appropriate place to capture this information. CMS and the FDA have called for including part of the UDI in the next claims form template update—slated for 2021. However, certification requirements allow EHRs to capture and transmit the full UDI. CHI views EHRs and registries as the most appropriate method to capture and manage the UDI. We do not support capturing UDI information in administrative claims as it represents a significant cost to providers, as well as the industry, and claims information does not follow a patient as they switch insurers. The claims form changes would also not require the capture of the full UDI, instead capturing only the device identifier ("DI") portion and excluding the product identifier portion. Both the Production Identifier and DI are key in providing the complete picture about a medical device when safety issues arise. Capturing this information in a patient's EHR allows the full medical device information to follow patients, and their longitudinal medical history, regardless of changes in insurance.

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:

CHI supports ONC's proposal, which is consistent with the Argonaut Implementation Guide 1.0.0's approach to allergies.

§ 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:

CHI supports ONC's proposal to adopt the C-CDA Templates for Clinical Notes R1 Companion Guide, Release 1and to update identified criteria to incorporate this standard.

§ 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:

CHI supports ONC's proposal to adopt the National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 at § 170.205(b) Electronic prescribing.

We suggest that, along with certifying the rest of the SCRIPT 2017071 transactions required by CMS, ONC should require certification to the SCRIPT electronic prior authorization (ePA) transactions included in the 2017071 standard. We are aware that lack of vendor support for the ePA transactions is a major barrier to physician use of the transactions, with only 21 percent of physicians reporting that their EHR supports prescription ePA.

SCRIPT 2017071 includes the new RxTransferRequest, RxTransferResponse, and RxTransferConfirm transactions which allow for one pharmacy to request the transfer of a prescription from another pharmacy. These transactions allow the transfer of unfilled controlled substance prescriptions—including Schedule II—between pharmacies. Facilitating inter-pharmacy transfer would be useful for all stakeholders involved.

ONC discusses collaborating with the Centers for Disease Control and Prevention (CDC) on a project to translate the CDC's Guideline for Prescribing Opioids for Chronic Pain into FHIR Clinical Decision Support (CDS) Hooks in EHRs, noting that "not all states have adopted the guideline, not all physicians are aware of them, and sound opioid prescribing guidelines are far from universally followed." It is critical that physicians be allowed to override the CDS Hooks if the patient's unique clinical situation warrants departure from the guideline. These guidelines are already being treated like one-size-fits-all mandate. HHS' Interagency Pain Care Task Force has highlighted growing inability of CDC guidelines to appropriately individualize patient care. We do not support CDS Hooks preventing the physician from prescribing medically necessary, appropriate opioid treatment.

§ 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

§ 170.315(b)(11) Electronic prescribing

Public Comment Field:

CHI supports the electronic prescribing certification criterion proposed for adoption at § 170.315(b)(11).

§ 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:

CHI supports that health IT be certified to the criterion that supports CMS QRDA Implementation Guidelines (IGs). However, we recommend that ONC monitor this part of the certification process for unintended consequences since CMS' IGs are updated on a yearly basis and CEHRT only occurs every few years. Given the lack of alignment with timing, eCQM measures and standards will continue to lack testing.

To reduce burden, ONC should consider a certification approach that permits vendors to only certify to standards based on the care setting(s) they serve. If a vendor serves both in-patient and out-patient settings, then they should have to certify to both settings to meet the various demands and needs of the providers.

§ 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:

No comment.

§ 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: No comment.	

§ 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:

CHI supports this proposal generally but requests specificity as to the meaning of "all the electronic health information the health IT produces and electronically manages." CHI also requests that ONC delete "metadata that refers to data is not present in the EHI export."

There are several layers of ambiguity that will inhibit uniform implementation and widespread use of this functionality. First, we note that patients requesting an EHI export will likely obtain vastly different payloads based on three factors: (1) the health IT developers certified to deliver the export; (2) the implementation decisions and customizations at each implementation; and (3) the institution's interpretation of what constitutes EHI. Second, we note that widespread use of this functionality will be inhibited because the task of making sense of the data falls largely on patients and families, not the developers or clinicians delivering the export.

CHI recommends ONC look for ways to constrain and/or guide implementation of these policies, while keeping the intent of these policies broad and inclusive. Specifically, CHI recommends ONC:

- Constrain EHI Export to comport with HIPAA's electronic protected health information (ePHI) regulation;
- Specify that transport standard for EHI Export for Patient Access leverage RESTful protocols; and
- Include EHI Export for Patient Access (§ 170.315 (b)(10)(i)) among the requisite criteria of real-world testing plans, proposed elsewhere in this NPRM.

By specifying a functional, yet non-exclusive, set of standards for EHI (i.e., ePHI) to be made available via API, we anticipate that industry stakeholders and government regulators can work toward a standardized API for managing export requests in future rulemakings, even as the non-USCDI data payloads themselves are likely to remain developer-specific (i.e. non-standardized) for some time into the future. Further, this paradigm will encourage more innovation to make the data useful to patients and families than a single and/or periodic "data dump" as the current proposal portends.

The EHI Export for Patient Access should be tied to "HIPAA compliant uses," which would be physician access for treatment, payment, or operations for the purposes of continuity of care, and patient data access for whatever purpose they deem appropriate. We stress that until such time EHR vendors utilize an API orchestration to provide patients direct EHI export capabilities, the ability to request an EHI export be medical practice-facing. We have concerns with the potential of hundreds or thousands of users' "requests" coming into an EHR for an export. This would severely bog down an EHR's performance, putting patients at risk. Furthermore, externally-facing EHI export capabilities (i.e., download or export functions provided via patient portals), would expose an EHR to denial-of-service attacks (DoS). To be clear, patients could still request their ePHI from the medical practice, but the act of querying the EHR should be reserved for authorized users, administrators, and medical office staff. Until such time that EHR vendors have proven capable of supporting patient-facing EHI requests while also mitigating privacy and security issues, EHI Export should be protected from potential abuse or exploitation.

We do not support inclusion of "software programs or services", as a "user" in the context of EHI Export for Patient Access without express consent from the patient, the patient's legal guardian, or caregiver. Given the current regulatory gaps that exist outside HIPAA, we are concerned that health app terms and conditions could expose all of a patients EHI without the patient's knowledge or desire. In addition, ONC needs to provide clear guidance and education.

We also generally support the flexibility regarding how the outcome of a database export is achieved so long as the system provides the relevant data dictionary and documentation, as outlined by ONC, and is required to complete a Database Export as part of initial Certification and consume a Database Export as part of initial Certification. Alternatively, a certified developer could demonstrate its capacity to deliver and consume a Database Export as part of real-world testing Maintenance of Certification requirements. To meet the spirit of this criterion a certified developer should be able to perform an export relatively easily, and a different certified developer should be able to consume the export equally easily.

ONC should require health IT developers to publish as part of the export format documentation the types of EHI they cannot support for export. Without this documentation, determining what has been done will simply be impossible and over time, and never determinable.

§ 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: CHI supports the use of strong encryption to protect patient safety and agrees with ONC's proposal to have health IT developers assess their Health IT Modules' capabilities for encrypted authentication credentials. We stress that ONC should not stipulate multi-factor requirements on EHRs and continue to only seek "yes" / "no" attestation.

§ 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:

CHI support's the certification requirements proposed by ONC at § 170.315(d)(13) Multi-factor authentication. We stress that ONC should not stipulate multi-factor requirements on EHRs and continue to only seek "yes" / "no" attestation.

§ 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: CHI supports ONC's proposed § 170.315(b)(12) Data segmentation for privacy – send.

§ 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: CHI supports ONC's proposed § 170.315(b)(13) Data segmentation for privacy – receive.

§ 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: Existing standards such as Consent2Share (C2S) and Data Segmentation for Privacy (DS4P) are not being utilized due to cost, maturity, or lack of adoption. We appreciate that ONC is proposing C2S and DS4P as optional certification criteria for health IT and that the DS4P proposal requires segmentation at the element level (as opposed to the document level). We understand that DS4P is viewed as a major development challenge for EHR vendors. In discussing privacy with the Substance Abuse and Mental Health Services Administration (SAMHSA), we have learned that FHIR-enabled C2S APIs provide both physician and patient-facing services and the infrastructure to segment data and manage consent. **We support requiring C2S in Base EHR health IT certification and encourage ONC to increase C2S adoption.** We are also aware that there is no longer funding to continue this important work. **CHI recommends ONC coordinate with SAMHSA to establish a public-private project to advance C2S.** Vendors and payers have expressed the need to address "the dual challenges of data standardization and easy information access" with the goal "to help payers and providers to positively impact clinical, quality, cost and care management outcomes" (http://www.hl7.org/about/davinci/). We expect health IT vendors and payers would welcome a public-private C2S effort. We recommend an analogous process to that of the Da Vinci Project, but one that is open, transparent, and excludes membership fees. The USCDI and the Interoperability Standards Advisory should be leveraged for support.

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 V – Modifications to the ONC Health IT Certification Program

§ 170.550 Health IT Module certification

* * * * *

(e) ONC-ACBs must provide an option for certification of Health IT Modules to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification through the Standards Version Advancement Process.

(f) [Reserved]

(g) * * *

(5) Section 170.315(b)(10) when the health IT developer of the health IT presented for certification produces and electronically manages electronic health information.

(h) * * *

(3) * * *

(i) Section 170.315(a)(1), (2), (3), (5) through (8), (11), and (12) are also certified to the certification criteria specified in § 170.315(d)(1) through (7). Section 170.315(a)(4), (9), (10), and (13) are also certified to the certification criteria specified in § 170.315(d)(1), (2), (3), (5), (6), and (7).

* * * * *

(iii) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1), (2)(i)(A), (B), (ii) through (v), (3), and (5);

* * * * *

(v) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A), (B), (ii) through (v), (3), (5), and (9);

* * * * *

(vii) Section 170.315(g)(7) through (11) is also certified to the certification criteria specified in § 170.315(d)(1) and (9); and (d)(2)(i)(A), (2)(i)(B), 2(ii) through (v), or (10);

(viii) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1), (2)(i)(A), (2)(i)(B), (2)(ii) through (v), and (3); and

* * * * *

(ix) If applicable, any criterion adopted in § 170.315 is also certified to the certification criteria specified in § 170.315(d)(12) and/or (13).

* * * * *

(l) Conditions of Certification Attestations. Before issuing a certification, ensure that the health IT developer of the Health IT Module has met its responsibilities under subpart D of this part.

Preamble FR Citation: 84 FR 7454-55 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7559 and 84 FR 7582-83 for estimates related to this proposal.

§ 170.550 Health IT Module certification

Public Comment Field:

No comment.

§ 170.523 Principles of proper conduct for ONC-ACBs (Authorized Certification Bodies)

* * * * *

(a) Accreditation. Maintain its accreditation in good standing to ISO/IEC 17065 (incorporated by reference in § 170.599).

* * * * *

(f) Reporting. * * *

(2) [Reserved]

(g) Records retention.

(1) Retain all records related to the certification of Complete EHRs and Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (g)(1) of this section;

(h) Testing. Only certify Health IT Modules that have been:

(1) Tested, using test tools and test procedures approved by the National Coordinator, by an:

(i) ONC-ATL;

(ii) ONC-ATL, NVLAP-accredited testing laboratory under the ONC Health IT Certification Program, and/or an ONC-ATCB for the purposes of performing gap certification; or

(2) Evaluated by it for compliance with a conformance method approved by the National Coordinator.

* * * * *

(k) Disclosures. * * *

(1) All adaptations of certified Health IT Modules;

(2) All updates made to certified Health IT Modules affecting the capabilities in certification criteria to which the “safety-enhanced design” criteria apply;

(3) All updates made to certified Health IT Modules in compliance with § 170.405(b)(3) and (4); and;

(4) All voluntary standards updates successfully made to certified Health IT Modules per § 170.405(b)(5).

* * * * *

(p) Real world testing.

(1) Review and confirm that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1).

(2) Review and confirm that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2).

§ 170.523 Principles of proper conduct for ONC-ACBs (Authorized Certification Bodies)

(3) Submit real world testing plans by December 15 of each calendar year and results by April 1 of each calendar year to ONC for public availability.

(q) Attestations. Review and submit health IT developer Conditions and Maintenance of Certification attestations made in accordance with § 170.406 to ONC for public availability.

(r) Test results from ONC-ATLs. Accept test results from any ONC-ATL that is:

(1) In good standing under the ONC Health IT Certification Program, and

(2) Compliant with its ISO 17025 accreditation requirements.

(s) Information for direct review. Report to ONC, no later than a week after becoming aware of, any information that could inform whether ONC should exercise direct review under § 170.580(a).

(t) Standards Voluntary Advancement Process Module Updates Notices. Ensure health IT developers opting to take advantage of the Standards Version Advancement Process flexibility per § 170.405(b)(5) provide timely advance written notice to the ONC-ACB and all affected customers.

(1) Maintain a record of the date of issuance and the content of developers' § 170.405(b)(5) notices; and

(2) Timely post content of each § 170.405(b)(5) notice received publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies.

Preamble FR Citation: 84 FR 7456-57 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7559 and 84 FR 7582-84 for estimates related to this proposal.

Public Comment Field:

CHI seeks clarity from ONC as to what metrics the National Coordinator will use to approve a conformance method. We are especially interested in ONC's plan to ameliorate fraudulent certification practices (e.g., eClinicalWorks, Greenway Health) given these proposals.

CHI supports ONC's proposal to include a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities—whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification.

§ 170.524 Principles of proper conduct for ONC-ATLs (Authorized Testing Laboratories)

* * * * *

(f) Records retention.

(1) Retain all records related to the testing of Complete EHRs and/or Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (f)(1) of this section.

Preamble FR Citation: 84 FR 7457 **Specific questions in preamble?** *Yes*

§ 170.524 Principles of proper conduct for ONC-ATLs (Authorized Testing Laboratories)
Regulatory Impact Analysis: Not applicable
Public Comment Field: No comment.

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: No comment.

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:
CHI recommends focusing attention on improving the integration of prescription drug monitoring programs (PDMPs) with EHRs and to facilitate electronic prescribing of controlled substances (EPCS). Additional burden reduction can be accomplished through adoption of the PDMP recommendations included on page 17 of the HHS Interagency Pain Management Best Practices Task Force draft report:

- Recommendation 1b calls for clinicians to be trained on accessing and interpreting PDMP data, and 1c says physicians should engage patients to discuss their PDMP data rather than making a judgement that may result in the patient not receiving appropriate care.
- Regarding burden reduction specifically, Recommendation 1d states the health care provider team should determine when to use PDMP data, and that PDMP use should not be mandated without proper clinical indications to avoid unnecessary burden in the inpatient setting.
- Recommendation 1e calls for studies to identify where PDMP data is best used, with PDMP use adjusted based on the study findings to minimize undue burdens and overutilization of resources.
- Recommendation 1f calls for EHR vendors to work to integrate PDMPs in their system design at minimal to no additional cost to providers.

CHI encourages ONC to consider the Pain Management Task Force recommendations as it develops OUD regulation.

CHI also highlights the current barriers EPCS. Current EPCS regulations, which have been unchanged since 2010, prevent user-friendly devices that are widely available in medical practices from being deployed to meet the multifactor authentication standards in the DEA rules. Current regulations have also driven down EPCS adoption. We support the recommendation from the President's Commission on Combating Drug Addiction and the Opioid Crisis that the DEA should increase EPCS uptake to prevent diversion and forgery and revise the EPCS regulations. We appreciate HHS' recognition of Section 2003(c) of the Substance Use–Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (P.L. 115-271), which calls on the Attorney General/DEA to "update the requirements for the biometric component of multifactor authentication with respect to electronic prescriptions of controlled substances." Current regulations are impeding the implementation of EPCS. Removing these barriers will significantly reduce fraudulent prescriptions for opioid analgesics and increase the adoption of EPCS to combat the epidemic of opioid overdose deaths. ONC should coordinate with the DEA through the lens of reducing physician burden—with particular focus on cost, usability, interoperability, and effectiveness of EPCS system regulation.

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: CHI supports this requirement. Physicians participating in the Quality Payment Program are already required to attest to a three-part information blocking statement. This statement is detailed and ties a physician's attestation to their EHR vendor's capabilities. For instance, physicians must attest they "implemented in a manner that allowed for the timely, secure, and trusted bidirectional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate CEHRT and health information technology (HIT) vendors." This is clearly technical and outside the control of most physicians. Alignment of expectations and requirements across stakeholders is necessary to ensure information blocking is curtailed. HHS should also strive for consistent policies to limit confusion. CHI recommends ONC require CEHRT attest to the same three requirements physicians are held accountable to.

§ 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:
ONC is proposing several changes to its certification program, including § 170.315(g)(10)-APIs, EHI export, USCDI adoption, Real World Testing, Standards Version Advancement Process, Communications, and Assurances. EHR vendors will require a considerable amount of time to make changes and comply with Conditions and Maintenance of Certification. ONC is proposing a 24-month development timeline for most of its proposed certification changes. ONC is also proposing to adjust the definition of 2015 Edition Base EHR to comport with ONC's certification requirements within 24 months final rule's effective date. Because most physicians are bound to the use of 2015 Edition Base EHRs through CMS program requirements, as proposed, the 24-month timeline would require EHR vendor development and physician EHR adoption, implementation, and use concurrently. Not only does this create an incredibly ambitious timeline, it also effectively usurps CMS' authority to determine when physicians use a particular Edition of Certified EHR Technology (CEHRT) requirements for incentive program participation.

EHR developers should be provided a specific timeline to develop, test, certify, publish, implement, and train their customers on new product features and functions. This timeline should be separate from physician adoption requirements, which is squarely in CMS' purview. While we support a two-year time horizon for development, implementation, and go-live, we do not support ONC dictating the adoption schedule for physicians. If ONC continues with its proposal it should, at the very least, provide physicians additional time beyond 24 months. Once our members have entered into their vendor's implementation queue, they continue to experience 12+ month timelines before EHRs are upgraded/installed. We reiterate that ONC should remain focused on the technology, while other HHS agencies and offices dictate adoption policies. We also caution ONC against using language that implies that both certified health IT developers and their customers are required to meet the 24-month timeline (e.g., health IT developers "must provide all of its customers…"); this wording extends ONC's regulatory reach beyond health IT developers to providers. Rather, ONC should require that health IT developers "make available" to its customers upgraded product features and functions within 24 months.

For this reason and to prevent significant confusion for physicians about program requirements, the CHI strongly recommends ONC refrain from adjusting the 2015 Edition Base EHR definition. We do not agree with ONC's reasoning to not propose a new Certified Health IT Edition designation. The proposed modifications to 2015 Edition CEHRT will make substantive changes to EHR design, functionality, use, and performance. ONC should release a new Edition, and we recommend 2020 Edition or the corresponding year in which this rule is effective. HHS should direct its agencies to update regulations to reflect the new Edition.

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:

Because the TEFCA is currently proposed as a voluntary framework, CHI is not supportive of requiring certain health IT developers to participate in the TEFCA. Whether the TEFCA is voluntary or mandatory (in part or in whole), it is essential that ONC provide clarity as to the relationship between its information blocking rules and the TEFCA.

§ 170.403 Communications

(a) Condition of Certification.

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

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

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

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

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

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

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

following purposes—

§ 170.403 Communications

(A) Making a disclosure required by law;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 170.403 Communications
(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information. (E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section. (b) Maintenance of Certification. (1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section: (i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer. (ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer. (2) Contracts and agreements. (i) A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section. (ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.
Preamble FR Citation: 84 FR 7467-76 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Please see 84 FR 7578 for estimates related to this proposal.

Public Comment Field:

CHI generally supports these requirements with the following recommendations:

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

In addition to health information exchange, the ONC should explicitly permit communication regarding CEHRT product safety, fees, or other costs associated with product use or maintenance.

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

ONC should clarify that physicians participating in developer programs that test products in real-world environments, or those that volunteer to test products on an ad hoc basis, are not considered developer contractors and therefore should not be restricted from communicating concerns. ONC should further clarify users should not be restricted from communicating concerns about issues unrelated to functions/features they are involved in testing even if they are considered contractors. Communication restrictions should only apply to specific EHR functions/features a "contractor" is directly involved in developing or testing.

(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.

ONC should clarify that user-developed examples or diagrams (e.g., flowcharts) are not prohibited. Flowcharts are important tools used in presentations to visually depict complex interfaces and systems. They are often important components in academic and peer-reviewed research.

(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.

CHI believes that one month, rather than six months, is sufficient time for health IT developers to contact their clients about current contract provisions. Further delaying physicians' ability to communicate concerns with EHR safety, security, and interoperability could jeopardize patient care. We request ONC explicitly state that any permitted communication made following the effective date of the final rule be inadmissible as a violation of a contract/agreement regardless of whether the customer has been notified.

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:

No comment.

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

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

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

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

Public Comment Field:

CHI supports ONC's efforts to utilize the FHIR standards. We urge ONC to keep ARCH as aligned as possible with the USCDI and incorporate our comments above regarding the USCDI and what data types to include within the USCDI.

CHI further notes that the HL7 Argonaut clinical notes implementation guide recommends use of both the DocumentReference and DiagnosticReport resources and urge for this rule proposal's alignment with that recommendation.

§ 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 patient's data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months.

(vii) Documentation.

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

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

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

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

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

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

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

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

Public Comment Field:

Write Access for Patients: As noted elsewhere in our comments here, the CHI supports ONC's rules requiring access-controlled write access to patient data for patients, with reasonable review and approval measures. We believe such a requirement will empower patients to improve their own health data and would also foster increased use of patient-generated health data in care widely, consistent with important policy changes made at CMS with regard to caregiver payment and reimbursement. ONC is proposing that EHI "use" provides apps the ability to "*read, write, modify, and manipulate"* EHI. To ensure API Technology Developers can protect bi-direction exchange of data, we request that ONC ensure that:

- A security controls framework for interoperability and data sharing is established; and
- API Technology Developers develop and test to security industry protective measures, prescribed standards, and security protocols.

FHIR Version: While this ONC proposal contemplates four different options as far as the use of the FHIR standard, CHI urges ONC to utilize the option supporting R4. We believe that it will be much more conducive to realizing an interoperable healthcare ecosystem if one version of FHIR is used. Given our support for FHIR R4, the CHI does not support adoption of associated FHIR Release 2 Implementation Specifications. Rather, we recommend ONC proceed with naming HL7 US Core Implementation Guides. We are cognizant that there is less experience with US Core IGs than Argonaut IGs, yet we anticipate the industry will coalesce around US Core IGs over the coming months—especially if ONC signals FHIR R4 as the standard underpinning the USCDI.

Clinical Notes Format: We support the proposal "…that the clinical note text included in this FHIR resource would need to be represented in its "raw" text form. In other words, it would be unacceptable for the note text to be converted to another file or format (e.g., .docx, PDF) when it is provided as part of an API response." However, in situations where the "raw" text format is not in a standard format (e.g., *.txt) and is in a proprietary EHR format, CHI believes that the text should be converted into a standard raw text format first.

User Authentication and App Authorization: CHI is supportive of the proposal to require availability of refresh tokens with a lifetime of 3 months as long as authorization servers must also provide a new refresh token with a lifetime of 3 months each time the client supplies a valid refresh token and makes a query for data. In the proposed rule, it is unclear as to whether a new refresh token is required or optional, and we request ONC update its proposal consistent with our recommendations on authentication and app authorization.

Search Parameters for Clinical Notes and Provenance: CHI recommends that ONC align its approach to search parameters for clinical notes and provenance with the Argonaut Clinical Notes guide and soon-to-be-released Argonaut Provenance guidance.

Documentation: CHI supports that all documentation "be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation."

Verification of Authenticity of App Developers: CHI generally offers its support for the proposed requirement that app authenticity be verified "within 5 business days of receipt of an application developer's request to register their software application with the API technology provider's authorization server." CHI proposed that ONC provide further clarity to this requirement by We propose amending the requirements to add, after "authorization server," the following: "and receipt of any additional requested information needed in order to verify the developer's authenticity."

In addition to constraining ONC's information blocking regulations and interpretation of EHI, ONC should require that all certified APIs include mechanisms to strengthen patients' control over their data. Patients should have complete access to their data. HIPAA reinforces this right. However, CHI believes that patients are just as interested in protecting their data's privacy as they are in accessing it.

CHI has identified an opportunity for multiple coexisting components to empower patients with meaningful knowledge and control over the use of their data. We believe that ONC has the responsibility to provide patients with a basic level of privacy and app transparency. CHI recommends ONC to take the following steps to ensure patient data is accessed, exchanged, and used pursuant with the goals outlined in Cures and the desires expressed by patients.

As part of an API Technology Supplier's certification, ONC should require APIs check an app's attestation to:

- Industry-recognized development guidance;
- Transparency statements and best practices; and
- The adoption of a model notice to patients.

One possible method to accommodate this would require an EHR vendor's API to check for three "yes/no" attestations from any consumer-facing app. For example: (1) an app developer could choose to assert conformance to Xcertia's Privacy Guidelines; (2) an app developer could attest to the Federal Trade Commission's (FTC) Mobile Health App Developers: FTC Best Practices and the CARIN Alliance Code of Conduct; and (3) an app developer could attest to adopting and implementing ONC's Model Privacy Notice. These could be viewed as value-add services as proposed by ONC. The app could be acknowledged or listed by the health IT developer in some special manner (e.g., in an "app store," "verified app" list). We would urge EHR vendors to also publicize the app developers' attestations; ONC could also require a vendor to do so as a prerequisite to product certification.

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

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

(a) Condition of Certification.

(1) General. An API Technology Supplier must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) Transparency conditions.

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

(ii) Terms and conditions.

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

—

—

—

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

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

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

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

(5) Register software applications.

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

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

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

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

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

(C) Application developer verification. An API Technology Supplier is permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology.

(3) Permitted fees conditions.

(i) General conditions.

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

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

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

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

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

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

(ii) Permitted fee – Development, deployment, and upgrades. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.

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

(A) Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information;

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

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

(iv) Permitted fee – Value-added services. An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

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

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

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

(i) Non-discrimination.

(A) An API Technology Suppler must provide API technology to API Data Providers on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

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

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

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

(2) The revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.

(ii) Rights to access and use API technology.

(A) An API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment, including:

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

(2) Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and

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

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

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

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

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

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

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

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

(6) Meet additional developer or product certification requirements.

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

(iii) Service and support obligations. An API Technology Supplier must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments.

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

(B) Changes to terms and conditions. Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

(b) Maintenance of Certification.

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

(2) Service Base URL publication. API Technology Supplier must support the publication of Service Base URLs for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider, and make such information publicly available (in a computable format) at no charge.

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

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

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

Public Comment Field:

CHI supports proposed § 170.404 Application programming interfaces condition and maintenance of certification provisions, specifically "to provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with its API technology or to comply with any revised terms or conditions." CHI supports this notice also complying with the API documentation requirement that all documentation should be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation.

CHI also agrees with ONC's encouragement that "API Technology Suppliers, health care providers, HINs and patient advocacy organizations to coalesce around the development of a public resource or service from which all stakeholders could benefit. We believe this would help scale and enhance the ease with which Service Base URLs could be obtained and used." CHI notes that CMS has proposed to use the NPPES standard as a solution to address this problem, which is workable if the data is made publicly available in an API. CHI also notes that a dedicated site for FHIR-based URL endpoints could be a helpful solution if hosted neutrally and made widely accessible.

CHI has concerns with the concept of "Dynamic Registration". Specifically, we have concerns with ONC's statement that the "verification process would need to focus specifically on the application developer—not its software application(s)". As discussed in our comments on ONC's proposals to leverage the FDA's Pre-Certification Program, there are challenges with verifying an app at the developer level is insufficient to ensure app performance, particularly when an app developer has no previous record of creating safe and effective products in the health care space.

CHI appreciates ONC's efforts to address excessive fees charged by EHR vendors to connect their products with other health IT systems, health information exchanges, and third-party applications. We recognize that API permitted fees and restrictions are a multi-pronged issue. Developing policy to accommodate every interaction between an API Technology Supplier, API Data Provider, and API User is untenable. While ONC has attempted to address most scenarios, the resulting proposed fee policy is complex and has limited usefulness for physicians. Our members are already expressing concerns over the increased costs they will encounter to hire consultants or seek legal support just to parse out the rights and responsibilities of each API actor.

CHI believes a more practical approach would be to establish a tiered fee structure for APIs. For instance, ONC could establish categories where the technology requirements designate the fees.

- A "no fee" category would limit API Technology Suppliers from charging API Data Providers or API Users any fees for exchanging data in compliance with federal requirements (e.g., costs associated with health information exchange, patient access, reporting quality measures, and data segmentation for privacy). Since all API Technology Suppliers will be certified by ONC, any API Technology Supplier-to-API Technology Supplier connections would also be in the "no fee" category.
- An "at cost" category would allow API Technology Suppliers to charge API Data Providers or API Users the cost of interfacing APIs with a non-API Technology Supplier's commercial technology (e.g., commercial lab systems, commercial PACS systems, commercial data analytics services).
- A "cost plus reasonable profit" category would allow API Technology Suppliers to charge API Data Providers or API Users a reasonable profit when conducting legitimate custom API development or creating custom apps (e.g., creating proprietary mappings for technology unique to a health system or establishing connections with non-commercially available technology.)

For the "at cost" and "cost plus reasonable profit" categories API Technology Suppliers should be restricted from implementing health IT in non-standard ways that unnecessarily increase the costs, complexity, and other burden of accessing, exchanging, or using EHI. We do not expect all scenarios will be addressed by this approach; however, we believe a clearer and more approachable fee structure will better empower physicians to be informed consumers of technology. We believe this also establishes fair and equitable fee structure for all parties involved.

As a part of the Condition and Maintenance of Certification for APIs, ONC proposes that an API Technology Supplier must public all terms and conditions needed to use any EHI that is obtained by means of the API technology. Due to the privacy concerns laid out above, CHI recommends that these terms and conditions needed to use EHI include patient consent and an explicit description as to how an individual's data will be used.

VII.B.5 Real World Testing

§ 170.405 Real world testing

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

(b) Maintenance of Certification.

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

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

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

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

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

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

(C) The timeline and plans for any voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

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

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

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

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

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

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

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

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

§ 170.405 Real world testing
(iv) A list of the key milestones met during real world testing; (v) The outcomes of real world testing including a description of any challenges encountered during real world testing; and (vi) At least one measurement/metric associated with the real world testing. (3) USCDI Updates for C-CDA. A health IT developer with health IT certified to § 170.315(b)(1), (e)(1), (g)(6), (f)(5), and/or (g)(9) prior to the effective date of this final rule must: (i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and (ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(3)(i) of this section within 24 months of the effective date of this final rule. (4) C-CDA Companion Guide Updates. A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (b)(9), (e)(1), (g)(6), and/or (g)(9) prior to the effective date of this final rule must: (i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and (ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(4)(i) of this section within 24 months of the effective date of this final rule. (5) Voluntary standards and implementation specifications updates. A health IT developer subject to paragraph (a) of this section that voluntary updates its certified health IT to a new version of an adopted standard that is approved by the National Coordinator through the Standards Version Advancement Process must: (i) Provide advance notice to all affected customers and its ONC-ACB – (A) Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator; (B) The developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world; (C) Whether the developer intends to continue to support the certificate for the existing certified Health IT Module version for some period of time and how long or if the existing certified Health IT Module version will be deprecated; and (ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in applicable 2015 Edition certification criterion specified in paragraph (a) of this section.
Preamble FR Citation: 84 FR 7495-97 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7578-82 for estimates related to this proposal.

Public Comment Field:

CHI recommends ONC include a description of "measurement" and provide clarity on the role of measurement—specificity for purpose or proof points. ONC should consider including updated metric expectations after the pilot year. Where real world testing is for both interoperability and use of received data, the ONC should consider specifying that there be at least one metric for interoperability and one metric for use. For instance, ONC could include the number of "clicks" it takes to perform an action (e.g., order an MRI) and include the number of clicks it takes to perform a health information exchange operation (e.g., reconciliation of USCDI data elements).

We also support the Standards Version Advancement Process (SVAP) as enabling needed industry flexibility. We view the ONC certification program as providing a floor that all certified technology will need to support, while the SVAP provides permissible progressions (that later can become the new floor in the next rule). With respect to the SVAP's ability to assert conformance in the absence of the test tools, there is a need to test once tools become available. ONC should provide more clarity when a version of standards is available under this process but does not yet have testing tools available to determine conformance. It is fairly clear vendors must factor all claimed versions of standards into their real-world testing, but ONC should clarify how the health IT developers are to address new versions for which tooling does not exist. ONC should clarify whether testing will be required in a subsequent year's real-world testing plan once tooling is available or whether the health IT developer's previous attestation is sufficient.

§ 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:

CHI supports proposed revisions to § 170.555 Certification to newer versions of certain standards.

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.

§ 170.406 Attestations

Public Comment Field:

CHI supports these requirements. Physicians participating in the Quality Payment Program are already required to attest to a three-part information blocking statement. This statement is detailed and ties a physician's attestation to their EHR vendor's capabilities. For instance, physicians must attest they "implemented in a manner that allowed for the timely, secure, and trusted bidirectional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate CEHRT and health information technology (HIT) vendors." This is clearly technical and outside the control of most physicians. Alignment of expectations and requirements across stakeholders is necessary to ensure information blocking is curtailed. HHS should also strive for consistent policies to limit confusion. CHI recommends ONC require EHR vendors to be held accountable for the same three requirements.

VII.D Enforcement

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

(a) * * *

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

(2) * * *

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

* * * * *

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

* * * * *

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

(3) * * *

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

(4) Coordination with the Office of Inspector General.

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

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

* * * * *

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

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

(b) * * *

(1) * * *

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

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

* * * * *

(iii) * * *

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

(2) * * *

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

* * * * *

(3) * * *

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

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

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

(iv) Any other relevant information.

(c) * * *

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

* * * * *

(e) * * *

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

* * * * *

(f) * * *

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

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

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

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

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

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

(1) Fact-finding;

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

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

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

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

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

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

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

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

* * * * *

(g) * * *

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

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

(A) Suspension;

(B) Termination; or

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

* * * * *

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

§ 170.580 ONC review of certified health IT or a health IT developer's actions
(i) Termination; (ii) Suspension; or (iii) Certification ban under § 170.581(a)(2). (3) * * * (i) A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of: (A) Suspension; (B) Termination; or (C) Certification ban under § 170.581(a)(2). * * * * * (4) Effect of appeal. (i) A request for appeal stays the termination of a certification issued to a Health IT Module, but the Health IT Module is prohibited from being marketed, licensed, or sold as "certified" during the stay. (ii) A request for appeal does not stay the suspension of a Health IT Module. (iii) A request for appeal stays a certification ban issued under § 170.581(a)(2). (5) * * * (i) The hearing officer may not review an appeal in which he or she participated in the initial suspension, termination, or certification ban determination or has a conflict of interest in the pending matter. * * * * * (6) * * * (v) ONC will have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf that clarifies, as necessary, its determination to suspend or terminate the certification or issue a certification ban. * * * * *
Preamble FR Citation: 84 FR 7503-07 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7583-84 for estimates related to this proposal.
Public Comment Field: No comment.

§ 170.505 Correspondence

(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.

(b) In circumstances where it is necessary for an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the official date of receipt for all parties will be the date of the delivery confirmation to the address on record.

Preamble FR Citation: 4 FR 7503-04 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

No comment.

§ 170.581 Certification ban

(a) Circumstances trigger a certification ban. The certification of any of a health IT developer's health IT is prohibited when:

(1) The certification of one or more of the health IT developer's Complete EHRs or Health IT Modules is:

(i) Terminated by ONC under the ONC Health IT Certification Program;

(ii) Withdrawn from the ONC Health IT Certification Program by an ONC-ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(iii) Withdrawn by an ONC-ACB because of a non-conformity with any of the certification criteria adopted by the Secretary under subpart C of this part;

(iv) Withdrawn by an ONC-ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary under subpart C of this part, including notice of pending surveillance; or

(2) ONC determines a certification ban is appropriate per its review under § 170.580(a)(2)(iii).

(b) Notice of certification ban. When ONC decides to issue a certification ban to a health IT developer, ONC will notify the health IT developer of the certification ban through a notice of certification ban. The notice of certification ban will include, but may not be limited to:

§ 170.581 Certification ban

(1) An explanation of the certification ban;

(2) Information supporting the certification ban;

(3) Instructions for appealing the certification ban if banned in accordance with paragraph (a)(2) of this section; and

(4) Instructions for requesting reinstatement into the ONC Health IT Certification Program, which would lift the certification ban.

(c) Effective date of certification ban.

(1) A certification ban will be effective immediately if banned under paragraphs (a)(1) of this section.

(2) For certification bans issued under paragraph (a)(2) of this section, the ban will be effective immediately after the following applicable occurrence:

(i) The expiration of the 10-day period for filing a statement of intent to appeal in § 170.580(g)(3)(i) if the health IT developer does not file a statement of intent to appeal.

(ii) The expiration of the 30-day period for filing an appeal in § 170.580(g)(3)(ii) if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(iii) A final determination to issue a certification ban per § 170.580(g)(7) if a health IT developer files an appeal timely.

(d) Reinstatement. The certification of a health IT developer's health IT subject to the prohibition in paragraph (a) of this section may commence once the following conditions are met.

(1) A health IT developer must request ONC's permission in writing to participate in the ONC Health IT Certification Program.

(2) The request must demonstrate that the customers affected by the certificate termination, certificate withdrawal, or non-compliance with a Condition or Maintenance of Certification have been provided appropriate remediation.

(3) For non-compliance with a Condition or Maintenance of Certification requirement, the non-compliance must be resolved.

(4) ONC is satisfied with the health IT developer's demonstration under paragraph (d)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

Preamble FR Citation: 84 FR 7504-06 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

No comment.

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:

CHI is generally supportive of ONC's efforts to prevent information blocking and facilitate greater data access throughout the care continuum. Using the most advanced approaches, including artificial intelligence, will bring unprecedented positive transformation to the US healthcare system widely, making ONC's rulemaking on information blocking more important than ever.

Regarding the specific exceptions proposed by ONC, we strongly urge for ONC to provide clarity as to the obligations of a Business Associate (BA) under HIPAA. CHI believes that ONC has, in its draft rule, clarified that technology companies that are BAs are not subject to information blocking rules being developed in this rulemaking, and we support this proposed approach. However, we request clarity that BAs will not be included in OIG information blocking investigations due to their role as a BA. We also note our support for the proposed privacy exception put forward by ONC as it would permit BAs to be held to the terms of their obligations under HIPAA (in other words, those covered by the information blocking rule should be responsible for satisfying the information blocking rules' requirements, and to ensure that its expectations of BAs are clearly communicated in the agreements they reach with their BAs). CHI urges ONC to provide this clarity through providing a safe harbor to BAs for actions consistent with their obligations to a relevant HIPAA Covered Entity under both the security and privacy exceptions.

§ 171.101 Applicability

This part applies to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks, as those terms are defined in § 171.102.

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

Regulatory Impact Analysis: Not applicable

Public Comment Field:

No comment.

§ 171.103 Information blocking

Information blocking means a practice that—

(a) Except as required by law or covered by an exception set forth in subpart B of this part, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and

(b) If conducted by a health information technology developer, health information exchange, or health information network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or

(c) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

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

Regulatory Impact Analysis: Please see 84 FR 7584-86 for estimates related to this proposal.

Public Comment Field:

No comment.

§ 171.102 Definitions

For purposes of this part:

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

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

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

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

Electronic Health Information (EHI) means—

(1) Electronic protected health information; and

(2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

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

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

§ 171.102 Definitions

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

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

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

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

(1) Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

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

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

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

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

Interoperability element means—

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

(2) Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements.

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

(4) Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.

§ 171.102 Definitions
(5) Any other means by which electronic health information may be accessed, exchanged, or used. Permissible purpose means a purpose for which a person is authorized, permitted, or required to access, exchange, or use electronic health information under applicable law. Person is defined as it is in 45 CFR 160.103. Protected health information is defined as it is in 45 CFR 160.103. Practice means one or more related acts or omissions by an actor. Use means the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.
Preamble FR Citation: 84 FR 7509-15 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable

Public Comment Field:

CHI strongly recommends that the definition of Health Information Network (HIN) be narrowed to include only entities that are an actual network (or formalized component of an actual network) and have an actual operational role and responsibility for the network. For example, to be a HIN, the network itself provides the ability to locate and transmit EHI between multiple persons and/or entities electronically, on demand, or pursuant to one or more automated processes. Moreover, to be a HIN, the entity should also be exchanging EHI in a live clinical environment using the network in some capacity. Thus, health care providers and organizations with limited exchange capabilities, such as interfaces for Admission, Discharge, and Transfer messages or lab results, should not be considered a HIN.

ONC should clarify that passive infrastructure tools used to perform health information exchange functions are excluded from the proposed definition of a "health information network." Health care providers use many different passive infrastructure tools (including computers, broadband connectivity, telephones, internal networking technology and cloud-based service applications) to manage and store health information and facilitate its movement within and beyond their internal systems. Passive infrastructure offerings are commonly acquired and operated under the direction of health care providers through contractual arrangements with third-party technology vendors and create the technological platform that provides the baseline information technology environment to meet the health provider's information exchange needs.

We do not believe that Congress intended to regulate passive infrastructure tools as health information networks. ONC should create an explicit exclusion in the regulatory text to exempt third-party vendors providing passive infrastructure tools used for purposes of health information technology. For instance, cloud-based technology is a passive infrastructure tool that is subject to HIPAA in its role as a business associate when it stores health data generated by the majority of health care providers and other health care stakeholders. Many cloud providers are developing or have developed API's based on FHIR standards to share health information as directed by health care providers in a manner that is consistent with HIPAA protections or as authorized by patients. This function is significantly distinct from the current understanding of a health information network, because the cloud is primarily a destination for obtaining and accessing information rather than an independent broker connecting two unaffiliated parties. Therefore, the mere fact that a passive storage solution enables the authorized exchange of information under the direction of a health care provider through an API should not trigger regulation of the cloud vendor as an health information network.

To avoid the unintended consequence of creating unnecessary regulatory burdens or red tape related to the use of passive infrastructure tools, we urge ONC to amend the proposed definition of a health information network at 45 CFR 171.102 as follows:

> *Health Information Network or HIN* –
> (1) M~~m~~eans an individual or entity that satisfies one or both of the following –
> (a~~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.
> (b~~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.
> (2) Does not mean a third-party vendor of passive infrastructure tools, including cloud-based technology."

HINs typically operate as Business Associates and currently have Business Associate agreements in place with their participants who are Covered Entities. These agreements facilitate the exchange of EHI since they perform functions or activities on behalf of, or provide certain services for Covered Entities such as determining and administering policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of health information between or among two or more Covered Entities. Therefore, for example, organizations that develop voluntary standards and policies that may be used by a HIN should not be considered a HIN.

FUNCTIONAL ELEMENT

In defining "Interoperability Element", ONC states that the term is not limited to functional elements and technical information but also encompasses technologies, services, policies, and other conditions necessary to support the uses of EHI. ONC's intent is to capture the potential means by which EHI may be accessed, exchanged, and used. CHI believes that Interoperability Element should not include the underlying substantive content because such content is not a potential means by which EHI may be accessed, exchanged, or used. Therefore, ONC should clarify that underlying substantive content is not included in the definition of Interoperability Element.

ELECTRONIC HEALTH INFORMATION

As previously mentioned, the CHI believes that the definition of EHI is too broad. We are also concerned about the impracticality of applying this subjective definition to the information blocking provisions to an extensive, highly situational and largely non-standardized data set. Instead, CHI recommends alignment between ONC's information blocking provisions, EHI, and USCDI proposals could happen in several ways. CHI is recommending two potential paths:

- ONC could constrain its definition of EHI to just the data elements represented by the USCDI for specified actors. Information blocking requirements would be subject to newly-scoped access, use, and exchange of the USCDI. Patients would retain their rights to request their designated record set as outlined by HIPAA (the Director of the HHS Office of Civil Rights has already noted publicly that patient access enforcement will increase this year). EHI export could be scoped to focus on ePHI as outlined by HIPAA. Additional data classes (e.g., payment and cost information) would propagate through the USCDI expansion process with support from the ISA and SVAP.
- Alternatively, ONC could retain its EHI definition, rescope the terms "access", "use", and "exchange", and include additional information blocking exceptions. ONC could establish an exception for actors only able to make the USCDI available. This exception should be concise, clear, implementable, and refrain from burdensome policy and procedure requirements. This could also be accomplished by modifying the proposed "Infeasibility of Request" exception. We encourage ONC to clarify that actors that do not comply with the request for access, exchange, or use of EHI, but that do comply to the best of their ability with requests for access, exchange, or use of the USCDI be able to claim this exception. Also, ONC should clarify that an actor could claim an exception for responding in "good faith" to requests beyond the USCDI.

Request for comment regarding the definition of "health care provider"
The term "health care provider" is defined in Public Health Service Act section 3000(3) (42 U.S.C. 300jj(3)). We propose to adopt this definition for purposes of section 3022 of the PHSA when defining "health care provider" in § 171.102. We note that this definition is different from the definition of "health care provider" under the HIPAA Privacy and Security Rules. We are considering adjusting the information blocking definition of "health care provider" to cover all individuals and entities covered by the HIPAA "health care provider" definition. We seek comment on whether this approach would be justified, and commenters are encouraged to specify reasons why doing so might be necessary to ensure that the information blocking provision applies to all health care providers that might engage in information blocking.
Preamble FR Citation: 84 FR 7510 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable
Public Comment Field: No comment.

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: *Pricing Information in EHI* CHI fully supports price transparency, but we believe that defining EHI to include various types of price information and then holding entities accountable under the information blocking provisions is inappropriate because this pricing information is generally held and controlled by health plans that are not subject to the information blocking provisions. Given the complexity surrounding specific plans, deductibles, level of coinsurance, and site of service, payment calculations for the future provision of health care to a patient may prove difficult in providing an accurate estimate. Pushing out price information for the sake of pushing out price information without it being meaningful and accurate is worthless and counterproductive. Moreover, determining whether a provider is in-network may be difficult because of outdated provider directories or confusion associated with multiple plan contracts. Price also varies depending on where the service is performed, which impacts cost and a patient's cost-sharing. The cumulative effects of each of these factors often make it difficult to provide accurate pricing information for an individual patient in the absence of an actual service claim.

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: Please see the above response to the price information RFI.

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:

We are very concerned with the complexity and broad reach resulting from the interaction of the pricing provisions of the proposed rule, in both information blocking practices and exception, with the very expansive definitions of actors and of EHI. Although ONC refers to "rent-seeking and other opportunistic pricing practices," its definition is not limited to such behaviors and will likely to be very subjective. For example, ONC implies that "value-based pricing"—an approach commonly used in industry—is "opportunistic" and would not be mitigated by any of the proposed exceptions. ONC goes on to emphasize that

> *"[T]he reach of the information blocking provision is not limited to these types of practices. We interpret the definition of information blocking to encompass any fee that materially discourages or otherwise imposes a material impediment to access, exchange, or use of EHI. We use the term "fee" in the broadest possible sense to refer to any present or future obligation to pay money or provide any other thing of value . . . We believe this scope may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services. Therefore, . . . we propose to create an exception that, subject to certain conditions, would permit the recovery of costs that are reasonably incurred to provide access, exchange, and use of EHI."*

It appears that ONC would view any fee as imposing a "material impediment" and therefore requiring use of the exception focused on recovering costs. ONC acknowledges that the definition of any fee as a practice that implicates information blocking "may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services". We agree with ONC on this latter point but are not convinced that simply providing an exception, which is itself very limiting, is a sufficient counter to the issues raised by the provision. In addition, the documentation required by these exceptions could be quite extensive and onerous. We note that Cures directs HHS to reduce physician burden, not increase it.

§ 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: No comment.

VIII.D Proposed Exceptions to the Information Blocking Provision

§ 171.201 Exception – Preventing harm
To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times. (a) The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from— (1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record; (2) Misidentification of a patient or patient's electronic health information; or (3) Disclosure of a patient's electronic health information in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination. (b) If the practice implements an organizational policy, the policy must be— (1) In writing; (2) Based on relevant clinical, technical, and other appropriate expertise; (3) Implemented in a consistent and non-discriminatory manner; and (4) No broader than necessary to mitigate the risk of harm. (c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.
Preamble FR Citation: 84 FR 7523-26 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable

Public Comment Field:

CHI generally supports this proposed exception, and believes that reliance on the USCDI should mitigate inaccurate or corrupted data being put into a patient's EHR. In the event that two patient records are erroneously merged and one of those patients accesses another patient's data through an API, neither patient should face liability under these rules.

Further, we share ONC's concern that "known inaccuracies in some data within a record may not be sufficient justification to withhold the entire record if the remainder of the patient's EHI could be effectively shared without also presenting the known incorrect or corrupted information as if it were trustworthy." This exception, nor any exception, should be interpreted to permit default systematic rejection of data requests couched in an exception. Specific to the exception for preventing harm, we request that ONC clarify that it is expected that API Data Providers would still share information that is known not to be incorrect or corrupted.

CHI is also concerned that ONC's expectations for the ability to carve out 42 CFR Part 2 covered data may far exceed current industry capabilities in terms of technology and operational capacity. In particular, carving out such data from notes for exchange and data export will be very challenging. We suggest that the focus on physical harm in the determination by a licensed health care professional is too narrow and should be expanded to include psychological and other forms of non-physical harm. Additionally, the proposed burden of proof is unreasonable and the need to demonstrate that a policy is sufficiently tailored is likely to create a costly compliance burden. We note that Cures directs HHS to reduce physician burden, not increase it.

§ 171.202 Exception – Promoting the privacy of electronic health information

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

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

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

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

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

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

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

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

(1) The actor's practice—

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

(A) Are in writing;

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

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

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

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

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

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

(3) The actor's practice is—

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

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

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

§ 171.202 Exception – Promoting the privacy of electronic health information
provide access, exchange, or use of electronic health information provided that the actor's practice— (1) Complies with applicable state or federal privacy laws; (2) Implements a process that is described in the actor's organizational privacy policy; (3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service; (4) Is tailored to the specific privacy risk or interest being addressed; and (5) Is implemented in a consistent and non-discriminatory manner. (d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3). (e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if— (1) The individual requests that the actor not provide such access, exchange, or use; (2) Such request is initiated by the individual without any improper encouragement or inducement by the actor; (3) The actor or its agent documents the request within a reasonable time period; and (4) The actor's practice is implemented in a consistent and non-discriminatory manner.
Preamble FR Citation: 84 FR 7526-35 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable

Public Comment Field:

Generally, CHI urges ONC to ensure that information blocking rule adherence does not undercut necessary patient privacy. For example, CHI strongly urges for ONC to provide clarity as to the obligations of a Business Associate (BA) under HIPAA. CHI believes that ONC has, in its draft rule, clarified that technology companies that are BAs are not subject to information blocking rules being developed in this rulemaking, and we support this proposed approach. However, we request clarity that BAs will not be included in OIG information blocking investigations due to their role as a BA. We also note our support for the proposed privacy exception put forward by ONC as it would permit BAs to be held to the terms of their obligations under HIPAA (in other words, those covered by the information blocking rule should be responsible for satisfying the information blocking rules' requirements, and to ensure that its expectations of BAs are clearly communicated in the agreements they reach with their BAs). CHI urges ONC to provide this clarity through providing a safe harbor to BAs for actions consistent with their obligations to a relevant HIPAA Covered Entity under both the security and privacy exceptions.

CHI notes its belief that patients should experience the privacy and security they expect whether HIPAA applies or not, and supports the ongoing role of the Federal Trade Commission in protecting patients against deceptive or unfair acts or practices.

We note that prioritizing data quantity over usability presents significant privacy concerns. For example, a directive to exchange all EHI with all actors for nearly any purpose may force covered entities to compromise the "minimum necessary" standard in the HIPAA. ONC's minimum necessary determination proposal effectively creates a new minimum necessary standard. CHI supports maintaining HIPAA's minimum necessary standard, which generally requires covered entities to share the minimum amount of information necessary to accomplish the intended purpose of the disclosure. For instance, we do not support requirements to disclose an entire designated record set to another covered entity. We also do not support a requirement to disclose psychotherapy notes—we note that even patients do not have access rights to their psychotherapy notes. Minimum necessary controls are particularly important given the Administration's clear intent to promote the exchange of information and the emerging capability of technology to extract bulk patient data out of an EHR. Confusion about HIPAA's minimum necessary standard versus ONC's EHI-based information blocking requirements may also lead to oversharing of patient data due to the burden associated with determining how much information to divulge so as not to violate HIPAA and face OCR enforcement or OIG enforcement; or empowering overbroad demands for more information than is needed. ONC should clarify that providing the minimum necessary information to an actor (including another covered entity) will not be considered information blocking. ONC should also remove consider reducing onerous requirements for documentation of decision-making associated with qualifying for privacy exceptions or sub-exceptions.

§ 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:

Generally, CHI urges ONC to ensure that information blocking rule adherence does not undercut necessary patient privacy. CHI strongly urges for ONC to provide clarity as to the obligations of a Business Associate (BA) under HIPAA. CHI believes that ONC has, in its draft rule, clarified that technology companies that are BAs are not subject to information blocking rules being developed in this rulemaking, and we support this proposed approach. However, we request clarity that BAs will not be included in OIG information blocking investigations due to their role as a BA. We also note our support for the proposed privacy exception put forward by ONC as it would permit BAs to be held to the terms of their obligations under HIPAA (in other words, those covered by the information blocking rule should be responsible for satisfying the information blocking rules' requirements, and to ensure that its expectations of BAs are clearly communicated in the agreements they reach with their BAs). CHI urges ONC to provide this clarity through providing a safe harbor to BAs for actions consistent with their obligations to a relevant HIPAA Covered Entity under both the security and privacy exceptions.

CHI notes its belief that patients should experience the privacy and security they expect whether HIPAA applies or not, and supports the ongoing role of the Federal Trade Commission in protecting patients against deceptive or unfair acts or practices.

CHI is also concerned with the burden associated with performing analyses of policies and practices against complex and incompletely defined terms—especially with the requirement to meet "all requirements at all times."

We note that this exception has a provision for cases where there is no written policy. In practice, it seems most likely that the absence of a policy means that one is dealing with an unexpected and evolving situation as best one can (e.g., a sustained and sophisticated attack). The exception calls for a determination that not only that the practice is necessary, but also that effectively there is no other way of having protected your security that might have been less likely to interfere with information access. In our view, such a requirement is asking too much of those dealing with urgent threats, often after hours and under considerable uncertainty. We suggest that ONC create a further "safety valve" for short-lived actions that are taken in good faith while a situation is being evaluated and understood. We believe this is a core need for small medical practices with limited resources.

We ask that ONC clarify that proactive and preventive security-focused activities are permitted so long as they meet the applicable criteria for security-related practices in this exception.

ONC should confirm that an organization can use security policies that exceed what is required by law or regulation based on their assessment of the threat environment, without violating this exception. ONC should recognize the valid need to allow for due diligence as distinct from simply delaying access and such due diligence should not need the security exception to avoid implicating or being judged as engaged in information blocking. The need for vetting of external locations of exchange includes but is not limited to apps (e.g., networks).

§ 171.204 Exception – Recovering costs reasonably incurred

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

(d) Compliance with the Conditions of Certification.

§ 171.204 Exception – Recovering costs reasonably incurred

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

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

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

Regulatory Impact Analysis: Not applicable

Public Comment Field:

CHI supports the proposal in § 171.204 Exception - Recovering costs reasonably incurred that neither individuals nor API users be charged a fee "for API uses that are associated with the access, exchange, and use of EHI by patients or their applications, technologies, or services."

CHI agrees that ONC should prioritize exchange, access, and use of "observational health information" (i.e., EHI that is created or maintained during the practice of medicine or the delivery of health care services to patients). In addition, we believe that ONC should also prioritize certain purposes or use cases for data exchange/access/use, specifically, the HIPAA categories of treatment, payment, and operations, relative to access (other than that needed to support a patient's HIPAA right of access) that is intended to serve primarily clinical care objectives of the party seeking data.

§ 171.205 Exception – Responding to requests that are infeasible

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

(a) Request is infeasible.

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

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

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

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

(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

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

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as

defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

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

§ 171.205 Exception – Responding to requests that are infeasible

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

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

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

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

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

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

(d) Provision of a reasonable alternative. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information.

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

Regulatory Impact Analysis: Not applicable

Public Comment Field:

CHI is concerned that this exception is too vague. This vagueness will create uncertainty as to whether claiming this exception will ultimately be validated by regulators and therefore lessen the benefit of this important exception.

CHI recommends ONC include requests for data that would use non-standard implementation specifications be refused as "infeasible". Furthermore, actors should be able to focus on specific use cases and refuse requests to expand access, exchange, or use to support additional use cases as "infeasible." At the same time, we believe that there should be a floor of the minimum set of use cases with associated interoperability standards that must be supported by a specific type of actor; perhaps the TEFCA provides a basis for such a floor.

We ask ONC to confirm that infeasibility could include not having the technical capability in production to meet a request (e.g., not having APIs or other technical means to support a specific type of exchange, access, or use, for example to enable write access to the EHR), when the cost of acquiring such capabilities are excessive and could reduce the ability to meet other project plans and customer commitments.

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

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

(a) Responding to requests. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:

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

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

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

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

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

(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Regulatory Impact Analysis: Not applicable

Public Comment Field:

CHI is deeply aware of the existing construct for FRAND licensing behavior in the context of standard-essential patents (SEPs). We note that FRAND case law, which ONC points to in its draft rule, has taken over 20 years of expensive litigation to develop and that its contours remain murky. Pure reliance on a reasonableness standard may create a similar situation as far as the reasonable fees for APIs in the context of this ONC rule. For example, ONC's draft rule does not propose specific caps on API fees. We believe that ONC should, to the extent practical, provide clear and unambiguous limits on API fees that can be charged. Further, CHI believes that API access for patients should be free of charge (including through third party apps that facilitate access to such data).

§ 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:

CHI asks that ONC recognize it is unlikely that a system would be made unavailable as part of deliberate information blocking and we question whether such downtime should be considered a practice that implicates information blocking. Caregivers have strong incentives to keep systems up and to respond quickly to unplanned outages. We recognize that system unavailability due to prevention of harm or security risks would fall under those exceptions and not this one. At the same time, subjecting urgent system downtime needs to the far-reaching requirements associated with any of these exceptions seems unwarranted.

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

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

Preamble FR Citation: 84 FR 7552	**Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable	

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

Public Comment Field:

Because the TEFCA is currently proposed as a voluntary framework, CHI is not supportive of requiring certain health IT developers to participate in the TEFCA. Whether the TEFCA is voluntary or mandatory (in part or in whole), it is essential that ONC provide clarity as to the relationship between its information blocking rules and the TEFCA.

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:

No comment.

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:

No comment.

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:
CHI does not support or see a need for any additional penalties or disincentives beyond what is currently in place. In addition to ONC's information blocking requirement, there are already three "levers" to incentivize sharing of and providing access to EHI.

For example, HIPAA requires providers to provide patients access to their designated record set. This includes providing individuals the right to inspect or obtain a copy, or both, of the ePHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. Providers could face enforcement actions and penalties with monetary fines in the hundreds of thousands, if not millions, for failing to comply with HIPAA regulation. Furthermore, the Office of Civil Rights (OCR) has expressed a desire to increase HIPAA enforcement on providers.

Additionally, to prevent actions that block the exchange of health information, the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) and the Quality Payment Program (QPP) requires eligible professionals (EP), eligible hospitals (EH) and critical access hospitals (CAH) that participate in both the Medicare and Medicaid Promoting Interoperability (PI) Programs to show that they have not knowingly and willfully limited or restricted the compatibility or interoperability of their certified electronic health record technology (CEHRT). EPs, EHs, and CAHs are required to show that they are meeting this requirement by attesting to three statements about how they implement and use CEHRT. Together, these three statements are referred to as the "Prevention of Information Blocking Attestation." Failing to attest to these statements will result in the EP, EH, or CAH scoring a 0 in PI—resulting in CMS reimbursement penalties. The Centers for Medicare and Medicaid Services (CMS) has also proposed publicly listing the names of EPs, EHs, and CAHs that attest "no".

Lastly, EPs, EHs, and CAHs participating in PI Programs, unless an exclusion is claimed, must submit collected data on four objectives and performance data for certain measures from each of the four objectives' measures. As the program's name entails, the objectives and measures are focused on promoting interoperability. Failing to submit data on the objectives, or performing poorly on the measures, will jeopardize the EPs, EHs, and CAHs, success in the PI Program—resulting in CMS reimbursement penalties.

Therefore, ONC should not create any new disincentives, modify any existing disincentives, or apply any other existing disincentives. Overall, ONC's and OIG's should have a general enforcement approach to encourage consistent compliance with the information blocking provisions rather than punishment. Prior to taking any action against health care providers for violating the information blocking provisions, the first priority should be to work with the health care provider through a corrective action and educational process to remedy the issue.

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 range of innovative connected health tools available today (and those in development), across patient conditions, offer key health IT functionalities that enable greater engagement in prevention and treatment as well as improved outcomes. Further, a diversity of APIs have emerged and are emerging to assist in bringing patient-generated health data (PGHD) into the continuum of care. CHI stresses that not all of these are necessarily well integrated with EHRs. While certified EHR technology (CEHRT) will be required to support APIs, many vendors will enable "read only" access, allowing for data to only flow out of the EHR rather than both in and out, reducing the utility of the EHR technology. We encourage ONC to advance a truly bidirectional flow of data throughout the healthcare continuum, and that an important step in this direction is the use of FHIR R4 as a baseline.

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: CHI supports additional validation that would support improved patient matching. Further, we note that use of the bi-directional FHIR API will allow for a patient to update their own demographic and health data, including privacy criteria and the role of providers as educators and advocates, subject to review and approval as needed, and we urge that such bi-directional functionality be mandated through ONC's information blocking rules. This RFI also inquires about further information that could be added to the USCDI that would assist in patient matching. CHI notes that more detail regarding the patient's address and including patient email would assist further in patient matching. We urge ONC to direct the HITAC to set up a sub-group to focus on Patient Matching with participation from technical experts from industry, to explore different creative technical approaches to accurately identify patient records.

Section XIII – Collection of Information Requirements

Collection of Information Requirements
Preamble FR Citation: 84 FR 7558-60 **Specific questions in preamble?** *No*
Public Comment Field: No comment.

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: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Supplemental Children's EHR Format Requirements for Recommendation 1
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.

Recommendation 2: Compute weigh-based drug dosage
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Supplemental Children's EHR Format Requirements for Recommendation 2
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.

Recommendation 3: Ability to document all guardians and caregivers
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.

Recommendation 3: Ability to document all guardians and caregivers
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Supplemental Children's EHR Format Requirements for Recommendation 3
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.

Recommendation 4: Segmented access to information
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Recommendation 4: Segmented access to information
Public Comment Field: No comment.

Supplemental Children's EHR Format Requirement for Recommendation 4
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.

Recommendation 5: Synchronize immunization histories with registries
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Supplemental Children's EHR Format Requirement for Recommendation 5

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

No comment.

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

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

No comment.

Public Comment Field:
No comment.

Public Comment Field:
No comment.

Public Comment Field:

No comment.

Recommendation 7: Transferrable access authority

See Pediatric Technical Worksheets at 84 FR 7605.

Public Comment Field:

No comment.

Public Comment Field:

Recommendation 7: Transferrable access authority
No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Supplemental Children's EHR Format Requirement for Recommendation 7
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.

Recommendation 8: Associate maternal health information and demographics with newborn
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Recommendation 8: Associate maternal health information and demographics with newborn
Public Comment Field: No comment.

Recommendation 9: Track incomplete preventative care opportunities
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.

Recommendation 10: Flag special health care needs
See Pediatric Technical Worksheets at 84 FR 7605.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.
Public Comment Field: No comment.