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

Overview

Elise Sweeney Anthony, Executive Director, Office of Policy, ONC
Michael Lipinski, Director, Regulatory Affairs Division, Office of Policy, ONC

Disclaimer

- ONC must protect the rulemaking process and comply with the Administrative Procedure Act. During the rulemaking process, ONC can only present the information that is in the NPRM as it is contained in the NPRM. ONC cannot interpret that information, nor clarify or provide any further guidance.

- ONC cannot address any comment suggestion or statement made by anyone attending the presentation or consider any such comment or suggestion in the rule writing process.

- Please submit comments through the formal process outlined in the Federal Register.

The Office of the National Coordinator for
Health Information Technology

Agenda

- Purpose of the Rule

- Deregulatory Actions for Previous Rulemakings

- Updates to the 2015 Edition Certification Criteria

- Conditions and Maintenance of Certification

- Enforcement of the Conditions and Maintenance of Certification Requirements

- Modifications to the ONC Health IT Certification Program

- Information Blocking

- Health IT for Pediatric Care and Practice Settings

- Additional Requests for Information (RFIs)

- Timeline

The Office of the National Coordinator for
Health Information Technology

Implementation of the 21st Century Cures Act

KEY PROVISIONS IN TITLE IV OF THE CURES ACT	ONC'S WORK IN SUPPORT OF THE CURES ACT
Sec. 4001 Pediatrics	• ONC engaged with stakeholders in the public and private sector. • ONC developed ten recommendations for the voluntary certification of health IT for pediatric care in response to the requirement set forth by Congress in Section 4001 of the Cures Act. • ONC proposes to adopt new and revised certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children. • ONC is also focused on non-regulatory initiatives that are nimble and responsive to stakeholders, including development of informational resources to support setting-specific implementation that aligns with the ONC Health IT Certification Program.
Sec. 4002 Conditions of Certification	• ONC proposes an approach whereby the Conditions and Maintenance of Certification express initial and ongoing requirements for health IT developers and their certified Health IT Modules. • The Conditions of Certification with accompanying Maintenance of Certification requirements, consistent with the Cures Act, would focus on: (a) information blocking; (b) assurances; (c) communications; (d) application programming interfaces (APIs); (e) real world testing of certified health IT; and (f) attestations. • ONC proposes an enforcement approach to encourage consistent compliance with the requirements. The proposed rule outlines a corrective action process for ONC to review and take action for potential or known instances where a Condition or Maintenance of Certification requirement is not being met by a health IT developer under the ONC Health IT Certification Program.
Sec. 4003 Interoperability Definition	• ONC proposes that interoperability means, with respect to health IT, such health IT that: (1) enables the secure exchange of electronic health information (EHI) with, and use of EHI from, other health IT without special effort on the part of the user; (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and (3) does not constitute information blocking • The proposed definition is consistent with the Cures Act interoperability definition.

Implementation of the 21st Century Cures Act

KEY PROVISIONS IN TITLE IV OF THE CURES ACT	ONC'S WORK IN SUPPORT OF THE CURES ACT
Sec. 4004 Information Blocking	• ONC proposes seven categories of practices that would be considered reasonable and necessary that, provided certain conditions are met, would not constitute information blocking. These categories were developed based on feedback from stakeholders and consultation with appropriate federal agencies. • If the actions of a regulated actor (health care provider, health IT developer, or health information exchange or network) satisfy an exception, the actions would not be treated as information blocking and the actor would not be, as applicable, subject to civil penalties or other disincentives under the law.
Sec. 4005 Exchange with Registries	• ONC's proposed rule includes a Request for Information (RFI) on how a standards-based API might support improved information exchange between a health care provider and a registry in support of public health reporting, quality reporting, and care quality improvement. • Public input on this RFI may be considered for future HHS rulemaking to support the bidirectional exchange of clinical data between health care providers and registries for a wide range of use cases.
Sec. 4006 Patient Access	• ONC proposes to promote policies that would ensure a patient's EHI is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient's health care providers and other individuals, including researchers, consistent with such patient's consent through the following proposals: United States Core Data for Interoperability (USCDI) standard; "EHI export" criterion; "standardized API for patient and population services" criterion, "data segmentation for privacy (DS4P)" criteria, "consent management for APIs" criterion; API Condition of Certification; and information blocking requirements, which include providing patients access to their EHI at no cost to them. • Patient access to their EHI would be improved through the adoption of the following proposed 2015 Edition standard and certification criteria: USCDI standard; standardized APIs for patient and population services; and EHI export.

Implementation of Executive Orders

EXECUTIVE ORDERS	ONC'S WORK IN SUPPORT OF EXECUTIVE ORDERS
Executive Order 13813 Promoting Healthcare Choice and Competition Across the United States	• ONC's proposed rule would contribute to fulfilling Executive Order 13813 by furthering patient (and health care provider) access to EHI and supporting competition in health care markets through new tools to access EHI and policies to address the hoarding of EHI. • ONC's proposed rule calls on the health care industry to adopt standardized APIs, which would allow individuals to securely and easily access structured EHI using new and innovative applications for smartphones and other mobile devices. • The proposed rule would establish information blocking provisions, focusing on improving patient and health care provider access, exchange, and use of EHI.
Executive Orders 13771 & 13777 Reducing Regulation and Controlling Regulatory Costs, and Enforcing the Regulatory Reform Agenda	• ONC reviewed and evaluated existing regulations to identify ways to reduce burden and implement deregulatory actions. • ONC proposes potential deregulatory actions that will reduce burden for health IT developers, providers, and other stakeholders. These six deregulatory actions are: (1) removal of a threshold requirement related to randomized surveillance; (2) removal of the 2014 Edition from the Code of Federal Regulations (CFR); (3) removal of the ONC-Approved Accreditor (ONC-AA) from the Certification Program; (4) removal of certain 2015 Edition certification criteria; (5) removal of certain Certification Program requirements; and (6) recognition of relevant Food and Drug Administration (FDA) certification processes with a request for information on the potential development of new processes for the ONC Health IT Certification Program.

Purpose

Increase Innovation and Competition
by giving patients and their health care providers safe and secure access to health information and to new tools, allowing for more choice in care and treatment.

Reduce Burden and Advance Interoperability
through the use of United States Core Data for Interoperability (USCDI) standard, new API requirements, and EHI export capabilities for the purposes of switching health IT or to provide patients their electronic health information.

Promote Patient Access
through a provision requiring that patients can electronically access *all* of their electronic health information (structured and/or unstructured) at no cost.

The Office of the National Coordinator for
Health Information Technology

https://www.healthit.gov/NPRM

Deregulatory Actions for Previous Rulemakings

Deregulatory Actions for Previous Rulemakings

Since the inception of the ONC Health IT Certification Program, ONC has aimed to implement and administer the ONC Health IT Certification Program in the least burdensome manner that supports our policy goals. Throughout the years, we have worked to improve the ONC Health IT Certification Program with a focus on ways to:

REDUCE BURDEN

OFFER FLEXIBILITY TO BOTH DEVELOPERS AND PROVIDERS

SUPPORT INNOVATION

EXECUTIVE ORDERS

In 2017, the President issued **Executive Orders 13771** and **13777** that require agencies to identify deregulatory actions and establish a process by which agencies review and evaluate existing regulations and make recommendations for repeal or simplification.

UPDATES TO THE ONC HEALTH IT CERTIFICATION PROGRAM

ONC has reviewed and evaluated existing ONC Health IT Certification Program regulations to identify ways to further reduce administrative burden, to implement deregulatory actions through guidance, and to propose potential new deregulatory actions in the proposed rule that will reduce burden for health IT developers, health care providers, and other stakeholders. **The proposed rule can be accomplished through six deregulatory activities:**

1. Removal of Randomized Surveillance Requirements
2. Removal of the 2014 Edition from the Code of Federal Regulations
3. Removal of the ONC-Approved Accreditor (ONC-AA) from the ONC Health IT Certification Program
4. Removal of Certain 2015 Edition Certification Criteria and Standards
5. Removal of Certain Program Requirements
6. Recognition of Food and Drug Administration (FDA) Processes

Deregulatory Actions for Previous Rulemakings

1. Removal of Randomized Surveillance Requirements

ONC-ACBs are required to conduct surveillance of certified health IT under the ONC Health IT Certification Program to ensure that health IT continues to conform and function as required by the full scope of the certification requirements.
On September 21, 2017, we exercised enforcement discretion with respect to the implementation of randomized surveillance by ONC-ACBs. We are now considering eliminating certain regulatory randomized surveillance requirements and changing the requirement that ONC-ACBs must conduct in-the-field, randomized surveillance, to specify that ONC-ACBs may conduct in-the-field, randomized surveillance.

Stakeholders have expressed concern that the benefits of in-the-field, randomized surveillance may not outweigh the time commitment required by providers, particularly if non-conformities are not found. The removal of randomized surveillance requirements would also give ONC-ACBs more time to focus on other priorities.

2. Removal of the 2014 Edition from the Code of Federal Regulations

The removal of the 2014 Edition from the Code of Federal Regulations (CFR) would make the 2015 Edition the baseline for health IT certification. Removal of the 2014 Edition would eliminate inconsistencies and costs caused by health IT certification and implementation of two different editions with different functionalities and versions of standards.

Patient care could improve through the reduced risk of error that comes with the health care system's consistent implementation and use of health IT certified to the 2015 Edition. Innovation could also improve with health IT developers (including third-party software developers) developing to only one set of newer standards and implementation specifications, which would be more predictable and less costly. Further, maintaining only the 2015 Edition would reduce the cost and burden for health IT developers, ONC-ACBs, and ONC-ATLs because they would no longer have to support two increasingly distinct sets of requirements.

Deregulatory Actions for Previous Rulemakings

3. Removal of the ONC-Approved Accreditor (ONC-AA) from the ONC Health IT Certification Program

The ONC-AA's role is to accredit certification bodies for the ONC Health IT Certification Program and to oversee the ONC-ACBs. However, years of experience and changes with the Program have led ONC to conclude that, in many respects, the role of the ONC-AA to oversee ONC-ACBs is now duplicative of ONC's direct oversight. More specifically, ONC's experience with administering the Principles of Proper Conduct for ONC-ACBs, as well as issuing necessary regulatory changes, has demonstrated that ONC, on its own, has the capacity to provide the appropriate oversight of ONC-ACBs. Therefore, we believe removal of the ONC-AA would reduce the ONC Health IT Certification Program's administrative complexity and burden.

4. Removal of Certain 2015 Edition Certification Criteria and Standards

ONC reviewed and analyzed the 2015 Edition Certification Criteria to determine whether there are certification criteria we could remove. We have identified both criteria and standards for removal. We believe the removal of these criteria and standards will reduce burden and costs for health IT developers and health care providers by eliminating the need to: design and meet specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting and disclosure requirements; maintain and update certifications for certified functionalities; and participate in surveillance of certified health IT.

Removed Criteria

2015 Base EHR Definition Criteria	x Problem list (§ 170.315(a)(6))	x Medication allergy list (§ 170.315(a)(8))
	x Medication list (§ 170.315(a)(7))	x Smoking status (§ 170.315(a)(11))
Other Criteria	x Drug formulary and preferred drug list checks (§ 170.315(a)(10)	x Common Clinical Data Set summary record –create (§ 170.315(b)(4))
	x Patient-specific education resource (§ 170.315(a)(13))	x Common Clinical Data Set summary record – receive (§ 170.315(b)(5))
		x Secure messaging (§ 170.315(e)(2))

Deregulatory Actions for Previous Rulemakings

5. Removal of Certain ONC Health IT Certification Program Requirements

We propose to remove certain mandatory disclosure requirements and a related attestation requirement. The disclosure requirements regarding certified health IT limitations are no longer necessary given the Cures Act information blocking provision and Conditions of Certification, which we are implementing with the proposed rule. We believe removal of these requirements will reduce costs and burden for ONC Health IT Certification Program stakeholders, particularly health IT developers and ONC-ACBs.

6. Agreement to Recognize Food and Drug Administration Processes

Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA), Public Law 112-144, required that the Food and Drug Administration (FDA), in consultation with ONC and the Federal Communications Commission (FCC) develop a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health IT, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication.

In 2017, FDA announced a voluntary Software Precertification (Pre-Cert) Pilot Program as part of a broader Digital Health Innovation Action Plan. It was developed to create a tailored approach for recognizing the unique characteristics of digital technology by looking first at the firm, rather than reviewing each product, as is currently done for traditional medical products. ONC believes that health IT developers that go through a finalized Software Pre-Certification Pilot Program and present health IT for certification under the Program could qualify for, and benefit from, further efficiencies under the Program.

Updates to the 2015 Edition Certification Criteria

This rule proposes to update the 2015 Edition by not only proposing criteria for removal, but by proposing to revise and add new certification criteria that would establish the capabilities and related standards and implementation specifications for the certification of health IT.

https://www.healthit.gov/sites/default/files/understanding-certified-health-it-2.pdf *

*Note: this is a link to the current certification criteria but it will need to be updated after the Cures Act final rule is released.

The Office of the National Coordinator for
Health Information Technology

Proposed Changes to the 2015 Edition Certification Criteria

Removed Criteria

2015 Base EHR Definition Criteria

- x Problem list (§ 170.315(a)(6))
- x Medication list (§ 170.315(a)(7))
- x Medication allergy list (§ 170.315(a)(8))
- x Smoking status (§ 170.315(a)(11))

Other Criteria

- x Drug formulary and preferred drug list checks (§ 170.315(a)(10)
- x Patient-specific education resource (§ 170.315(a)(13))
- x Common Clinical Data Set summary record – create (§ 170.315(b)(4))
- x Common Clinical Data Set summary record – receive (§ 170.315(b)(5))
- x Secure messaging (§ 170.315(e)(2))

Updated Criteria

Remove

- x Electronic prescribing (§ 170.315(b)(3))
- x Data export (§ 170.315(b)(6))
- x Data segmentation for privacy – send (§ 170.315(b)(7))
- x Data segmentation for privacy – receive (§ 170.315(b)(8))
- x Application access – data category request (§ 170.315(g)(8))

Update with

- ✓ Electronic prescribing (§ 170.315(b)(11))
- ✓ Electronic health information (EHI) export (§ 170.315(b)(10))
- ✓ Data segmentation for privacy – send (§ 170.315(b)(12))
- ✓ Data segmentation for privacy – receive (§ 170.315(b)(13))
- ✓ Standardized API for patient and population services (§ 170.315(g)(10))

Revised Criteria

- ✓ Clinical Quality Measures (CQMs) – report criterion (§ 170.315(c)(3))
- ✓ Common Clinical Data Set/ United States Core Data for Interoperability criteria (§ 170.315(b)(1), (e)(1), (f)(5), (g)(6), and (g)(9))
- ✓ C-CDA Companion Guide criteria (The above listed criteria and § 170.315(b)(2) and (b)(9))
- ✓ Minimum Standards Code Sets criteria

New Criteria

- + Encrypt authentication credentials (§ 170.315(d)(12))
- + Multi-factor authentication (MFA) (§ 170.315(d)(13))
- + Consent management for application programming interfaces (§ 170.315(g)(11))

Proposed Revised 2015 Edition Base EHR Definition

Statutory Capabilities	Certification Criteria Status for Revised Base EHR Definition
Includes patient demographic and clinical health information, such as medical history and problem lists	**Demographics** § 170.315(a)(5) ~~Problem List § 170.315(a)(6)~~ ~~Medication List § 170.315(a)(7)~~ ~~Medication Allergy List § 170.315(a)(8)~~ ~~Smoking Status § 170.315(a)(11)~~ **Implantable Device List** § 170.315(a)(14)
Capacity to provide clinical decision support	**Clinical Decision Support** § 170.315(a)(9)
Capacity to support physician order entry	**Computerized Provider Order Entry (medications, laboratory, or diagnostic imaging)** § 170.315(a)(1), (2) or (3)
Capacity to capture and query information relevant to health care quality	**Clinical Quality Measures – Record and Export** § 170.315(c)(1)
Capacity to exchange electronic health information with, and integrate such information from other sources	**Transitions of Care** § 170.315(b)(1) **Data Export** § 170.315(b)(6) **Electronic Health Information Export** § 170.315(b)(10)* **Application Access – Patient Selection** § 170.315(g)(7) **Application Access – Data Category Request** § 170.315(g)(8)* **Application Access – All Data Request** § 170.315(g)(9) **Standardized API for Patient and Population Services** § 170.315(g)(10)* **Direct Project** § 170.315(h)(1) or **Direct Project, Edge Protocol, and XDR/XDM** § 170.315(h)(2)

KEY
- ■ unchanged
- ■ proposed for removal
- ■ proposed revisions
- ■ propose to replace current criterion with a new criterion over a 24-month transition period from the effective date of the final rule

The United States Core Data for Interoperability Standard

We propose to remove the "Common Clinical Data Set" (CCDS) definition and its references from the 2015 Edition and replace it with the "United States Core Data for Interoperability" (USCDI) standard. This will increase the minimum baseline of data classes that must be commonly available for interoperable exchange.
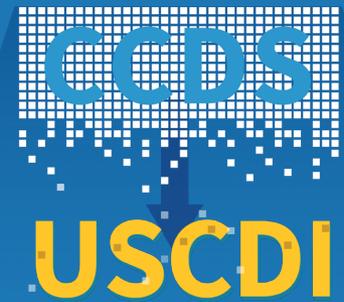
USCDI reflects the same data classes referenced by the CCDS definition and includes the following new required data classes and data elements:

Provenance

Clinical Notes

Pediatric Vital Signs

Address & Phone Number

If adopted, health IT developers will need to update their certified health IT to support the USCDI for all certification criteria affected by this change.

USCDI Standard Annual Update Schedule
ONC intends 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.

https://www.healthit.gov/NPRM
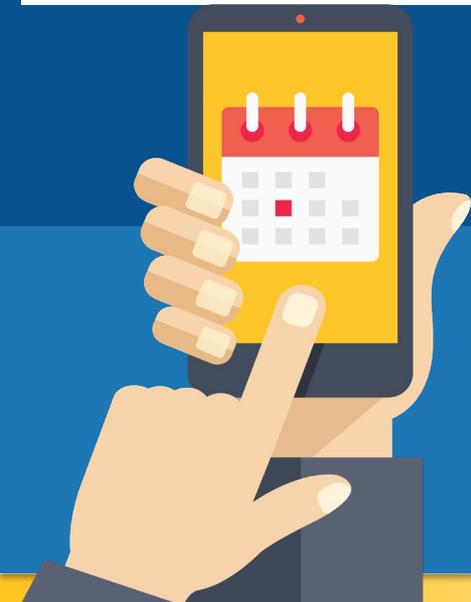
Electronic Health Information (EHI) Export Criterion
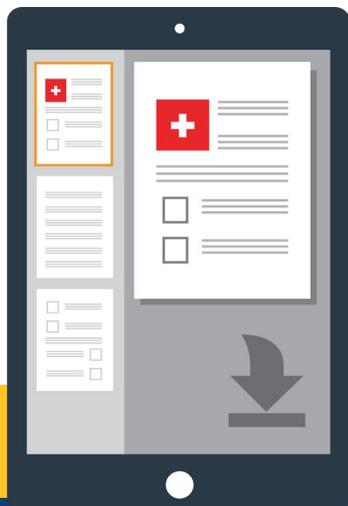
- Our new proposal would require health IT developers to provide the capability to electronically export all EHI that they produce and electronically manage in a computable format.

- We propose to make this criterion part of the 2015 Edition Base EHR definition, and for providers and developers to implement this within 24 months of the final rule's effective date.

HOW WILL IT WORK?

The proposed EHI Export certification requirement requires that:

1

All EHI produced and electronically managed by a developer's health IT must be readily available to export for:

A. a single patient upon request for their health data, and

B. all patients when a provider seeks to change Health IT systems.

2

The export file must:

A. be computable, and

B. include documentation to allow for interpretation and use of EHI. The documentation must be made publicly available via a hyperlink.

Note: Health IT developers would have the flexibility to determine their products' export standards.

https://www.healthit.gov/NPRM

Application Programming Interface (API) Criterion

- We propose to adopt a new API criterion in § 170.315(g)(10), which would replace the "application access – data category request" certification criterion (§ 170.315(g)(8)) and become part of the 2015 Edition Base EHR definition. This new certification criterion would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications.

  » https://www.hl7.org/fhir/overview.html

- Supports two types of API-enabled services:

  » Services for which a **single patient's data** is the focus

  » Services for which **multiple patients' data** are the focus

  https://www.healthit.gov/NPRM

Electronic Prescribing and Clinical Quality Measures

ELECTRONIC PRESCRIBING (e-Rx) STANDARD AND CERTIFICATION CRITERION

- We propose to update the e-Rx SCRIPT standard in 45 CFR 170.205(b) to NCPDP SCRIPT 2017071, which would result in a new e-Rx standard eventually becoming the baseline for certification. We also propose to adopt a new certification criterion in § 170.315(b)(11) for e-Rx to reflect these updated proposals.
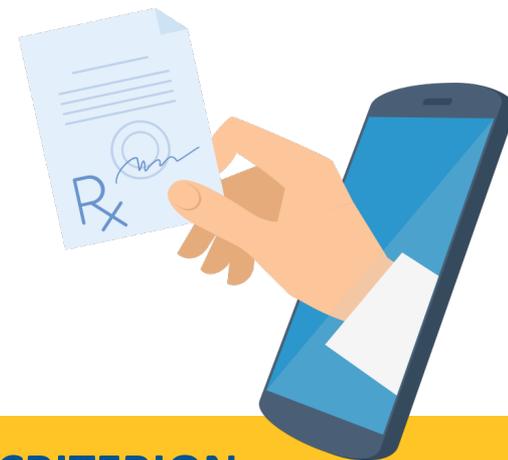
CLINICAL QUALITY MEASURES (CQMs) – REPORT CRITERION

- We propose to remove the HL7 Quality Reporting Document Architecture (QRDA) base standard conformance requirements from the 2015 Edition "CQMs – report" criterion in § 170.315(c)(3) and, in their place, require Health IT Modules to support the CMS QRDA Implementation Guide (IGs).
    - This would reduce the burden for health IT developers by only having to support one implementation of the QRDA standard rather than two (i.e., the HL7 and CMS IGs).
    - https://ecqi.healthit.gov/qrda-quality-reporting-document-architecture

The Office of the National Coordinator for
Health Information Technology

Privacy and Security Transparency Attestation Criteria

- We propose to add two new criteria to the 2015 Edition privacy and security certification framework:

  » **Encrypt Authentication Credentials**
    - Must be in accordance with FIPS Publication 140-2

  » **Multi-factor Authentication**
    - Must be in accordance with industry recognized standards (e.g. NIST Special Publication 800-63B Digital Authentication Guidelines, ISO 27001)

- Developers choose whether to have these functionalities for their certified health IT.
- These criteria are attestation based and developers would not be tested to these criteria.
- Developer must attest **YES or NO** to having the functionality; however developers' attestations would be listed on the Certified Health IT Product List
- Already certified health IT would need to be "re-certified" to these criteria within 6 months of the final rule effective date*

For health IT certified for the first time after the final rule effective date, they would need to meet the criteria at the time of certification

The Office of the National Coordinator for
Health Information Technology

Data Segmentation for Privacy and Consent Management Criteria

The **Data Segmentation for Privacy (DS4P)** standard describes the ability to apply and recognize security labels in a summary document (C-CDA) so that the recipient of the document can recognize the existence of sensitive elements within the summary document. The current DS4P criteria focus on document level "tagging." Under the proposed new criteria, health IT would be required to be able to tag data at the **document-level**, the **section-level**, and individual **data element-level**.

Consent2Share is an open source application for data segmentation and consent management. SAMHSA created a FHIR implementation guide that describes how the Consent2Share application and associated access control solution uses the FHIR Consent resource to represent and persist patient consent for treatment, research, or disclosure. Under the new "consent management for APIs" criterion, we propose to support data segmentation and consent management through an API in accordance with the Consent IG.

PROPOSED UPDATES

Remove current DS4P Criteria

CCDA Criteria

- DS4P-send (§ 170.315(b)(7))
- DS4P-receive (§ 170.315(b)(8))

Replace with new

DS4P and Consent Management certification criteria

C-CDA Criteria Based on HL7 DS4P Standard

+ **New DS4P-send** (§ 170.315(b)(12))

+ **New DS4P-receive** (§ 170.315(b)(13))

FHIR Criteria

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

Conditions and Maintenance of Certification

Conditions and Maintenance of Certification

The 21st Century Cures Act (Section 4002) requires the Secretary of HHS to establish Conditions and Maintenance of Certification requirements for the ONC Health IT Certification Program

ONC proposes an approach whereby the Conditions and Maintenance of Certification express initial requirements and ongoing requirements for health IT developers and their certified Health IT Module(s). Any noncompliance with the proposed Conditions and Maintenance of Certification requirements would be subject to ONC direct review, corrective action, and enforcement procedures under the ONC Health IT Certification Program.

There are seven Conditions of Certification with accompanying Maintenance of Certification Requirements. They are:

1. **Information Blocking**

2. **Assurances**

3. **Communications**

4. **Application Programming Interfaces (APIs)**

5. **Real World Testing**

6. **Attestations**

7. *(Future) Electronic Health Record (EHR) Reporting Criteria Submission*

https://www.healthit.gov/NPRM

Information Blocking - § 170.401

CONDITIONS OF CERTIFICATION

- As a Condition of Certification and to maintain such certification, a health IT developer must not take any action that constitutes information blocking as defined in section 4004 of the Cures Act

- This provision is subject to the seven proposed exceptions to the information blocking definition, which define certain reasonable and necessary activities that would not constitute information blocking (e.g., exceptions for preventing harm, promoting the privacy of EHI, promoting the security of EHI, etc.)

MAINTENANCE OF CERTIFICATION

- No accompanying Maintenance of Certification requirements beyond ongoing compliance with the Condition

Assurances - § 170.402

CONDITION OF CERTIFICATION

A health IT developer must provide assurances to the Secretary (unless for reasonable and necessary activities identified by the Secretary) that it will not take any action that constitutes information blocking or any other action that may inhibit the appropriate exchange, access, and use of electronic health information (EHI)

a. Full Compliance and Unrestricted Implementation of Certification Criteria Capabilities

- A health IT developer must ensure that its certified health IT conforms to the full scope of the applicable certification criteria
- Developers of certified health IT must provide assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes

b. Certification to the "Electronic Health Information (EHI) Export" Criterion

- A health IT developer that produces and electronically manages EHI must certify health IT to the 2015 Edition "electronic health information export" certification criterion in § 170.315(b)(10)

MAINTENANCE OF CERTIFICATION
Such developer must provide all of its customers with certified health IT with the functionality included in § 170.315(b)(10) within 24 months of the final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer

c. Records and Information Retention

MAINTENANCE OF CERTIFICATION
Health IT developers would have to retain records and information necessary to demonstrate ongoing compliance

d. Trusted Exchange Framework and the Common Agreement - *Request for Information*

- ONC is requesting comment as to whether certain health IT developers should be required to participate in, and adhere to, the Trusted Exchange Framework and Common Agreement
- This requirement would apply to health IT developers that certify to capabilities used for interoperability (i.e., §§ 170.315(b)(1), (c)(1) and (c)(2), (e)(1), (f), and (g)(9) through (11))

The Office of the National Coordinator for
Health Information Technology

Communications - § 170.403

CONDITIONS OF CERTIFICATION

- Requires that a health IT developer does not prohibit or restrict communication regarding the following subjects for the health IT:
  - Usability
  - Interoperability
  - Security
  - User experiences
  - Business practices
  - The manner in which a user of health IT has used such technology

- The Condition includes very limited exceptions to the prohibition (e.g., certain prohibitions and restrictions on communications by the health IT developer could be permissible when it would infringe the intellectual property rights existing in the developer's health IT)

MAINTENANCE OF CERTIFICATION

- A health IT developer must notify all customers within six months of the effective date of a subsequent final rule, that any communication or contract/agreement provision that violates the Communications Condition of Certification will not be enforced by the health IT developer

- Notice to customers would need to be provided annually up to and until the health IT developer amends the contract or agreement to remove or void any contractual provisions that violate this Condition of Certification

  - Developer must amend their contracts or agreements within a reasonable period of time, but not to exceed 2 years

Application Programming Interfaces - § 170.404

API TECHNOLOGY ROLES

API Technology Supplier
Health IT developer that creates API technology presented for certification in the ONC Health IT Certification Program

API Data Provider
Health care organization that deploys the API technology

API User
Persons and entities that use or create software applications that interact with API technology

ONC has designed API Conditions of Certification that will complement the technical capabilities described in our other proposals, while addressing the broader technology and business landscape in which these API capabilities will be deployed and used.

Note: The API Conditions of Certification only apply to API Technology Suppliers with health IT certified to any API-focused certification criteria

TRANSPARENCY	PERMITTED FEES	PRO-COMPETITIVENESS
ONC has proposed that API Technology Suppliers make business and technical documentation necessary to interact with their APIs in production freely and publicly accessible.	ONC has proposed to adopt specific conditions that would set boundaries for the fees API Technology Suppliers would be permitted to charge and to whom those permitted fees could be charged.	ONC has proposed that API Technology Suppliers would have to comply with certain requirements to promote an open and competitive marketplace.

https://www.healthit.gov/NPRM

Application Programming Interfaces (APIs) - § 170.404

CONDITIONS OF CERTIFICATION

- Requires health IT developers to publish APIs that allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law

  - Through the APIs, a developer must also provide access to all data elements (i.e., the USCDI) of a patient's EHR to the extent permissible under applicable privacy laws

- An API Technology Supplier must make business and technical documentation necessary to interact with their APIs in production freely and publicly accessible

- All fees related to API technology, not otherwise permitted by this section, are prohibited from being imposed by an API technology Supplier

- API Technology Suppliers must grant API Data Providers (i.e., health care providers who purchase or license API technology) the sole authority and autonomy to permit API Users to interact with the API technology

MAINTENANCE OF CERTIFICATION

- An API Technology Supplier must register and enable all applications for production use within one business day of completing its verification of an applications developer's authenticity

- An API Technology Supplier must Support the publication of "Service Base URLs" (i.e., FHIR® server endpoints) 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 at no charge

- An API Technology Supplier with API technology certified to § 170.315(g)(8) must provide all API Data Providers with a (g)(10)-certified API within 24 months of this final rule's effective date

Real World Testing - § 170.405

CONDITIONS OF CERTIFICATION

- Requires that health IT developers have successfully tested the real-world use of the technology for interoperability in the type of setting in which such technology would be marketed

- This Condition of Certification applies to health IT developers with Health IT Module(s) certified to certain certification criteria focused on interoperability and data exchange (i.e., §§ 170.315(b), (c)(1) through (c)(3), (e)(1), (f), (g)(7) through (g)(11), and (h))

MAINTENANCE OF CERTIFICATION

- Health IT developers must submit publicly available prospective annual real world testing plans and retrospective annual real world testing results for certified health IT products focused on interoperability

- Standards Version Advancement Process: permits health IT developers to voluntarily use newer versions of adopted standards. Please also see the Standards Version Advancement Process fact sheet for more details.

Standards Version Advancement Process

- The Standards Version Advancement Process would allow developers to choose among the versions of standards and implementation specifications listed in regulation or National Coordinator (NC)-approved newer version updates for any or all standards applicable to criteria subject to real world testing requirements.

- This flexibility to choose among NC-approved versions of standards and implementation specifications would be available both when developers seek initial certification or to maintain certification of a Health IT Module.

HOW WILL IT WORK?

To take advantage of the flexibility to update to NC-approved versions, a developer will need to:

- Notify its ONC-Authorized Certification Body (ONC-ACB) and its customers of its intent to move to newer NC-approved standards version updates as well as whether, and for how long, they might plan to continue supporting prior versions of the standards.

- Ensure that the standards version updates are effectively implemented.

- Address standards version updates in the required annual real world testing plans and results.

- Demonstrate conformance of its health IT to all applicable criteria including, but not limited to, any NC-approved standards versions it has chosen to incorporate into its certified Health IT Module.

How Versions Get Approved

Consider Available Updates
Publish Draft
Comments on Draft
Comment Review
Determinations Published

Ongoing Dialogue

https://www.healthit.gov/NPRM

Attestations - § 170.406

CONDITION OF CERTIFICATION

- A health IT developer must provide an attestation, as applicable, to compliance with the Conditions and Maintenance of Certification, except for the "EHR reporting criteria submission" Condition of Certification

MAINTENANCE OF CERTIFICATION

- Health IT developers must submit their attestations every six months

Enforcement of the Conditions and Maintenance of Certification Requirements

Enforcement Approach

ONC DIRECT REVIEW OF THE CONDITIONS AND MAINTENANCE OF CERTIFICATION

- ONC would be the sole party responsible for enforcing compliance. ONC may, however, coordinate its review with the HHS Office of Inspector General (OIG) or defer to the OIG to lead review of a claim of information blocking.

- ONC will utilize the processes established for ONC direct review of certified health IT in the Enhanced Oversight and Accountability (EOA) final rule for enforcement. Using the established processes delivers multiple benefits:

  - EOA processes address non-conformities with Program requirements. Any noncompliance with the Conditions and Maintenance of Certification would constitute a Program non-conformity

  - Health IT developers are familiar with the ONC direct review provisions

  - The processes established for working with health IT developers is thorough and transparent, with clear corrective action procedures and remedies for Program non-conformities

  - Direct review provides equitable opportunities for health IT developers to respond to ONC actions and appeal certain determinations

Enforcement Approach

STEP 1 Initiating Review and Health IT Developer Notice

STEP 2 Records Access

STEP 3 Corrective Action Plan

STEP 4 Certification Ban and/or Termination

STEP 5 Appeal

STEP 6 Public Listing of Certification Ban and/or Terminations

Enforcement Approach

If ONC has reasonable belief that a health IT developer has not complied with the Conditions and Maintenance of Certification, ONC may initiate review and issue the health IT developer a notice of potential non-conformity or notice of non-conformity.

Effect on Existing Program Requirements and Processes

ONC's Authorized Certification Bodies (ONC-ACBs) would report to ONC any information that could inform whether ONC should exercise direct review for noncompliance with a Condition of Certification or any matter within the scope of ONC direct review.

No Suspension Processes

ONC believes the more streamlined processes proposed for addressing noncompliance with the Conditions and Maintenance of Certification alleviates the need to proceed through a suspension process.

Concurrent Enforcement and Coordination with the Office of the Inspector General (OIG)

The Cures Act authorizes the OIG to investigate claims that a health IT developer of certified health IT has engaged in information blocking. OIG is also authorized to investigate claims that a health IT developer of certified health IT has submitted a false attestation for the Conditions of Certification. We emphasize that ONC's and OIG's respective authorities under the Cures Act (and in general) are independent and that either or both offices may exercise these authorities at any time.

- ONC may coordinate its review of a claim of information blocking with the OIG or defer to the OIG to lead a review of a claim of information blocking.
- ONC may also rely on OIG findings to form the basis of a direct review action.

Enforcement Approach

ONC, or third parties acting on its behalf, must have access to the information necessary to enforce the Conditions and Maintenance of Certification. ONC would implement appropriate safeguards to ensure, to the extent permissible with federal law, that any proprietary business information or trade secrets would be kept confidential.

If ONC determines that a health IT developer is noncompliant with a Condition of Certification, ONC would work with the health IT developer to establish a corrective action plan (CAP) to remedy the issue.

If a health IT developer under ONC direct review for noncompliance with a Condition of Certification failed to work with ONC or was otherwise noncompliant with the requirements of the CAP and/or CAP process, ONC could issue a certification ban for the health IT developer (and its subsidiaries and successors). ONC may also terminate Health IT Module certificates if there is a nexus between the developer's actions or business practices and certified Health IT Module(s).

However, ONC's first and foremost priority is to work with health IT developers to remedy any noncompliance to ensure health IT developers are compliant with ONC Health IT Certification Program requirements in order to foster an environment where electronic health information (EHI) is exchanged in an interoperable way.

No Proposed Termination Step

- Different from the EOA direct review processes for proposed termination, ONC is not including "proposed termination" when a health IT developer fails to take appropriate and timely corrective action for noncompliance with a Condition of Certification.

- ONC may proceed directly to issuing a certification ban or notice of termination if deemed appropriate, as noncompliance with these areas is likely to undermine the integrity of the Program and impede widespread interoperability and information exchange.

Enforcement Approach

STEP 5 Appeal

A health IT developer would have an opportunity to appeal an ONC determination to issue a certification ban and/or termination resulting from a non-conformity with a Condition of Certification.

STEP 6 Public Listing of Certification Ban and /or Terminations

ONC would publicly list banned health IT developers and/or terminated Health IT Modules on ONC's website for noncompliance with the Conditions and Maintenance of Certification requirements.

Modifications to the

ONC Health IT Certification

Program

Modifications to the ONC Health IT Certification Program – Updates to the Principles of Proper Conduct

ONC-ACBs MUST NOW:

1. Accept test results from any ONC-ATL in good standing.

2. Review and confirm health IT developer submission of real world testing plans and results and make plans and results publicly available.

3. Collect health IT developers' quarterly attestations and note in Certified Health IT Product List (CHPL) when Health IT Modules are updated under the Standards Version Advancement Process (VAP) flexibility.

4. Ensure that health IT developers seeking to take advantage of the Standards VAP flexibility comply with the applicable requirements, retain records of the timing and content of developers' § 170.405(b)(5) notices, and timely post each notice's content publicly on the CHPL.

5. Review and submit health IT developer Conditions and Maintenance of Certification attestations to ONC for public availability.

6. Report to ONC any information that could lead ONC to perform direct review, including potential noncompliance with a Condition of Certification.

NEW FLEXIBILITIES FOR ONC-ACBs:

1. The role of the ONC-AA would be eliminated, permitting ONC-ACBs to select the ISO/IEC 17065 accreditation body of their choice.

2. Certain randomized surveillance requirements would be eliminated.

3. ONC-ACBs would be able to certify Health IT Modules that they have evaluated for conformance with certification criteria without first passing through an ONC-ATL as long as conformity methods were approved by the National Coordinator.

NO LONGER REQUIRED:

1. Certain disclosure requirements regarding certified health IT limitations.

2. Transparency attestations by health IT developer regarding the sharing of information in its mandatory disclosures.

Information Blocking

Information Blocking

⭐ Section 4004 of the Cures Act authorizes the Secretary to identify reasonable and necessary activities that do not constitute information blocking.

⭐ In consultation with stakeholders, we have identified seven categories of practices that would be reasonable and necessary, provided certain conditions are met.

"Actors" regulated by the information blocking provision:

- Health Care Providers
- Health IT Developers of Certified Health IT
- Health Information Exchanges
- Health Information Networks

⭐ The seven categories of reasonable and necessary practices, and their corresponding conditions, are defined through the exceptions proposed at 45 CFR 171.201–207.

⭐ If the actions of a regulated actor (health care provider, health IT developer, or health information exchange or network) satisfy one or more exception, the actions would not be treated as information blocking and the actor would not be subject to civil penalties and other disincentives under the law.

https://www.healthit.gov/NPRM

★ What is information blocking?

A practice by a health care provider, health IT developer, health information exchange, or health information network that, except as required by law or specified by the Secretary as a reasonable and necessary activity, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.
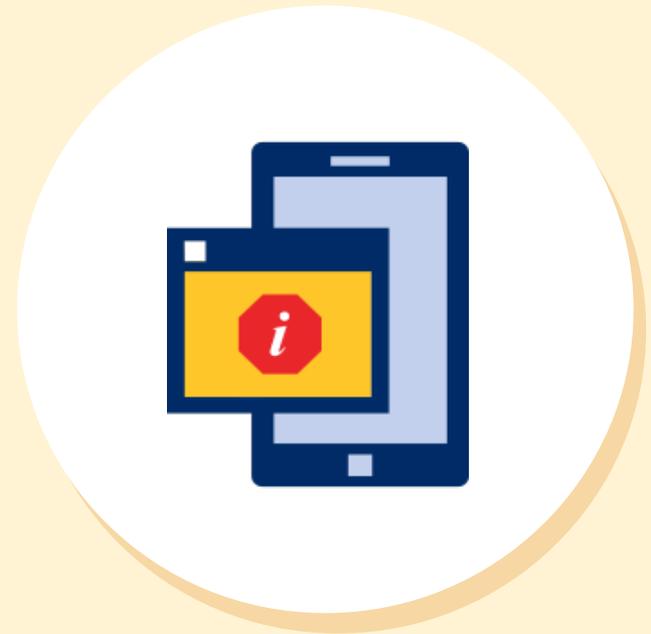
Key Concepts

- We propose to define EHI to mean electronic protected health information (as defined in HIPAA), and any other information that:

  » is transmitted by or maintained in electronic media (as defined in 45 CFR 160.103);

  » identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual;

  » 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.

- Not limited to information that is created or received by a health care provider.

- Does not include health information that is de-identified consistent with the requirements of 45 CFR 164.514(b).

The Office of the National Coordinator for
Health Information Technology

Price Information – Request for Information

- The fragmented and complex nature of pricing within the health care system has decreased the efficiency of the health care system and has had negative impacts on patients, health care providers, health systems, plans, plan sponsors and other key health care stakeholders.

- Consistent with its statutory authority, the Department is considering subsequent rulemaking to expand access to price information for the public, prospective patients, plan sponsors, and health care providers.

- ONC has a unique role in setting the stage for such future actions by establishing the framework to prevent the blocking of price information.

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

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

The Office of the National Coordinator for
Health Information Technology

Information Blocking Exceptions

- **§ 171.201 Exception** | Preventing Harm

  » An actor may engage in practices that are reasonable and necessary to prevent physical harm to a patient or another person.

  » The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of physical harm to a patient or another person.

  » The practice must implement an organizational policy that meets certain requirements or must be based on an individualized assessment of the risk in each case.

This proposed exception acknowledges that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of electronic health information (EHI).

Information Blocking Exceptions

- **§ 171.202 Exception** | Promoting the Privacy of Electronic Health Information

  » An actor may engage in practices that protect the privacy of EHI.

  » An actor must satisfy at least one of four discrete sub-exceptions that address scenarios that recognize existing privacy laws and privacy-protective practices: (1) practices that satisfy preconditions prescribed by privacy laws; (2) certain practices not regulated by HIPAA but which implement documented and transparent privacy policies; (3) denial of access practices that are specifically permitted under HIPAA; (4) practices that give effect to an individual's privacy preferences.

  » The information blocking provision will not require that actors provide access, exchange, or use of EHI in a manner that is not permitted under the HIPAA Privacy Rule.

  » General conditions apply to ensure that practices are tailored to the specific privacy risk or interest being addressed and implemented in a consistent and non-discriminatory manner.

This proposed exception would advance the goal of preventing information blocking for improper or self-interested purposes while maintaining and upholding the privacy rights that patients now have.

Information Blocking Exceptions

- **§ 171.203 Exception** | Promoting the Security of Electronic Health Information

  » An actor may implement measures to promote the security of EHI.

  » The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.

  » The practice must be tailored to specific security risks and must be implemented in a consistent and non-discriminatory manner.

  » The practice must implement an organizational security policy that meets certain requirements or must be based on an individualized determination regarding the risk and response in each case.

This proposed exception would protect actors who mitigate security risks and implement appropriate safeguards to secure the EHI they control.

Information Blocking Exceptions

- **§ 171.204 Exception** | Recovering Costs Reasonably Incurred

  » An actor may recover costs that it reasonably incurs, in providing access, exchange, or use of EHI.

  » Fees must be: (1) charged on the basis of objective and verifiable criteria uniformly applied to all similarly situated persons and requests; (2) related to the costs of providing access, exchange, or use; and (3) reasonably allocated among all customers that use the product/service.

  » Fees must not be based on anti-competitive or other impermissible criteria.

  » Certain costs would be specifically excluded from coverage under this exception, such as costs that are speculative or subjective or costs associated with electronic access by an individual to their EHI.

This proposed exception acknowledges that actors should be able to recover costs that they reasonably incur to develop technologies and provide services that enhance interoperability and promote innovation, competition, and consumer welfare.

Information Blocking Exceptions

- **§ 171.205 Exception** | Responding to Requests that are Infeasible

  » An actor may decline to provide access, exchange, or use of EHI in a manner that is infeasible.

  » Complying with the request must impose a substantial burden on the actor that is unreasonable under the circumstances (taking into account the cost to the actor, actor's resources, etc.).

  » The actor must timely respond to infeasible requests and work with requestors to provide a reasonable alternative means of accessing the EHI.

This proposed exception acknowledges that there may be legitimate practical challenges beyond an actor's control that may limit its ability to comply with requests for access, exchange, or use of EHI.

Information Blocking Exceptions

- **§ 171.206 Exception** | Licensing of Interoperability Elements on Reasonable and Non-discriminatory Terms

    » An actor that controls technologies or other interoperability elements that are necessary to enable access to EHI will not be information blocking so long as it licenses such elements on reasonable and non-discriminatory terms.

    » The license can impose a reasonable royalty but must include appropriate rights so that the licensee can develop, market, and/or enable the use of interoperable products and services.

    » The terms of the license must be based on objective and verifiable criteria that are uniformly applied and must not be based on impermissible criteria, such as whether the requestor is a potential competitor.

This proposed exception would allow actors to protect the value of their innovations and earn returns on the investments they have made to develop, maintain, and update those innovations.

Information Blocking Exceptions

- **§ 171.207 Exception** | Maintaining and Improving Health IT Performance

  » An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT.

  » An actor must ensure that the health IT is unavailable for no longer than necessary to achieve the maintenance or improvements.

  » The practice must be implemented in a consistent and non-discriminatory manner.

  » In circumstances when health IT is supplied to an individual or entity, the individual or entity (e.g., customer) must agree to the unavailability of health IT.

The proposed exception recognizes that it may be reasonable and necessary for actors to make health IT, and in turn EHI, temporarily unavailable for the benefit of the overall performance of health IT.

Complaint Process and Requests for Information

- Complaint Process
  - » Section 3022(d)(3)(A) of the PHSA directs the National Coordinator to implement a standardized process for the public to submit reports on claims of health information blocking.
  - » We intend to implement and evolve this complaint process by building on existing mechanisms, including the complaint process currently available at https://www.healthit.gov/healthit-feedback.
  - » We request comment on this approach and any alternative approaches that would best effectuate this aspect of the Cures Act.

- Additional Exceptions
  - » We are considering whether we 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.
  - » We welcome comment on any potential new exceptions we should consider for future rulemaking.

- 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.

The Office of the National Coordinator for
Health Information Technology

Health IT for Pediatric Care and Practice Settings

Health IT for Pediatric Care and Practice Settings

In response to the requirements set forth in section 4001 of the Cures Act, ONC has:
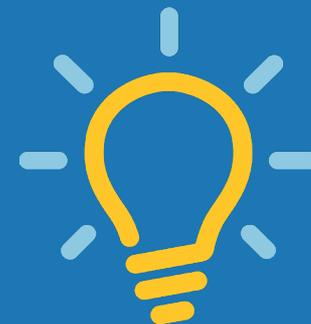
1 Developed ten recommendations for the voluntary certification of health IT for pediatric care that does NOT include a separate certification program for pediatric care and practice settings.

2 Identified current and proposed new 2015 Edition certification criteria that support pediatric care and practice settings.

3 Focused on non-regulatory initiatives that are nimble and responsive to stakeholders, including development of informational resources to support setting-specific implementation that aligns with the ONC Health IT Certification Program.

https://www.healthit.gov/NPRM

Health IT for Pediatric Care and Practice Settings

ONC DEVELOPED RECOMMENDATIONS BASED ON STAKEHOLDER-IDENTIFIED CLINICAL PRIORITIES AND THE CHILDREN'S EHR FORMAT

Pediatric stakeholders identified clinical priorities and evaluated them with ONC.

Access Children's EHR Format Here

ONC RECOMMENDATIONS FOR PEDIATRIC HEALTH IT VOLUNTARY CERTIFICATION CRITERIA

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

ONC CERTIFICATION CRITERIA TO SUPPORT PEDIATRIC CARE AND PRACTICE SETTINGS

CURRENT 2015 EDITION CRITERIA:

- Transitions of Care
- Care Plan
- View, Download, Transmit
- Application Programming Interface (API)
- Data Segmentation for Privacy
- Problem List
- Electronic Prescribing
- Common Clinical Data Set (CCDS)
- Social, Psychological, and Behavioral Data
- Clinical Quality Measure (CQM)
- Clinical Decision Support
- Immunizations
- Demographic data capture
- Family health history
- Patient health data capture
- Privacy and security

PROPOSED NEW 2015 EDITION CRITERIA:

- United States Core Data Set for Interoperability (USCDI)
- Electronic prescribing
- FHIR-based API
- Data segmentation for privacy

https://www.healthit.gov/NPRM

Additional Requests for Information (RFIs)

ONC recognizes that health IT offers promising strategies to help medical specialties and sites of service as they combat opioid use disorder (OUD).

- We request public comment on how our existing Program requirements and the proposals in this rulemaking may support use cases related to opioid use disorder (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.

The Office of the National Coordinator for
Health Information Technology
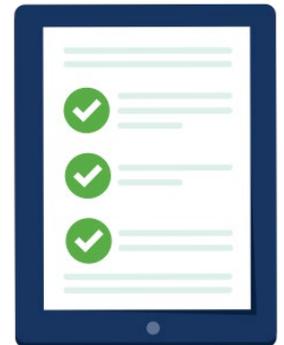
Patient Matching RFI

Patient matching is a critical component to interoperability and the nation's health information technology infrastructure. Accurate patient matching helps health care providers access and share the right information on the right patient when and where it is needed.

- Section 4007 of the 21st Century Cures Act directed the Government Accountability Office (GAO) to conduct a study on patient matching.

  » The GAO report, *Approaches and Challenges to Electronically Matching Patients' Records across Providers*, was released in January 2019. https://www.gao.gov/assets/700/696426.pdf

- 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 and CMS collaborated to jointly issue complementary requests for information regarding patient matching.

Exchange with Registries

- Section 4005 (a) and (b) of the Cures Act focuses on interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. ONC is approaching these provisions from several angles to address the technical capability of EHRs to exchange data with registries in accordance with applicable recognized standards.
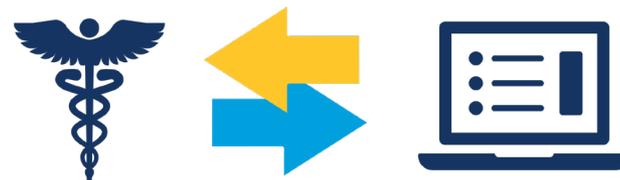
  » We include an RFI in the proposed rule on how a standards-based API might support improved information exchange between a health care provider and a registry to support public health reporting, quality reporting, and care quality improvement. Public input on this RFI may be considered for future HHS rulemaking to support the bidirectional exchange of clinical data between health care providers and registries for a wide range of use cases.

The Office of the National Coordinator for
Health Information Technology

21st Century Cures Act NPRM – Regulatory Implementation Milestones
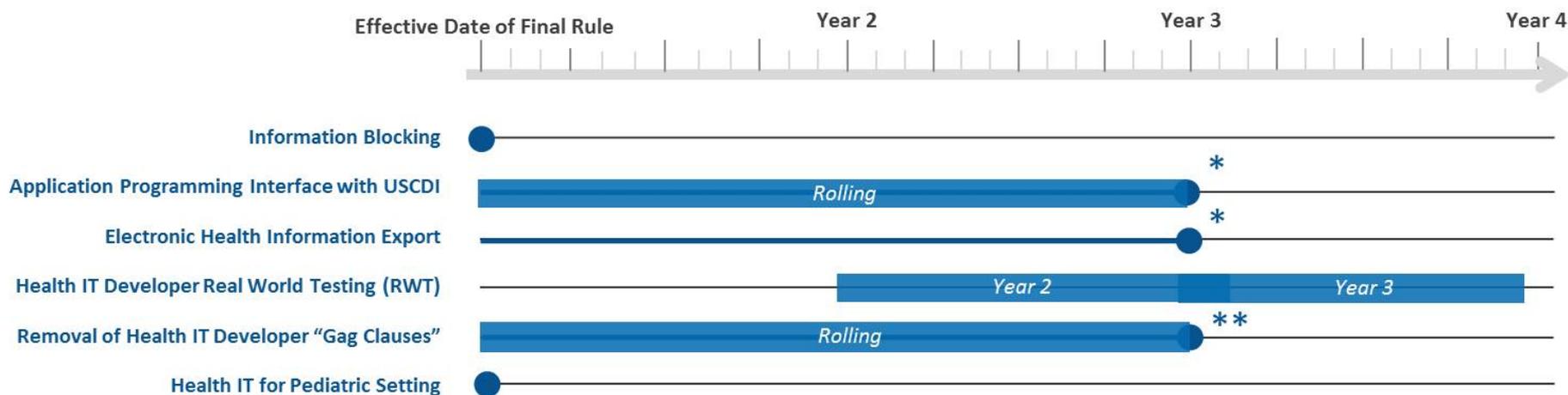
*Last day for health IT developers to implement for customers (health care providers)
**Last day to remove "gag clauses" from health IT contracts

The Office of the National Coordinator for
Health Information Technology

Questions

CONTACT INFORMATION

Elise Sweeney Anthony
Elise.Anthony@hhs.gov

Michael Lipinski
Michael.Lipinski@hhs.gov

@ONC_HealthIT   @HHSONC   HealthIT.gov