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

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

## Preface

This public comment template supports a specific proposed rule that would implement certain provisions of the 21st Century Cures Act. The template is not intended to substitute for review of the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program proposed rule published in the *Federal Register* at 84 FR 7424. A PDF copy of the official version of the rule is available from the FederalRegister.gov website at [https://www.govinfo.gov/content/pkg/FR-2019-](https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02224.pdf)  [03-04/pdf/2019-02224.pdf.](https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02224.pdf)

This template is intended to provide a simple way to organize and present comments on the new and modified provisions in 45 CFR Parts 170 and 171, and responses to specific questions posed in the preamble of the proposed rule. While use of this document is entirely voluntary, commenters may find it helpful to use the document in lieu of unstructured comments, or to use it as an addendum to narrative cover pages.

To further enhance the public comment experience, in complement to this public comment template, an 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.](https://www.healthit.gov/sites/default/files/page/2019-03/ONCCuresActProposedRule.docx) We believe having a copy of the rule available in Microsoft Word will make it easier for commenters to access and copy portions of the proposed rule for use in their individual comments.

The following tables are organized according to the table of contents of the proposed rule, and the order in which proposed new and revised provisions are discussed in the preamble of the rule rather than the order in which the proposals would be codified in regulatory text. Tables pertaining to proposals include the *Federal Register* page(s) of the proposed rule where the regulatory impact analysis related to the proposal can be found. All tables include the *Federal Register* page(s) of the proposed rule where the preamble discussion of the proposal can be found. Each table provides a field for submitting comments on the proposals or requests for information, including, but not limited to, responses to specific questions or requests for comment posed in the preamble. This field can be expanded as necessary for commenting.

To be considered, all comments (including comments organized using this document) must be submitted according to the instructions in the proposed rule. Electronic submissions are strongly encouraged and can be easily completed through the regulations.gov website (The proposed rule’s docket is at <https://www.regulations.gov/document?D=HHS-ONC-2019-0002-0001>). Look for the “Comment Now” button on the upper right.

# 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:**  Click here to enter comments on proposed removals and revisions to regulatory surveillance requirements in § 170.556(c). |

|  |
| --- |
| **Removal of the 2014 Edition from the Code of Federal Regulations** |
| We propose to remove the 2014 Edition certification criteria [(§ 170.314](https://www.law.cornell.edu/cfr/text/45/170.314)) 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:**  Click here to enter comments on proposed removal of 2014 Edition certification criteria and all related terms and processes. |

|  |
| --- |
| **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:**  Click here to enter comments on proposal to remove the ONC-Approved Accreditor from the Program, including processes, definitions, and related rules. |

|  |
| --- |
| **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:**  Click here to enter comments on the proposal to remove the identified 2015 Edition criteria and standards, including any other 2015 Edition criteria and standards that should be considered for removal. |

|  |
| --- |
| **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:**  Click here to enter comments on the proposal to remove these requirements and any other certification requirements we should consider for removal. |

|  |
| --- |
| **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:**  Click here to enter comments our proposed “recognition” approach, including the 2015 Edition certification criteria that should be eligible for “recognition.” |

|  |
| --- |
| **Request for Information on the Development of Similar Independent Program Processes** |
| Recognition of the FDA Software Pre-Certification Program for purposes of certification of health IT to 2015 Edition criteria may eventually be determined to be infeasible or insufficient to meet our goals of reducing burden and promoting innovation. With this in mind, we request comment on whether ONC should establish new regulatory processes tailored towards recognizing the unique characteristics of health IT (e.g., electronic health record (EHR) software) by looking first at the health IT developer, rather than primarily at the health IT presented for certification, as is currently done under the Program. We also welcome more specific comments on the health IT developer criteria for such an approach and what the Conditions and/or Maintenance of Certification requirements should be to support such an approach within the framework of the proposed Conditions and Maintenance of Certification requirements discussed in section VII of this proposed rule. |
| **Preamble FR Citation:** 84 FR 7439 **Specific questions in preamble?** *No* |
| **Regulatory Impact Analysis:** Not applicable |
| **Public Comment Field:**  Click here to enter input in response to this request for information on development of similar independent program processes.. |

## 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:**  Click here to enter comments on § 170.213 United States Core Data for Interoperability and revisions to the CCDS-dependent 2015 Edition certification criteria. |

|  |
| --- |
| **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:**  Click here to enter comments on the proposed approach to updated versions of vocabulary standard code sets.. |

|  |
| --- |
| **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:**  Click here to enter comments on the proposed requirement of the C-CDA UDI IG for health IT to meet the requirements of the UDI USCDI Data Class. |

|  |
| --- |
| **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:**  Click here to enter comments the proposed alternative approach to the USCDI Medication Allergies data element.. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on 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:**  Click here to enter comments on the proposal to adopt the National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 at § 170.205(b) Electronic prescribing. |

|  |
| --- |
| **§ 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:   1. Ask mailbox (GetMessage). 2. Relay acceptance of transaction (Status). 3. Error response (Error). 4. Create new prescriptions (NewRx, NewRxRequest, NewRxResponseDenied). 5. Change prescriptions (RxChangeRequest, RxChangeResponse). 6. Renew prescriptions (RxRenewalRequest, RxRenewalResponse). 7. Resupply (Resupply). 8. Return receipt (Verify) 9. Cancel prescriptions (CancelRx, CancelRxResponse). 10. Receive fill status notifications (RxFill, RxFillIndicatorChange). 11. Drug administration (DrugAdministration). 12. Transfer (RxTransferRequest, RxTransferResponse, RxTransferConfirm). 13. Recertify (Recertification). 14. Request and receive medication history (RxHistoryRequest, RxHistoryResponse). 15. Complete risk evaluation and mitigation strategy transactions (REMSInitiationRequest, REMSInitiationResponse, REMSRequest, and REMSResponse). 16. 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. 17. *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. 18. Limit a user’s ability to prescribe all oral liquid medications in only metric standard units of mL (i.e., not cc). 19. 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:**  Click here to enter comments on 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:**  Click here to enter comments on proposed modifications to § 170.205(h) Clinical quality measure data import, export and reporting standards. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on proposed modifications to § 170.205(k) Clinical quality measure aggregate reporting standards. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on proposed modifications to the § 170.315(c)(3) Clinical quality measures – report certification criterion. |

|  |
| --- |
| **§ 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.   1. 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. 2. A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate. 3. 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. 4. The export file(s) created must be electronic and in a computable format. 5. The export file(s) format, including its structure and syntax, must be included with the exported file(s). 6. Database export. Create an export of all the electronic health information the health IT produces and electronically manages.    1. The export created must be electronic and in a computable format.    2. 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:**  Click here to enter comments on proposed modifications to the § 170.315(c)(3) Clinical quality measures – report certification criterion. |

|  |
| --- |
| **§ 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:   1. “Yes.” Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2). 2. “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:**  Click here to enter comments on the certification requirements proposed at § 170.315(d)(12) Encrypt authentication credentials. |

|  |
| --- |
| **§ 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:   1. “Yes.” Health IT Module supports authentication through multiple elements the identity of the user with industry recognized standards. 2. “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:**  Click here to enter comments on the certification requirements proposed at § 170.315(d)(13) Multi-factor authentication. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on 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:   1. 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 2. 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:**  Click here to enter comments on 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:   1. The standard adopted in § 170.215(c)(1); and 2. The implementation specification adopted in § 170.215(c)(2). 3. Documentation.    1. 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:**  Click here to enter comments on proposed § 170.315(g)(11) Consent management for APIs. |

*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*](#_bookmark0) [*VII,*](#_bookmark0) *below.*

## Section V – Modifications to the ONC Health IT Certification Program

|  |
| --- |
| **§ 170.550 Health IT Module certification** |
| \* \* \* \* \*   1. 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. 2. [Reserved]   (g) \* \* \*   1. 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) \* \* \*   * 1. 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);  \* \* \* \* \*   1. 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); 2. 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   \* \* \* \* \*   1. 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:**  Click here to enter comments on § 170.550 Health IT Module certification. |

### § 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).

\* \* \* \* \*

1. Reporting. \* \* \*

(2) [Reserved]

1. 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;
2. Testing. Only certify Health IT Modules that have been:
   1. Tested, using test tools and test procedures approved by the National Coordinator, by an:
      1. ONC-ATL;
      2. 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.

\* \* \* \* \*

1. 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).

\* \* \* \* \*

1. 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.   1. Attestations. Review and submit health IT developer Conditions and Maintenance of Certification   attestations made in accordance with § 170.406 to ONC for public availability.   1. 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. 2. 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). 3. 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:**  Click here to enter comments on § 170.523 Principles of proper conduct for ONC-ACBs. |

|  |
| --- |
| **§ 170.524 Principles of proper conduct for ONC-ATLs (Authorized Testing Laboratories)** |
| \* \* \* \* \*   1. 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:**  Click here to enter comments on revisions to § 170.524 Principles of proper conduct for ONC-ATLs. |

## 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:**  Click here to enter comments on our approach to health IT for the care continuum and implementing § 4001(b) of the Cures Act. |

|  |
| --- |
| **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:**  Click here to enter input in response to the request for information on health IT and opioid use disorder prevention and treatment. |

***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** |
| 1. 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. 2. Maintenance of Certification*.* [Reserved] |
| **Preamble FR Citation:** 84 FR 7465 **Specific questions in preamble?** *No* |
| **Regulatory Impact Analysis:** Not applicable |
| **Public Comment Field:**  Click here to enter comments on proposed § 170.401 Information blocking Condition and Maintenance of Certification requirement. |

|  |
| --- |
| **§ 170.402 Assurances** |
| 1. 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). 2. 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:       1. A period of 10 years beginning from the date each of a developer’s health IT is first certified under the Program; or       2. 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:**  Click here to enter comments on proposed §170.402 Assurances. |

|  |
| --- |
| **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:**  Click here to enter input in response to the request for more information on participation of health IT developers in the Trusted Exchange Framework and Common Agreement. |

### § 170.403 Communications

* + 1. Condition of Certification.
       1. A health IT developer may not prohibit or restrict the communication regarding—
          1. The usability of its health IT;
          2. The interoperability of its health IT;
          3. The security of its health IT;
          4. Relevant information regarding users' experiences when using its health IT;
          5. The business practices of developers of health IT related to exchanging electronic health information; and
          6. 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.
          1. 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

1. Making a disclosure required by law;
2. Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;
3. Communicating information about cybersecurity threats and incidents to government agencies;
4. Communicating information about information blocking and other unlawful practices to government agencies; or
5. 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.
   * + - 1. 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.

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

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.

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—

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

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.

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

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;

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

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;

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

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

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.   1. 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:       1. 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.       2. 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.    1. A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section.    2. 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:**  Click here to enter comments on proposed § 170.403 Communications. |

## 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:**  Click here to enter comments on these key terms relevant to the API condition, as we propose to adopt them at § 170.102 Definitions. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on our proposed adoption of the API Resource Collection in Health implementation specification at § 170.215(a)(2). |

|  |
| --- |
| **§ 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.   1. 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). 2. Search support. Respond to search requests for data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4). 3. App registration. Enable an application to register with the technology’s “authorization server.” 4. 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). 5. Authentication and app authorization – 1st time connection. The first time an application connects to request data the technology:    1. 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).    2. 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. 6. Authentication and app authorization – Subsequent connections. Demonstrates that an application can access a single patient’s data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months. 7. Documentation. 8. 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:**  Click here to enter comments on proposed § 170.315(g)(10) Standardized API for patient and population services certification criterion, including the API standards and implementation specifications it references. |

### § 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).

1. 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.
      1. 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.
      2. Terms and conditions.
         1. 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.
         2. 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)

* + - * 1. 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.
      1. 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.
  1. Permitted fees conditions.
     1. General conditions.

1. All fees related to API technology not otherwise permitted by this section are prohibited from being imposed by an API Technology Supplier.
2. 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.
      1. 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.
      2. 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:
         1. 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;
         2. Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or
         3. Opportunity costs, except for the reasonable forward-looking cost of capital.
      3. 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)

* + 1. 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.

1. 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.
   1. Non-discrimination.
2. 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.
3. 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.
4. 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.
   3. Rights to access and use API technology.
      1. 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.
      2. 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)** |
| 1. Not compete with the API Technology Supplier in any product, service, or market. 2. Deal exclusively with the API Technology Supplier in any product, service, or market. 3. Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology. 4. 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.   1. 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.    1. 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.    2. 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. 2. 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:**  Click here to enter comments on proposed § 170.404 Application programming interfaces condition and maintenance of certification provisions. |

## Real World Testing

### § 170.405 Real world testing

* + - * 1. 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.
        2. Maintenance of Certification.

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.

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.

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

1. 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:
   1. 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;
   2. 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;
   3. 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.
   4. A schedule of key real world testing milestones;
   5. A description of the expected outcomes of real world testing;
   6. At least one measurement/metric associated with the real world testing; and
   7. A justification for the health IT developer’s real world testing approach.

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:

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

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

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

|  |
| --- |
| **§ 170.405 Real world testing** |
| 1. A list of the key milestones met during real world testing; 2. The outcomes of real world testing including a description of any challenges encountered during real world testing; and 3. At least one measurement/metric associated with the real world testing. 4. 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:   * 1. Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and   2. 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.  1. 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:   * 1. Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and   2. 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.  1. 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:    1. Provide advance notice to all affected customers and its ONC-ACB – 2. Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator; 3. 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; 4. 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:**  Click here to enter comments on proposed § 170.405 Real world testing provisions. |

|  |
| --- |
| **§ 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:    1. 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    2. 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:**  Click here to enter comments on revisions to § 170.555 Certification to newer versions of certain standards. |

## Attestations

|  |
| --- |
| **§ 170.406 Attestations** |
| 1. 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—       1. The usability of its health IT;       2. The interoperability of its health IT;       3. The security of its health IT;       4. Relevant information regarding users' experiences when using its health IT;       5. The business practices of developers of health IT related to exchanging electronic health information; and       6. The manner in which a user of the health IT has used such technology; and 2. 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; 3. 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.   1. 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:**  Click here to enter comments on proposed § 170.406 Attestations, including the appropriate frequency and timing of attestations. |

## 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) \* \* \*

* 1. Certified health IT causing or contributing to unsafe conditions. \* \* \*

\* \* \* \* \*

* 1. Impediments to ONC-ACB oversight of certified health IT. \* \* \*

\* \* \* \* \*

* 1. 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.

1. Coordination with the Office of Inspector General.
   1. 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.
   2. ONC may rely on Office of Inspector General findings to form the basis of a direct review action.

\* \* \* \* \*

1. 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.
2. 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) \* \* \*

1. All records related to the development, testing, certification, implementation, maintenance and use of its certified health IT;
2. Any complaint records related to the certified health IT;
3. All records related to the Condition(s) and Maintenance of Certification requirements, including marketing and distribution records, communications, and contracts; and
4. 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:

1. A determination is made that termination is appropriate after considering the information provided

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

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

1. 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
2. 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:
   1. 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.
   2. 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;
   3. The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;
   4. The health IT developer fails to timely submit in writing a proposed corrective action plan;
   5. 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;
   6. The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or
   7. 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:

* + - 1. ONC incorrectly applied ONC Health IT Certification Program requirements for a

1. Suspension;
2. Termination; or
3. Certification ban under § 170.581(a)(2); or

\* \* \* \* \*

* + 1. 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** |
| 1. Termination; 2. Suspension; or 3. Certification ban under § 170.581(a)(2). (3) \* \* \* 4. A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of:    1. Suspension;    2. Termination; or    3. Certification ban under § 170.581(a)(2).   \* \* \* \* \*   1. Effect of appeal.    1. 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.    2. A request for appeal does not stay the suspension of a Health IT Module.    3. 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:**  Click here to enter comments on proposed § 170.580 ONC review of certified health IT or a health IT developer’s actions. |

|  |
| --- |
| **§ 170.505 Correspondence** |
| 1. 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. 2. 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:**  Click here to enter comments on proposed revisions to § 170.505 Correspondence. |

**§ 170.581 Certification ban**

1. 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:
      1. Terminated by ONC under the ONC Health IT Certification Program;
      2. 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;
      3. 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;
      4. 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. 5. 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:       1. 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.       2. 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.       3. A final determination to issue a certification ban per § 170.580(g)(7) if a health IT developer files an appeal timely. 6. 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:**  Click here to enter comments on proposed modifications to § 170.581 Certification ban. |

## Section VIII – Information Blocking

|  |
| --- |
| **§ 171.100 Statutory basis and purpose** |
| 1. Basis. This part implements section 3022 of the Public Health Service Act, 42 U.S.C. 300jj-52. 2. 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:**  Click here to enter comments on § 171.100 Statutory basis and purpose. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on § 171.101 Applicability. |

|  |
| --- |
| **§ 171.103 Information blocking** |
| Information blocking means a practice that—   1. 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 2. 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 3. 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:**  Click here to enter comments on the definition of § 171.103 Information blocking. |

### § 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:**  Click here to enter comments on § 171.102 Definitions. |

|  |
| --- |
| **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:**  Click here to enter comments on the definition of health care provider in § 171.102 |

|  |
| --- |
| **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:**  Click here to enter comments on this request for comment regarding price information. |

|  |
| --- |
| **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:**  Click here to enter comments on in response to this request. |

|  |
| --- |
| **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:**  Click here to enter comments in response to this request. |

|  |
| --- |
| **§ 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:**  Click here to enter comments on § 171.200 Availability and effect of exceptions. |

## 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.   1. 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. 2. 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:**  Click here to enter comments on proposed § 171.201 Exception - Preventing harm. |

### § 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.

* 1. 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.

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

1. 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.
2. 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.
   1. 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—
         1. Conforms to the actor’s organizational policies and procedures that:
3. Are in writing;
4. 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
5. 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
   * + 1. 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
     1. If the precondition relies on the provision of consent or authorization from an individual, the actor:
        1. Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and
        2. Did not improperly encourage or induce the individual to not provide the consent or authorization.
     2. The actor’s practice is—
        1. Tailored to the specific privacy risk or interest being addressed; and
        2. 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. 6. 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). 7. 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:**  Click here to enter comments on proposed § 171.202 Exception - Promoting the privacy of electronic health information. |

|  |
| --- |
| **§ 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.   1. The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information. 2. The practice must be tailored to the specific security risk being addressed. 3. The practice must be implemented in a consistent and non-discriminatory manner. 4. 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. 5. 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:**  Click here to enter comments on proposed § 171.203 Exception - Promoting the security of electronic health information. |

### § 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.

1. 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.
2. 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.
3. 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.

1. 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:**  Click here to enter comments on proposed § 171.204 Exception - Recovering costs reasonably incurred. |

### § 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.

1. 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—
      1. The type of electronic health information and the purposes for which it may be needed;
      2. The cost to the actor of complying with the request in the manner requested;
      3. The financial, technical, and other resources available to the actor;
      4. 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;
      5. 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;
      6. 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;
      7. 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.   1. 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.    1. Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.    2. Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee. 2. Responding to requests. The actor 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. 3. Written explanation. The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request. 4. Provision of a reasonable alternative. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information. |
| **Preamble FR Citation:** 84 FR 7542-44 **Specific questions in preamble?** *Yes* |
| **Regulatory Impact Analysis:** Not applicable |
| **Public Comment Field:**  Click here to enter comments on proposed § 171.205 Exception - Responding to requests that are infeasible. |

**§ 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.

1. 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.
   1. 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.
   2. Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.
   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.
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.
   1. The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.
   2. 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.
   3. 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.
   1. 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.
   2. The terms must not be based in any part on—
      1. 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
      2. 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.
   1. Not compete with the actor in any product, service, or market.
   2. Deal exclusively with the actor in any product, service, or market.
   3. 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** |
| 1. License, grant, assign, or transfer to the actor any intellectual property of the licensee. 2. 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. 3. 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—    1. The agreement states with particularity all information the actor claims as trade secrets; and    2. Such information meets the definition of a trade secret under applicable law. 4. 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:**  Click here to enter comments on proposed § 171.206 Exception - Licensing of interoperability elements on reasonable and non-discriminatory terms. |

|  |
| --- |
| **§ 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.   1. Maintenance and improvements to health IT. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, 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. 2. Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor 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. 3. Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to 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:**  Click here to enter comments on proposed § 171.207 Exception – Maintaining and improving health IT performance |

|  |
| --- |
| **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:**  **C**lick here to enter input in response to the request for more information regarding a potential additional exception to the information blocking definition for complying with the Common Agreement for Trusted Exchange to be considered for inclusion in future rulemaking. |

|  |
| --- |
| **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:**  Click here to enter input in response to the request for more information regarding potential new exceptions to the information blocking definition. |

## 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:**  Click here to enter input in response to the request for comment on the information blocking complaint process. |

* 1. ***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:**  Click here to enter input in response to the request for more information on disincentives for health care providers with respect to information blocking. |

***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:**  Click here to enter input in response to the request for more information regarding registries. |

***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:**  Click here to enter input in response to the request for more information regarding patient matching. |

***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:**  Click here to enter input on collection of information requirements. |

**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:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 1 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 1 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 1 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 1 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Supplemental Children’s EHR Format Requirements for Recommendation 1** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments about the relevance of the potential supplemental Children’s EHR Format requirements 1-3 and their correlation to recommendation 1. |

|  |
| --- |
| **Recommendation 2: Compute weigh-based drug dosage** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 2 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 2 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 2 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 2 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Supplemental Children’s EHR Format Requirements for Recommendation 2** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments about the relevance of the potential Children’s EHR Format requirements 1-2 and their correlation to recommendation 2. |

|  |
| --- |
| **Recommendation 3: Ability to document all guardians and caregivers** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 3 in practice. |

|  |
| --- |
| **Recommendation 3: Ability to document all guardians and caregivers** |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 3 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 3 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 3 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Supplemental Children’s EHR Format Requirements for Recommendation 3** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments about the relevance of the potential supplemental Children’s EHR Format requirements 1-4 and their correlation to recommendation 3. |

|  |
| --- |
| **Recommendation 4: Segmented access to information** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 4 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 4 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 4 for voluntary certification of health IT for pediatric care. |

**Recommendation 4: Segmented access to information**

**Public Comment Field:**

Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 4 should be removed as a correlated item to support any of this recommendation.

|  |
| --- |
| **Supplemental Children’s EHR Format Requirement for Recommendation 4** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments about the relevance of this potential supplemental Children’s EHR Format requirement and its correlation to recommendation 4. |

|  |
| --- |
| **Recommendation 5: Synchronize immunization histories with registries** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 5 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 5 as it involves provider training, establishing workflow, and other related safety and usability considerations.. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 5 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 5 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Supplemental Children’s EHR Format Requirement for Recommendation 5** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments about the relevance of this potential Children’s EHR Format requirement and its correlation to recommendation 5. |

|  |
| --- |
| **Recommendation 6: Age- and weight-specific single-dose range checking** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 6 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 6 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 6 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 6 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Recommendation 7: Transferrable access authority** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 7 in practice. |
| **Public Comment Field:** |

|  |
| --- |
| **Recommendation 7: Transferrable access authority** |
| Click here to enter comments on how the effective use of IT can support recommendation 7 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 7 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 7 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Supplemental Children’s EHR Format Requirement for Recommendation 7** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments about the relevance of this potential Children’s EHR Format requirement and its correlation to recommendation 7. |

|  |
| --- |
| **Recommendation 8: Associate maternal health information and demographics with newborn** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 8 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 8 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 8 for voluntary certification of health IT for pediatric care. |

|  |
| --- |
| **Recommendation 8: Associate maternal health information and demographics with newborn** |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 8 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Recommendation 9: Track incomplete preventative care opportunities** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 9 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 9 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 9 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 9 should be removed as a correlated item to support any of this recommendation. |

|  |
| --- |
| **Recommendation 10: Flag special health care needs** |
| See Pediatric Technical Worksheets at 84 FR 7605. |
| **Public Comment Field:**  Click here to enter comments on relevant gaps, barriers, safety concerns, and/or resources (including available best practices, activities, and tools) that may impact or support feasibility of recommendation 10 in practice. |
| **Public Comment Field:**  Click here to enter comments on how the effective use of IT can support recommendation 10 as it involves provider training, establishing workflow, and other related safety and usability considerations. |
| **Public Comment Field:**  Click here to enter comments regarding the inclusion (or removal) of recommendation 10 for voluntary certification of health IT for pediatric care. |
| **Public Comment Field:**  Click here to enter comments on whether any of the functional criteria listed under the “Alignment with 2015 Edition Certification Criteria” and the “Alignment with Proposed New or Updated Certification” for recommendation 10 should be removed as a correlated item to support any of this recommendation. |