manner prescribed by HHS, documenting specific implementation and oversight activities performed during the quarter, including progress in implementing the State's approved Medicaid HIT plan.

(b) The quarterly progress reports must include, but need not be limited to providing, updates on the following:

(1) State system implementation dates.

(2) Provider outreach.

(3) Auditing.

(4) State-specific State Medicaid HIT Plan tasks.

(5) State staffing levels and changes.

(6) The number and type of providers that qualified for an incentive payment on the basis of having adopted, implemented or upgraded certified EHR technology and the amounts of incentive payments.

(7) The number and type of providers that qualified for an incentive payment on the basis of having demonstrated that they are meaningful users of certified EHR technology and the amounts of incentive payments.

Dated: March 10, 2015.

Andrew M. Slavitt,

Acting Administrator, Centers for Medicare & Medicaid Services.

Approved: March 18, 2015.

Sylvia M. Burwell,

Secretary, Department of Health and Human Services.

[FR Doc. 2015–06685 Filed 3–20–15; 3:00 pm]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 170

RIN 0991–AB93

2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Notice of proposed rulemaking with comment period.

SUMMARY: This notice of proposed rulemaking introduces a new edition of certification criteria (the 2015 Edition health IT certification criteria or ''2015 Edition''), proposes a new 2015 Edition Base EHR definition, and proposes to modify the ONC Health IT Certification Program to make it open and accessible to more types of health IT and health IT that supports various care and practice settings. The 2015 Edition would also establish the capabilities and specify the related standards and implementation specifications that Certified Electronic Health Record (EHR) Technology (CEHRT) would need to include to, at a minimum, support the achievement of meaningful use by eligible professionals (EPs), eligible hospitals, and critical access hospitals (CAHs) under the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) when such edition is required for use under these programs.

DATES: To be assured consideration, written or electronic comments must be received at one of the addresses provided below, no later than 5 p.m. on May 29, 2015.

ADDRESSES: You may submit comments, identified by RIN 0991–AB93, by any of the following methods (please do not submit duplicate comments). Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

- *Federal eRulemaking Portal:* Follow the instructions for submitting comments. Attachments should be in Microsoft Word, Microsoft Excel, or Adobe PDF; however, we prefer Microsoft Word. *http://www.regulations.gov.*
- *Regular, Express, or Overnight Mail:* Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Attention: 2015 Edition Health IT Certification Criteria Proposed Rule, Hubert H. Humphrey Building, Suite 729D, 200 Independence Ave SW., Washington, DC 20201. Please submit one original and two copies.
- *Hand Delivery or Courier:* Office of the National Coordinator for Health Information Technology, Attention: 2015 Edition Health IT Certification Criteria Proposed Rule, Hubert H. Humphrey Building, Suite 729D, 200 Independence Ave SW., Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Enhancing the Public Comment Experience: To facilitate public comment on this proposed rule, a copy will be made available in Microsoft Word format. We believe this version will make it easier for commenters to access and copy portions of the proposed rule for use in their individual comments. Additionally, a separate document will be made available for the public to use to provide comments on the proposed rule. This document is meant to provide the public with a simple and organized way to submit comments on the certification criteria, associated standards and implementation specifications, and respond to specific questions posed in the preamble of the proposed rule. While use of this document is entirely voluntary, we encourage commenters to consider using the document in lieu of unstructured comments or to use it as an addendum to narrative cover pages. Roughly 30% of the public comments submitted to our past two editions of certification criteria proposed rules used the provided template, which greatly assisted in our ability to rapidly process and more accurately categorize public comments. Because of the technical nature of this proposed rule, we believe that use of the document may facilitate our review and understanding of the comments received. The Microsoft Word version of the proposed rule and the document that can be used for providing comments can be found at *http://www.regulations.gov* as part of this proposed rule's docket and on ONC's Web site (*http://www.healthit.gov*).

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. Please do not include anything in your comment submission that you do not wish to share with the general public. Such information includes, but is not limited to: a person's social security number; date of birth; driver's license number; state identification number or foreign country equivalent; passport number; financial account number; credit or debit card number; any personal health information; or any business information that could be considered proprietary. We will post all comments that are received before the close of the comment period at *http://www.regulations.gov.*

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Hubert H. Humphrey Building, Suite 729D, 200 Independence Ave SW., Washington, DC 20201 (call ahead to the contact listed below to arrange for inspection).

FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Commonly Used Acronyms

API	Application Programming Interface
CAH	Critical Access Hospital
CDA	Clinical Document Architecture
CDC	Centers for Disease Control and Prevention
CDS	Clinical Decision Support
CEHRT	Certified Electronic Health Record Technology
CFR	Code of Federal Regulations
CHPL	Certified Health IT Product List
CLIA	Clinical Laboratory Improvement Amendments
CMS	Centers for Medicare & Medicaid Services
CQM	Clinical Quality Measure
EHR	Electronic Health Record
HHS	Department of Health and Human Services
HISP	Health Information Service Providers
HIT	Health Information Technology
HITPC	HIT Policy Committee
HITSC	HIT Standards Committee
HL7	Health Level Seven
IG	Implementation Guide
LOINC®	Logical Observation Identifiers Names and Codes
ONC	Office of the National Coordinator for Health Information Technology
SNOMED CT®	Systematized Nomenclature of Medicine Clinical Terms

Table of Contents

I. Executive Summary
A. Purpose of Regulatory Action
B. Summary of Major Provisions
1. Overview of the 2015 Edition Health IT Certification Criteria
2. Base EHR Definition and Certified EHR Technology Definition
3. The ONC Health IT Certification Program and Health IT Module
C. Costs and Benefits
II. Background
A. Statutory Basis
1. Standards, Implementation Specifications, and Certification Criteria
2. HIT Certification Programs
B. Regulatory History
1. Standards, Implementation Specifications, and Certification Criteria Rules
2. Medicare and Medicaid EHR Incentive Programs Rules
3. ONC Health IT Certification Programs Rules
III. Provisions of the Proposed Rule Affecting Standards, Implementation Specifications, Certification Criteria, and Definitions
A. 2015 Edition Health IT Certification Criteria
1. Applicability
2. Standards and Implementation Specifications
3. Certification Criteria
4. 2015 Edition Gap Certification Eligibility Table
5. Pharmacogenomics Data—Request for Comment
B. Definitions
1. Base EHR Definitions
2. Certified EHR Technology Definition
3. Common Clinical Data Set Definition
4. Cross-Referenced FDA Definitions
IV. Provisions of the Proposed Rule Affecting the ONC Health IT Certification Program
A. Subpart E—ONC Health IT Certification Program
B. Modifications to the ONC Health IT Certification Program
1. Health IT Modules
2. ''Removal'' of Meaningful Use Measurement Certification Requirements
3. Types of Care and Practice Settings
4. Referencing the ONC Health IT Certification Program
C. Health IT Module Certification Requirements
1. Privacy and Security
2. Design and Performance (§ 170.315(g))
D. Principles of Proper Conduct for ONC–ACBs
1. ''In-the-Field'' Surveillance and Maintenance of Certification
2. Transparency and Disclosure Requirements
3. Open Data Certified Health IT Product List (CHPL)
4. Records Retention
5. Complaints Reporting
6. Adaptations and Updates of Certified Health IT
E. ''Decertification'' of Health IT—Request for Comment
V. Response to Comments
VI. Incorporation by Reference
VII. Collection of Information Requirements
VIII. Regulatory Impact Statement
A. Statement of Need
B. Overall Impact
1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis
2. Regulatory Flexibility Act
3. Executive Order 13132—Federalism
4. Unfunded Mandates Reform Act of 1995

I. Executive Summary

A. Purpose of Regulatory Action

Building on past rulemakings, this proposed rule further identifies how health IT certification can support the establishment of an interoperable nationwide health information infrastructure. It reflects stakeholder feedback received through various outreach initiatives, including the regulatory process, and is designed to broadly support the health care continuum through the use of certified health IT. To achieve this goal, this rule proposes to:

- Improve interoperability for specific purposes by adopting new and updated vocabulary and content standards for the structured recording and exchange of health information, including a Common Clinical Data Set composed primarily of data expressed using adopted standards; and rigorously testing an identified content exchange standard (Consolidated Clinical Document Architecture (C–CDA));
- Facilitate the accessibility and exchange of data by including enhanced data portability, transitions of care, and application programming interface (API) capabilities in the 2015 Edition Base EHR definition;
- Establish a framework that makes the ONC Health IT Certification Program open and accessible to more types of health IT, health IT that supports a variety of care and practice settings, various HHS programs, and public and private interests;
- Support the Medicare and Medicaid EHR Incentive Programs (EHR Incentive Programs) through the adoption of a set of certification criteria that align with proposals for Stage 3;
- Address health disparities by providing certification: To standards for the collection of social, psychological, and behavioral data; for the exchange of sensitive health information (Data Segmentation for Privacy); and for the accessibility of health IT;
- Ensure all health IT presented for certification possess the relevant privacy and security capabilities;
- Improve patient safety by: Applying enhanced user-center design principles to health IT, enhancing patient matching, requiring relevant patient information to be exchanged (*e.g.,* Unique Device Identifiers), improving the surveillance of certified health IT, and making more information about certified products publicly available and accessible;
- Increase the reliability and transparency of certified health IT through surveillance and disclosure requirements; and
- Provide health IT developers with more flexibility and *opportunities* for certification that support both interoperability and innovation.

B. Summary of Major Provisions

1. Overview of the 2015 Edition Health IT Certification Criteria

The 2015 Edition health IT certification criteria (''2015 Edition'') would facilitate greater interoperability for several clinical health information purposes and enable health information exchange through new and enhanced certification criteria, standards, and implementation specifications. It incorporates changes that are designed to spur innovation, open new market opportunities, and provide more choices to providers when it comes to electronic health information exchange. To achieve these goals, we propose a new ''Application Access to Common Clinical Data Set'' certification criterion that would require the demonstration of an API that responds to data requests for any one of the data referenced in the Common Clinical Data Set as well as for all of the data referenced in the Common Clinical Data Set. To further validate the continued interoperability of certified health IT and the ability to exchange health information, we propose a new certification criterion that would rigorously assess a product's C–CDA creation performance (for both C–CDA version 1.1 and 2.0) when presented for certification for such capabilities.

2. Definitions

a. Base EHR Definitions

We propose to adopt a Base EHR definition specific to the 2015 Edition (*i.e.,* a 2015 Edition Base EHR definition) at § 170.102 and rename the current Base EHR definition at § 170.102 as the 2014 Edition Base EHR definition. For the proposed 2015 Edition Base EHR definition, it would differ from the 2014 Edition Base EHR definition in the following ways:

- It does not include privacy and security capabilities and certification criteria. We believe privacy and security capabilities would be more appropriately addressed through our new proposed approach for the privacy and security certification of Health IT Modules to the 2015 Edition, as discussed under ''Privacy and Security'' in section IV.C.1 of the preamble. Our new privacy and security approach would eliminate eligible professionals (EPs)', eligible hospitals', and critical access hospitals (CAHs)' responsibilities to ensure that they have technology certified to all the necessary privacy and security criteria. Rather, as part of certification, health IT developers would need to meet applicable privacy and security certification criteria.
- It only includes the capability to record and export CQM data (§ 170.315(c)(1)). To note, the capabilities to import, calculate and report CQM data are not included in the proposed 2015 Edition Base EHR definition or any other CQM-related requirements. Please refer to the ''Clinical Quality Measures'' section (III.A.3) later in the preamble for a more detailed discussion of the CQM certification criteria. Please also see the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register** for proposals related to CQMs, including the CEHRT definition proposal.
- It includes the 2015 Edition ''smoking status,'' ''implantable device list,'' and ''application access to Common Clinical Data Set'' certification criteria. For a detailed discussion of these certification criteria, please refer to section III.A.3 of the preamble.
- It includes the proposed 2015 Edition certification criteria that correspond to the remaining 2014 Edition certification criteria referenced in the ''2014 Edition'' Base EHR definition (*i.e.,* Computerized Provider Order Entry (CPOE), demographics, problem list, medication list, medication allergy list, clinical decision support (CDS), transitions of care, data portability, and relevant transport certification criteria). On the inclusion of transport certification criteria, we propose to include the ''Direct Project'' criterion (§ 170.315(h)(1)) as well as the ''Direct Project, Edge Protocol and XDR/XDM''[1] criterion (§ 170.315(h)(2)) as equivalent alternative means for meeting the 2015 Edition Base EHR definition for the reasons discussed under ''Transport Methods and Other Protocols'' in section III.A.3 of the preamble.

We refer readers to section III.B.1 for a more detailed discussion of the proposed 2015 Edition Base EHR definition.

b. CEHRT Definition

We propose to remove the Certified EHR Technology (CEHRT) definition from § 170.102 for the following reasons. The CEHRT definition has always been defined in a manner that supports the EHR Incentive Programs. As such, the CEHRT definition would more appropriately reside solely within the EHR Incentive Programs regulations. This would also be consistent with our approach in this proposed rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. Further, this approach should add administrative simplicity in that regulatory provisions, which EHR Incentive Programs participants must meet (*e.g.,* the CEHRT definition), would be defined within the context of rulemakings for those programs. We understand that the CEHRT definition proposed by CMS would continue to include the Base EHR definition(s) defined by ONC, including the 2015 Edition Base EHR definition proposed in this proposed rule. We also refer readers to Table 2 (''2015 Edition Proposed Certification Criteria Associated with the EHR Incentive Programs Stage 3'') found in section III.A.3 of this preamble. Table 2 crosswalks proposed 2015 Edition certification criteria with the proposed CEHRT definition and proposed EHR Incentive Programs Stage 3 objectives.

c. Common Clinical Data Set

We propose to revise the ''Common MU Data Set'' definition in § 170.102. We propose to change the name to ''Common Clinical Data Set,'' which aligns with our approach throughout this proposed rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. We also propose to change references to the ''Common MU Data Set'' in the 2014 Edition (§ 170.314) to ''Common Clinical Data Set.''

We propose to revise the definition to account for the new and updated standards and code sets we propose to adopt in this proposed rule that would improve and advance interoperability through the exchange of the Common Clinical Data Set. We also propose to revise the definition to support patient safety through clearly referenced data elements and the inclusion of new patient data. These proposed revisions would *not* change the standards, codes sets, and data requirements specified in the Common Clinical Data Set for 2014 Edition certification. They would only apply to health IT certified to the 2015 Edition Health IT certification criteria that reference the Common Clinical Data Set.

3. The ONC Health IT Certification Program and Health IT Module

We propose to change the name of the ONC HIT Certification Program to the ''ONC Health IT Certification Program'' (referred to as the ''ONC Health IT Certification Program'' throughout this proposed rule). We also propose to modify the ONC Health IT Certification Program in ways that would further open access to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond the ambulatory and inpatient settings. These modifications would also serve to support other public and private programs that may reference the use of health IT certified under the ONC Health IT Certification Program. When we established the certification

[1] XDR stands for Cross-Enterprise Document Reliable Interchange. XDM stands for Cross-Enterprise Document Media Interchange.

program (76 FR 1294), we stated our initial focus would be on EHR technology and supporting the EHR Incentive Programs, which focus on the ambulatory setting and inpatient setting. Our proposals in this proposed rule would permit other types of health IT (*e.g.,* laboratory information systems (LISs)), and technology implemented by health information service providers (HISPs) and health information exchanges (HIEs)) to receive appropriate attribution and not be referenced by a certificate with ''EHR'' in it. Our proposals also support health IT certification for other care and practice settings such as long-term post-acute care (LTPAC), behavioral health, and pediatrics. Further, the proposals in this rule would make it simpler for certification criteria and certified health IT to be referenced by other HHS programs (*e.g.,* Medicaid and Medicare payment programs and various grant programs), other public programs, and private entities and associations.

As part of our approach to evolve the ONC Health IT Certification Program, we have replaced prior rulemaking use of ''EHR'' and ''EHR technology'' with ''health IT.'' The term health IT is reflective of the scope of ONC's authority under the Public Health Service Act (§ 3000(5) as ''health information technology'' is so defined), and represents a broad range of technology, including EHR technology. It also more properly represents some of the technology, as noted above, that has been previously certified to editions of certification criteria under the ONC Health IT Certification Program and may be certified to the proposed 2015 Edition in the future. Similarly, to make the ONC Health IT Certification Program more open and accessible, we propose to rename the EHR Module as ''Health IT Module'' and will use this term throughout the proposed rule.

We propose *not* to require ONC-Authorized Certification Bodies (ACBs) to certify all Health IT Modules to the 2015 Edition ''meaningful use measurement'' certification criteria (§ 170.315(g)(1) ''automated numerator recording'' and § 170.315(g)(2) ''automated measure calculation''). We note that *CMS has proposed* to include the 2015 Edition ''meaningful use measurement'' certification criteria in the CEHRT definition as a unique program requirement for the EHR Incentive Programs.

We propose a new, simpler, straight-forward approach to privacy and security certification requirements for Health IT Modules certified to the 2015 Edition. In essence, we identify the privacy and security certification criteria that would be applicable to a Health IT Module presented for certification based on the other capabilities included in the Health IT Module and for which certification is sought. Under the proposed approach, a health IT developer would know exactly what it needed to do in order to get its Health IT Module certified and a purchaser of a Health IT Module would know exactly what privacy and security functionality against which the Health IT Module had to be tested in order to be certified.

We propose new and revised principles of proper conduct (PoPC) for ONC–ACBs. We propose to require ONC–ACBs to report an expanded set of information to ONC for inclusion in the open data file that would make up the Certified Health IT Product List (CHPL). We propose to revise the PoPC in order to provide for more meaningful disclosure of certain types of costs and limitations that could interfere with the ability of users to implement certified health IT in a manner consistent with its certification. We propose that ONC–ACBs retain records longer and consistent with industry standards. We propose to require that ONC–ACBs obtain a record of all adaptations and updates, including changes to user-facing aspects, made to certified health IT, on a monthly basis each calendar year. We propose to require that ONC–ACBs report to the National Coordinator complaints received on certified health IT. We propose to adopt new requirements for ''in-the-field'' surveillance under the ONC Health IT Certification Program that would build on ONC–ACBs' existing surveillance responsibilities by specifying requirements and procedures for in-the-field surveillance. We believe these proposed new and revised PoPC would promote greater transparency and accountability for the ONC Health IT Certification Program. We also include a request for comment on the potential ''decertification'' of health IT that proactively blocks the sharing of information.

C. Costs and Benefits

Our estimates indicate that this proposed rule is an economically significant rule as its overall costs for health IT developers may be greater than $100 million in at least one year. We have, therefore, projected the costs and benefits of the proposed rule. The estimated costs expected to be incurred by health IT developers to develop and prepare health IT to be tested and certified in accordance with the 2015 Edition health IT certification criteria (and the standards and implementation specifications they include) are represented in monetary terms in Table 1 below. We note that this proposed rule does not impose the costs cited as compliance costs, but rather as investments which health IT developers voluntarily take on and expect to recover with an appropriate rate of return.

The dollar amounts expressed in Table 1 are expressed in 2013 dollars.

TABLE 1—DISTRIBUTED TOTAL DEVELOPMENT AND PREPARATION COSTS FOR HEALTH IT DEVELOPERS (4-YEAR PERIOD)—TOTALS ROUNDED

Year	Ratio (%)	Total low cost estimate ($M)	Total high cost estimate ($M)	Total average cost estimate ($M)
2015	25	49.36	101.80	75.58
2016	30	59.23	122.16	90.70
2017	30	59.23	122.16	90.70
2018	15	29.61	61.08	45.35
4-Year Totals		197.43	407.20	302.32

We believe that there will be several significant benefits that may arise from this proposed rule for patients, health care providers, and health IT developers. The 2015 Edition continues to improve health IT interoperability through the adoption of new and updated standards and implementation specifications. For example, many proposed certification criteria include standards and implementation specifications for interoperability that directly support the EHR Incentive Programs, which include objectives and measures for the interoperable exchange of health information and for providing patients electronic access to their health information in structured formats. In addition, proposed certification criteria that support the collection of patient data that could be used to address health disparities would not only benefit patients, but the entire health care delivery system through improved quality of care. The 2015 Edition also supports usability and patient safety through new and enhanced certification requirements for health IT.

Our proposals to make the ONC Health IT Certification Program open and accessible to more types of health IT and for health IT that supports a variety of care and practice settings should benefit health IT developers, providers practicing in other care/practice settings, and consumers through the availability and use of certified health IT that includes capabilities that promote interoperability and enhanced functionality.

II. Background

A. Statutory Basis

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the Recovery Act) (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created ''Title XXX—Health Information Technology and Quality'' (Title XXX) to improve health care quality, safety, and efficiency through the promotion of HIT and electronic health information exchange.

1. Standards, Implementation Specifications, and Certification Criteria

The HITECH Act established two new federal advisory committees, the Health IT Policy Committee (HITPC) and the Health IT Standards Committee (HITSC) (sections 3002 and 3003 of the PHSA, respectively). Each is responsible for advising the National Coordinator for Health Information Technology (National Coordinator) on different aspects of standards, implementation specifications, and certification criteria. The HITPC is responsible for, among other duties, recommending priorities for the development, harmonization, and recognition of standards, implementation specifications, and certification criteria. Main responsibilities of the HITSC include recommending standards, implementation specifications, and certification criteria for adoption by the Secretary under section 3004 of the PHSA, consistent with the ONC-coordinated Federal Health IT Strategic Plan.

Section 3004 of the PHSA identifies a process for the adoption of health IT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria. As specified in section 3004(a)(1), the Secretary is required, in consultation with representatives of other relevant federal agencies, to jointly review standards, implementation specifications, and certification criteria endorsed by the National Coordinator under section 3001(c) and subsequently determine whether to propose the adoption of any grouping of such standards, implementation specifications, or certification criteria. The Secretary is required to publish all determinations in the **Federal Register**.

Section 3004(b)(3) of the PHSA titled, Subsequent Standards Activity, provides that the Secretary shall adopt additional standards, implementation specifications, and certification criteria as necessary and consistent with the schedule published by the HITSC. We consider this provision in the broader context of the HITECH Act to grant the Secretary the authority and discretion to adopt standards, implementation specifications, and certification criteria that have been recommended by the HITSC and endorsed by the National Coordinator, as well as other appropriate and necessary health IT standards, implementation specifications, and certification criteria. Throughout this process, the Secretary intends to continue to seek the insights and recommendations of the HITSC.

2. Health IT Certification Programs

Section 3001(c)(5) of the PHSA provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health IT. Specifically, section 3001(c)(5)(A) specifies that the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology, shall keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria adopted under this subtitle (*i.e.,* certification criteria adopted by the Secretary under section 3004 of the PHSA).

The certification program(s) must also include, as appropriate, testing of the technology in accordance with section 13201(b) of the [HITECH] Act. Overall, section 13201(b) of the HITECH Act requires that with respect to the development of standards and implementation specifications, the Director of the National Institute of Standards and Technology (NIST), in coordination with the HITSC, shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. The HITECH Act also indicates that the development of this conformance testing infrastructure may include a program to accredit independent, non-Federal laboratories to perform testing.

B. Regulatory History

1. Standards, Implementation Specifications, and Certification Criteria Rules

The Secretary issued an interim final rule with request for comments titled, ''Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology'' (75 FR 2014, Jan. 13, 2010) (the ''S&CC January 2010 interim final rule''), which adopted an initial set of standards, implementation specifications, and certification criteria. After consideration of the public comments received on the S&CC January 2010 interim final rule, a final rule was issued to complete the adoption of the initial set of standards, implementation specifications, and certification criteria and realign them with the final objectives and measures established for the EHR Incentive Programs Stage 1 (formally titled: Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule, (75 FR 44590, July 28, 2010) and referred to as the ''2011 Edition final rule''). The 2011 Edition final rule also established the first version of the Certified EHR Technology (CEHRT) definition. Subsequent to the 2011 Edition final rule (October 13, 2010), we issued an interim final rule with a request for comment to remove certain implementation specifications related to public health surveillance that had been previously adopted in the 2011 Edition final rule (75 FR 62686).

The standards, implementation specifications, and certification criteria adopted by the Secretary in the 2011 Edition final rule established the capabilities that CEHRT must include in order to, at a minimum, support the achievement of EHR Incentive Programs Stage 1 by EPs, eligible hospitals, and CAHs under the EHR Incentive Programs Stage 1 final rule (the ''EHR Incentive Programs Stage 1 final rule'') (see 75 FR 44314 for more information about meaningful use and the Stage 1 requirements).

The Secretary issued a proposed rule with request for comments titled ''Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology'' (77 FR 13832, March 7, 2012) (the ''2014 Edition proposed rule''), which proposed new and revised standards, implementation specifications, and certification criteria. After consideration of the public comments received on the 2014 Edition proposed rule, a final rule was issued to adopt the 2014 Edition set of standards, implementation specifications, and certification criteria and realign them with the final objectives and measures established for the EHR Incentive Programs Stage 2 as well as Stage 1 revisions (Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology (77 FR 54163, Sept. 4, 2012) (the ''2014 Edition final rule''). The standards, implementation specifications, and certification criteria adopted by the Secretary in the 2014 Edition final rule established the capabilities that CEHRT must include in order to, at a minimum, support the achievement of the EHR Incentive Programs Stage 2 by EPs, eligible hospitals, and CAHs under the EHR Incentive Programs Stage 2 final rule (the ''EHR Incentive Programs Stage 2 final rule'') (see 77 FR 53968 for more information about the EHR Incentive Programs Stage 2 requirements).

On December 7, 2012, an interim final rule with a request for comment was jointly issued and published by ONC and CMS to update certain standards that had been previously adopted in the 2014 Edition final rule. The interim final rule also revised the EHR Incentive Programs by adding an alternative measure for the Stage 2 objective for hospitals to provide structured electronic laboratory results to ambulatory providers, corrected the regulation text for the measures associated with the objective for hospitals to provide patients the ability to view online, download, and transmit information about a hospital admission, and made the case number threshold exemption policy for clinical quality measure (CQM) reporting applicable for eligible hospitals and CAHs beginning with FY 2013. The rule also provided notice of CMS's intent to issue technical corrections to the electronic specifications for CQMs released on October 25, 2012 (77 FR 72985). On September 4, 2014, a final rule (Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program for 2014 and Other Changes to the EHR Incentive Program; and Health Information Technology: Revisions to the Certified EHR Technology Definition and EHR Certification Changes Related to Standards; Final Rule) (79 FR 52910) was published adopting these proposals.

On November 4, 2013, the Secretary published an interim final rule with a request for comment, 2014 Edition Electronic Health Record Certification Criteria: Revision to the Definition of ''Common Meaningful Use (MU) Data Set'' (78 FR 65884), to make a minor revision to the Common MU Data Set definition. This revision was intended to allow more flexibility with respect to the representation of dental procedures data for EHR technology testing and certification.

On February 26, 2014, the Secretary published a proposed rule titled ''Voluntary 2015 Edition Electronic Health Record (EHR) Certification Criteria; Interoperability Updates and Regulatory Improvements'' (79 FR 10880) (''Voluntary Edition proposed rule''). The proposed rule proposed a voluntary edition of certification criteria that was designed to enhance interoperability, promote innovation, and incorporate ''bug fixes'' to improve upon the 2014 Edition. A correction notice was published for the Voluntary Edition proposed rule on March 19, 2014, entitled ''Voluntary 2015 Edition Electronic Health Record (EHR) Certification Criteria; Interoperability Updates and Regulatory Improvements; Correction'' (79 FR 15282). This correction notice corrected the preamble text and gap certification table for four certification criteria that were omitted from the list of certification criteria eligible for gap certification for the 2015 Edition EHR certification criteria. On September 11, 2014, a final rule was published titled ''2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange'' (79 FR 54430) (''2014 Edition Release 2 final rule''). The final rule adopted a small subset of the original proposals in the Voluntary Edition proposed rule as optional and revised 2014 Edition EHR certification criteria that provide flexibility, clarity, and enhance health information exchange. It also finalized administrative proposals (*i.e.,* removal of regulatory text from the Code of Federal Regulations (CFR)) and proposals for the ONC HIT Certification Program that provide improvements.

On May 23, 2014, CMS and ONC jointly published the ''Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record Incentive Programs for 2014; and Health Information Technology: Revisions to the Certified EHR Technology Definition'' proposed rule (79 FR 29732). The rule proposed to update the EHR Incentive Programs Stage 2 and Stage 3 participation timeline. It proposed to revise the CEHRT definition to permit the use of EHR technology certified to the 2011 Edition to meet the CEHRT definition for FY/CY 2014. It also proposed to allow EPs, eligible hospitals, and CAHs that could not fully implement EHR technology certified to the 2014 Edition for an EHR reporting period in 2014 due to delays in the availability of such technology to continue to use EHR technology certified to the 2011 Edition or a combination of EHR technology certified to the 2011 Edition and 2014 Edition for the EHR reporting periods in CY 2014 and FY 2014. On September 4, 2014, a final rule (''CEHRT Flexibility final rule'') was published (79 FR 52910) adopting these proposals.

2. Medicare and Medicaid EHR Incentive Programs Rules

On January 13, 2010, CMS published the EHR Incentive Programs Stage 1 proposed rule (75 FR 1844). The rule proposed the criteria for Stage 1 of the EHR Incentive Programs and regulations associated with the incentive payments made available under Division B, Title IV of the HITECH Act. Subsequently, CMS published a final rule (75 FR 44314) for Stage 1 and the EHR Incentive Programs on July 28, 2010, simultaneously with the publication of the 2011 Edition final rule. The EHR Incentive Programs Stage 1 final rule established the objectives, associated measures, and other requirements that EPs, eligible hospitals, and CAHs must satisfy to meet Stage 1.

On March 7, 2012, CMS published the EHR Incentive Programs Stage 2 proposed rule (77 FR 13698). Subsequently, CMS published a final rule (77 FR 53968) for the EHR Incentive Programs on Sept. 4, 2012, simultaneously with the publication of the 2014 Edition final rule. The EHR Incentive Programs Stage 2 final rule established the objectives, associated measures, and other requirements that EPs, eligible hospitals, and CAHs must satisfy to meet Stage 2 as well as revised some Stage 1 requirements.

As described above in Section II.B.1, ONC and CMS jointly issued an interim final rule with a request for comment that was published on December 7, 2012 and a final rule that published on September 4, 2014. Also, as described above in Section II.B.1, ONC and CMS jointly issued proposed and final rules that were published on May 23, 2014 and September 4, 2014, respectively.

3. ONC Health IT Certification Program Rules

On March 10, 2010, ONC published a proposed rule (75 FR 11328) titled, ''Proposed Establishment of Certification Programs for Health Information Technology'' (the ''Certification Programs proposed rule''). The rule proposed both a temporary and permanent certification program for the purposes of testing and certifying HIT. It also specified the processes the National Coordinator would follow to authorize organizations to perform the certification of HIT. A final rule establishing the temporary certification program was published on June 24, 2010 (75 FR 36158) (''Temporary Certification Program final rule'') and a final rule establishing the permanent certification program was published on January 7, 2011 (76 FR 1262) (''the Permanent Certification Program final rule'').

On May 31, 2011, ONC published a proposed rule (76 FR 31272) titled ''Permanent Certification Program for Health Information Technology; Revisions to ONC-Approved Accreditor Processes.'' The rule proposed a process for addressing instances where the ONC–Approved Accreditor (ONC–AA) engaged in improper conduct or did not perform its responsibilities under the permanent certification program, addressed the status of ONC-Authorized Certification Bodies in instances where there may be a change in the accreditation organization serving as the ONC–AA, and clarified the responsibilities of the new ONC–AA. All these proposals were finalized in a final rule published on November 25, 2011 (76 FR 72636).

The 2014 Edition final rule made changes to the permanent certification program. The final rule adopted a proposal to change the Permanent Certification Program's name to the ''ONC HIT Certification Program,'' revised the process for permitting the use of newer versions of ''minimum standard'' code sets, modified the certification processes ONC–ACBs need to follow for certifying EHR Modules in a manner that provides clear implementation direction and compliance with the new certification criteria, and eliminated the certification requirement that every EHR Module be certified to all the mandatory ''privacy and security'' certification criteria.

The Voluntary Edition proposed rule included proposals that focused on improving regulatory clarity, simplifying the certification of EHR Modules that are designed for purposes other than meeting Meaningful Use requirements, and discontinuing the use of the Complete EHR definition. As noted above, we issued the 2014 Edition Release 2 final rule to complete the rulemaking for the Voluntary Edition proposed rule. The 2014 Edition Release 2 final rule discontinued the ''Complete EHR'' certification concept beginning with the proposed 2015 Edition, adopted an updated standard (ISO/IEC 17065) for the accreditation of ONC–ACBs, and adopted the ''ONC Certified HIT'' certification and design mark for required use by ONC–ACBs under the ONC Health IT Certification Program.

III. Provisions of the Proposed Rule Affecting Standards, Implementation Specifications, and Certification Criteria

A. 2015 Edition Health IT Certification Criteria

This rule proposes new, revised, and unchanged certification criteria that would establish the capabilities and related standards and implementation specifications for the certification of health IT, including EHR technology. We refer to these new, revised, and unchanged certification criteria as the ''2015 Edition health IT certification criteria'' and propose to add this term and its definition to § 170.102. As noted in the Executive Summary, we also refer to these criteria as the ''2015 Edition'' in this preamble. We propose to codify the 2015 Edition in § 170.315 to set them apart from other editions of certification criteria and make it easier for stakeholders to quickly determine the certification criteria the 2015 Edition includes.

Health IT certified to these proposed certification criteria and associated standards and implementation specifications could be implemented as part of an EP's, eligible hospital's, or CAH's CEHRT and used to demonstrate meaningful use (as identified in Table 2 below). We note that Table 2 does *not* identify certification criteria that are included in conditional certification requirements, such as privacy and security, safety-enhanced design, and quality management system certification criteria. We do, however, classify these types of certification criteria as ''associated'' with the EHR Incentives Programs Stage 3 for the purposes of the regulatory impact analysis we performed for this proposed rule (see section VIII.B.1).

Health IT certified to the proposed certification criteria and associated standards and implementation specifications could also be used to meet other HHS program requirements (*e.g.*, grant and contract requirements) or referenced by private sector associations and entities.

TABLE 2—2015 EDITION PROPOSED CERTIFICATION CRITERIA ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3

Proposed CFR citation	Certification criterion	Proposed inclusion in 2015 edition base EHR definition	Relationship to the proposed CEHRT[2] definition and proposed stage 3 objectives
§ 170.315(a)(1)	Computerized Provider Order Entry (CPOE)—medications.	Included[3]	Objective 4.
§ 170.315(a)(2)	CPOE—laboratory	Included[4]	Objective 4.
§ 170.315(a)(3)	CPOE—diagnostic imaging	Included[5]	Objective 4.

TABLE 2—2015 EDITION PROPOSED CERTIFICATION CRITERIA ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3—Continued

Proposed CFR citation	Certification criterion	Proposed inclusion in 2015 edition base EHR definition	Relationship to the proposed CEHRT[2] definition and proposed stage 3 objectives
§ 170.315(a)(4)	Drug-drug, Drug-allergy Interaction Checks for CPOE.	Not included	Objective 3.
§ 170.315(a)(5)	Demographics	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(a)(7)	Problem List	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(a)(8)	Medication List	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(a)(9)	Medication Allergy List	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(a)(10)	Clinical Decision Support	Included	Objective 3.
§ 170.315(a)(11)	Drug-formulary and Preferred Drug List Checks.	Not included	Objective 2.
§ 170.315(a)(12)	Smoking Status	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(a)(14)	Family Health History	Not included	CEHRT[6].
§ 170.315(a)(15)	Family Health History—pedigree	Not included	CEHRT[7].
§ 170.315(a)(17)	Patient-specific Education Resources	Not included	Objective 5.
§ 170.315(a)(19)	Patient Health Information Capture	Not included	CEHRT Objective 6.
§ 170.315(a)(20)	Implantable Device List	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(b)(1)	Transitions of Care	Included	Objective 7.
§ 170.315(b)(2)	Clinical Information Reconciliation and Incorporation.	Not included	Objective 7.
§ 170.315(b)(3)	Electronic Prescribing	Not included	Objective 2.
§ 170.315(b)(6)	Data Portability	Included	No additional relationship beyond the Base EHR definition.
§ 170.315(c)(1)[8]	Clinical Quality Measures—record and export.	Included	CEHRT.
§ 170.315(e)(1)	View, Download, and Transmit to Third Party.	Not included	Objective 5 Objective 6.
§ 170.315(e)(2)	Secure Messaging	Not included	Objective 6.
§ 170.315(f)(1)	Transmission to Immunization Registries.	Not included	Objective 8.[9]
§ 170.315(f)(2)	Transmission to Public Health Agencies—syndromic surveillance.	Not included	Objective 8.
§ 170.315(f)(3)	Transmission to Public Health Agencies—reportable laboratory tests and values/results.	Not included	Objective 8.
§ 170.315(f)(4)	Transmission to Cancer Registries	Not included	Objective 8.
§ 170.315(f)(5)	Transmission to Public Health Agencies—case reporting.	Not included	Objective 8.
§ 170.315(f)(6)	Transmission to Public Health Agencies—antimicrobial use and resistance reporting.	Not included	Objective 8.
§ 170.315(f)(7)	Transmission to Public Health Agencies—health care surveys.	Not included	Objective 8.
§ 170.315(g)(1)	Automated Numerator Recording	Not included	CEHRT.
§ 170.315(g)(2)	Automated Measure Calculation	Not included	CEHRT.
§ 170.315(g)(7)	Application Access to Common Clinical Data Set.	Included	Objective 5 Objective 6.
§ 170.315(h)(1)	Direct Project	Included[10]	No additional relationship beyond the Base EHR definition.
§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM.	Included[11]	No additional relationship beyond the Base EHR definition.

[2] CMS' CEHRT definition would include the criteria adopted in the Base EHR definition. For more details on the CEHRT definition, please see the CMS EHR Incentive Programs proposed rule published elsewhere in this issue of the **Federal Register**.

[3] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[4] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[5] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[6] Technology needs to be certified to § 170.315(a)(14) or (a)(15).

[7] Technology needs to be certified to § 170.315(a)(14) or (a)(15).

[8] As discussed in the preamble for the "clinical quality measures—report" criterion, additional CQM certification policy may be proposed in or with CMS payment rules in CY15. As such, additional CQM certification criteria may be proposed for the Base EHR and/or CEHRT definitions.

[9] For the public health certification criteria in § 170.315(f), technology would only need to be certified to those criteria that are required to meet the options the provider intends to report in order to meet the proposed Objective 8: Public Health and Clinical Data Registry Reporting.

[10] Technology needs to be certified to § 170.315(h)(1) or (h)(2) to meet the proposed Base EHR definition.

[11] Technology needs to be certified to § 170.315(h)(1) or (h)(2) to meet the proposed Base EHR definition.

1. Applicability

Section 170.300 establishes the applicability of subpart C—Certification Criteria for Health Information Technology. We propose to revise paragraph (d) of § 170.300 to add in a reference to § 170.315 and revise the parenthetical in the paragraph to say ''*i.e.,* apply to any health care setting'' instead of ''*i.e.,* apply to both ambulatory and inpatient settings.'' These proposed revisions would clarify which specific capabilities *within* a certification criterion included in § 170.315 have general applicability (*i.e.,* apply to any health care setting) or apply only to an inpatient setting or an ambulatory setting. The proposed revision to change the language of the parenthetical aligns with our proposed approach to make the ONC Health IT Certification Program more agnostic to health care settings and accessible to health IT that supports care and practice settings beyond the ambulatory and inpatient settings. We refer readers to section IV.B of this preamble for a detailed discussion of our proposals to modify the ONC Health IT Certification Program.

We note that, with the proposed 2015 Edition, we no longer label certification criteria as either optional or ambulatory/inpatient (at the second paragraph level). For example, the proposed 2015 Edition certification criterion for electronic medication administration record is simply ''electronic medication administration record'' instead of ''inpatient setting only—electronic medication administration record.'' Similarly, the proposed 2015 Edition certification criterion for ''accounting of disclosures'' is simply ''accounting of disclosures'' instead of ''optional—accounting of disclosures.'' These simplifications are possible given that, beginning with the 2015 Edition health IT certification criteria, ''Complete EHR'' certifications will no longer be issued (see 79 FR 54443–45). Therefore, there is no longer a need to designate an entire certification criterion in this manner. Again, this approach supports our goal to make the ONC Health IT Certification Program more agnostic to health care settings and accessible to health IT that supports care and practice settings beyond the ambulatory and inpatient settings.

We propose to replace the term ''EHR technology'' in paragraphs (d)(1) and (d)(2) with ''health IT'' to align with our proposed approach to make the ONC Health IT Certification Program more clearly open to the certification of all types of health IT. Again, we refer readers to section IV.B of this preamble for a detail discussion of our proposals to modify the ONC Health IT Certification Program.

2. Standards and Implementation Specifications

a. National Technology Transfer and Advancement Act

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. § 3701 et. seq.) and the Office of Management and Budget (OMB) Circular A–119 [12] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. In this proposed rule, we refer to voluntary consensus standards, except for:

- The standards adopted in § 170.202. (These standards were developed by groups of industry stakeholders committed to advancing the Direct Project,[13] which included initiatives under the Standards and Interoperability (S&I) Framework.[14] These groups used consensus processes similar to those used by other industry stakeholders and voluntary consensus standards bodies.);
- The standards we propose to adopt at § 170.205(a)(5)(iii) and (iv) for electronic submission medical documentation (esMD) (These standards were developed by groups of industry stakeholders committed to advancing esMD,[15] which included initiatives under the Standards and Interoperability (S&I) Framework.[16] These groups used consensus processes similar to those used by other industry stakeholders and voluntary consensus standards bodies.);
- The standards we propose to adopt at § 170.205(d)(4) and (e)(4) for reporting of syndromic surveillance and immunization information to public health agencies, respectively (These standards go through a process similar within the public health community to those used by other industry stakeholders and voluntary consensus standards bodies.);
- The standard we propose to adopt at § 170.207(f)(2) for race and ethnicity; and
- Certain standards related to the protection of electronic health information adopted in § 170.210.

We are aware of no voluntary consensus standard that would serve as an alternative to these standards for the purposes that we have identified in this proposed rule.

b. Compliance With Adopted Standards and Implementation Specifications

In accordance with Office of the Federal Register regulations related to ''incorporation by reference,'' 1 CFR part 51, which we follow when we adopt proposed standards and/or implementation specifications in any subsequent final rule, the entire standard or implementation specification document is deemed published in the **Federal Register** when incorporated by reference therein with the approval of the Director of the Federal Register. Once published, compliance with the standard and implementation specification includes the entire document unless we specify otherwise. For example, if we adopted the HL7 Laboratory Orders Interface (LOI) implementation guide (IG) proposed in this proposed rule, health IT certified to certification criteria referencing this IG would need to demonstrate compliance with all mandatory elements and requirements of the IG. If an element of the IG is optional or permissive in any way, it would remain that way for testing and certification unless we specified otherwise in regulation. In such cases, the regulatory text would preempt the permissiveness of the IG.

c. ''Reasonably Available'' to Interested Parties

The Office of the Federal Register has established new requirements for materials (*e.g.,* standards and implementation specifications) that agencies propose to incorporate by reference in the **Federal Register** (79 FR 66267; 1 CFR 51.5(a)). To comply with these requirements, in section VI (''Incorporation by Reference'') of this preamble, we provide summaries of, and uniform resource locators (URLs) to, the standards and implementation specifications we propose to adopt and subsequently incorporate by reference in the **Federal Register**. To note, we also provide relevant information about

[12] *http://www.whitehouse.gov/omb/circulars_a119.*

[13] *http://www.healthit.gov/policy-researchers-implementers/direct-project.*

[14] *http://www.healthit.gov/policy-researchers-implementers/standards-interoperability-si-framework.*

[15] *http://wiki.siframework.org/esMD+-+Author+of+Record* and *http://wiki.siframework.org/esMD+-+Provider+Profiles+Authentication.*

[16] *http://www.healthit.gov/policy-researchers-implementers/standards-interoperability-si-framework.*

these standards and implementation specifications throughout this section of the preamble (section III), including URLs.

d. ''Minimum Standards'' Code Sets

We propose to adopt newer versions of four previously adopted minimum standards code sets in this proposed rule for the 2015 Edition. These code sets are the September 2014 Release of the U.S. Edition of SNOMED CT®, LOINC® version 2.50, the February 2, 2015 monthly version of RxNorm, and the February 2, 2015 version of the CVX code set. We also propose to adopt two new minimum standards code sets (the National Drug Codes (NDC)—Vaccine Codes, updates through January 15, 2015 and the ''Race & Ethnicity—CDC'' code system in the PHIN Vocabulary Access and Distribution System (VADS) Release 3.3.9 (June 17, 2011)). As we have previously articulated (77 FR 54170), the adoption of newer versions improve interoperability and health IT implementation, while creating little additional burden through the inclusion of new codes. As many of these minimum standards code sets are updated frequently throughout the year, we will consider whether it may be more appropriate to adopt a version of a minimum standards code set that is issued before we publish a final rule for this proposed rule. In making such determination, as we have done with these proposed versions of minimum standards code sets, we will give consideration to whether it includes any new substantive requirements and its effect on interoperability. If adopted, a newer version of a minimum standards code set would serve as the baseline for certification. As with all adopted minimum standards code sets, health IT can be certified to newer versions of the adopted baseline version minimum standards code sets for purposes of certification, unless the Secretary specifically prohibits the use of a newer version (see § 170.555 and 77 FR 54268).

e. Object Identifiers (OIDs) for Certain Code Systems

We are providing the following table of OIDs for certain code systems to assist health IT developers in the proper identification and exchange of health information coded to the vocabulary standards proposed in this proposed rule.

Code system OID	Code system name
2.16.840.1.113883.6.96	IHTSDO SNOMED CT.®
2.16.840.1.113883.6.1	LOINC.®
2.16.840.1.113883.6.88	RxNorm.
2.16.840.1.113883.12.292	HL7 Standard Code Set CVX-Vaccines Administered.
2.16.840.1.113883.6.69	National Drug Code Directory.
2.16.840.1.113883.6.8	Unified Code of Units of Measure (UCUM[17]).
2.16.840.1.113883.6.13	Code on Dental Procedures and Nomenclature (CDT).
2.16.840.1.113883.6.4	International Classification of Diseases, 10th Revision, Procedure Coding System (ICD–10–PCS).
2.16.840.1.113883.6.238	Race & Ethnicity—Centers for Disease Control and Prevention (CDC).
2.16.840.1.113883.6.316	Tags for Identifying Languages—Request for Comment (RFC) 5646 (preferred language).

f. Subpart B—Standards and Implementation Specifications for Health Information Technology

In§ 170.200, we propose to remove term ''EHR Modules'' and add in its place ''Health IT Modules.'' In § 170.210, we propose to remove the term ''EHR technology'' and add in its place ''health IT.'' These proposals are consistent with our overall approach to this rulemaking as discussed in the Executive Summary.

3. Certification Criteria

We discuss the certification criteria that we propose to adopt as the 2015 Edition below. In a header for each criterion, we specify where the proposed certification criteria would be included in § 170.315. We discuss each certification criterion in the chronological order in which it would appear in the CFR. In other words, the preamble that follows will discuss the proposed certification criteria in § 170.315(a) first, then § 170.315(b), and so on.

We identify the certification criteria as new, revised, or unchanged in comparison to the 2014 Edition. In the 2014 Edition final rule we gave meaning to the terms ''new,'' ''revised,'' and ''unchanged'' to both describe the differences between the 2014 Edition certification criteria and the 2011 Edition certification criteria as well as establish what certification criteria in the 2014 Edition were eligible for gap certification (see 77 FR 54171, 54202, and 54248). Given that beginning with the 2015 Edition ''Complete EHR'' certifications will no longer be issued (see also 79 FR 54443–45) and that our proposals in this proposed rule to make the ONC Health IT Certification Program more open and accessible to other health care/practice settings, we propose to give new meaning to these terms for the purpose of a gap certification analysis.

- ''*New''* certification criteria are those that as a whole only include capabilities never referenced in previously adopted certification criteria editions and to which a Health IT Module presented for certification to the 2015 Edition could have never previously been certified. As a counter example, the splitting of a 2014 Edition certification criterion into two criteria as part of the 2015 Edition would not make those certification criteria ''new'' for the purposes of a gap certification eligibility analysis.
- ''*Revised''* certification criteria are those that include within them capabilities referenced in a previously adopted edition of certification criteria as well as changed or additional new capabilities; and to which a Health IT Module presented for certification to the 2015 Edition could *not* have been previously certified to all of the included capabilities.
- ''*Unchanged''* certification criteria would be certification criteria that include the same capabilities as compared to prior certification criteria of adopted editions; and to which a Health IT Module presented for certification to the 2015 Edition could have been previously certified to all of the included capabilities.

We explain the proposed certification criteria and provide accompanying rationale for the proposed certification criteria, including citing the recommendations of the HITPC and HITSC, where appropriate. For 2015 Edition health IT certification criteria

[17] Copyright © 1998–2013, Regenstrief Institute, Inc. and the UCUM Organization. All rights reserved.

that have been revised in comparison to their 2014 Edition counterparts, we focus the discussion on any revisions and clarifications in comparison to the 2014 Edition version of the criteria. A revised 2015 Edition certification criterion would also include all the other capabilities that were included in the 2014 Edition version. For example, we propose to adopt a 2015 Edition ''drug-drug, drug-allergy interaction checks for CPOE'' certification criterion (§ 170.315(a)(4)) that is revised in comparison to the 2014 Edition ''drug-drug, drug-allergy interaction checks'' criterion (§ 170.314(a)(2)). We only discuss clarifications (*e.g.,* the criterion name change) and revisions we propose as part of the 2015 Edition ''drug-drug, drug-allergy interaction checks for CPOE'' certification criterion. However, the 2015 Edition criterion also includes all the other capabilities of the 2014 Edition ''drug-drug, drug allergy interaction checks'' criterion. We refer readers to § 170.315 of the proposed regulation text near the end of this document, which specifies all the capabilities included in each proposed 2015 Edition certification criterion.

We include an appendix (Appendix A) to this proposed rule, which provides a table with the following data for each proposed 2015 Edition certification criterion, as applicable: (1) Proposed CFR citation; (2) estimated development hours; (3) proposed privacy and security certification requirements (approach 1);[18] (4) conditional certification requirements (§ 170.550); (5) gap certification eligibility; (6) proposed inclusion in the 2015 Edition Base EHR definition; and (7) relationship to proposed Stage 3 of the EHR Incentive Programs, including the CEHRT definition.

We propose, and readers should interpret, that the following terms used in the proposed 2015 Edition have the same meanings we adopted in the 2014 Edition final rule (77 FR 54168–54169), in response to public comment: ''user,'' ''record,'' ''change,'' ''access,'' ''incorporate,'' ''create,'' and ''transmit,'' but apply to all health IT not just ''EHR technology.'' For the term ''incorporate,'' we also direct readers to the additional explanation we provided under the ''transitions of care'' certification criterion (77 FR 54218) in the 2014 Edition final rule and in the Voluntary Edition proposed rule (79 FR 10898). We propose that the scope of a 2015 Edition certification criterion is the same as the scope previously assigned to a 2014 Edition certification criterion (for further explanation, see the discussion at 77 FR 54168). That is, certification to proposed 2015 Edition health IT certification criteria at § 170.315 would occur at the second paragraph level of the regulatory section and encompass all paragraph levels below the second paragraph level. We also propose to continue to use the same specific descriptions for the different types of ''data summaries'' established in the 2014 Edition final rule (77 FR 54170–54171) for the proposed 2015 Edition health IT certification criteria (*i.e.,* ''export summary,'' ''transition of care/referral summary,'' ''ambulatory summary,'' and ''inpatient summary.'')

As with the adoption of the 2011 and 2014 editions of certification criteria (see the introductory text to §§ 170.302, 170.304, 170.306, and 170.314), all capabilities mentioned in certification criteria are expected to be performed electronically, unless otherwise noted. Therefore, we no longer include ''electronically'' in conjunction with each capability included in a certification criterion proposed under § 170.315 because the proposed introductory text to § 170.315 (which covers all the certification criteria included in the section) clearly states that health IT must be able to *electronically* perform the following capabilities in accordance with all applicable standards and implementation specifications adopted in the part.

- Computerized Provider Order Entry

In the 2014 Edition Release 2 final rule, we adopted separate computerized provider order entry (CPOE) certification criteria based on the clinical purpose (*i.e.,* medications, laboratory, and diagnostic imaging) (79 FR 54435–36). We propose to take the same approach for the 2015 Edition and propose to adopt three certification criteria for CPOE, as compared to a single criterion that would include combined functionality for all three clinical purposes (*e.g.,* § 170.314(a)(1)).

We request comment on whether we should specify, for the purposes of testing and certification to the 2015 Edition CPOE criteria, certain data elements that a Health IT Module must be able to include in a transmitted order. In particular, we request comment on whether a Health IT Module should be able to include any or all of the following data elements: secondary diagnosis codes; reason for order; and comment fields entered by the ordering provider, if they are provided to the ordering provider in their order entry screen. We also request comment on whether there are any other data elements that a Health IT Module should be able to include as part of an order for the purposes of testing and certification. We clarify, however, that any specific data requirements for a transmitted order that may be adopted in a final rule would only apply in the absence of a standard for testing and certification. As discussed below, we propose a laboratory order standard for the ambulatory setting. If we were to adopt this standard in a final rule, any potential required data elements for a transmitted order adopted in response to this proposal would not be made applicable to the ambulatory setting for the ''CPOE—laboratory'' certification criterion.

- *Computerized Provider Order Entry—Medications*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(1) (Computerized provider order entry—medications)

We propose to adopt a 2015 Edition CPOE certification criterion specific to medication ordering. This proposed criterion does not reference any standards or implementation specifications and is unchanged in comparison to the 2014 Edition CPOE—medications criterion adopted at § 170.314(a)(18).

- *Computerized Provider Order Entry—Laboratory*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(2) (Computerized provider order entry—laboratory)

We propose to adopt a 2015 Edition CPOE certification criterion specific to laboratory ordering that is revised in comparison to the CPOE—laboratory criterion adopted at § 170.314(a)(19) as well as § 170.314(a)(1).

We propose to adopt and include in this criterion, for the *ambulatory setting,* the HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders (LOI) from EHR, Draft Standard for Trial Use, Release 2—US Realm (''Release 2'').[19] Due to the absence of a consensus standard for the purpose of sending laboratory orders from EHRs to laboratories, this standard was developed in conjunction with laboratories representative of the industry, health IT developers, and

[18] Please see section IV.C.1 (''Privacy and Security'') for a detailed discussion of approach 1.

[19] *http://www.hl7.org/special/committees/projman/searchableprojectindex.cfm?action=edit&ProjectNumber=922* and *http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember.* Access to the current draft of the LOI Release 2 IG is freely available for review during the public comment period by establishing an HL7 user account.

provider stakeholders through an open consensus-based process under the Standards and Interoperability Framework (S&I Framework). Release 1 of the standard was balloted and approved through HL7, a standards developing organization. Release 2 is currently under ballot reconciliation with HL7 and should be published in the next few months. Release 2 would:

- Implement common formats across US Realm IGs for consistent reader experience (*e.g.,* sequence of sections, formatting, layout, and terminology);
- Adopt HL7 version 2.8 fields developed to fill gaps identified in the development of Release 1;
- Include harmonized data type ''flavors'' for use across the US Realm Lab IGs;
- Introduce initial requirements for error reporting conditions and severity (hard/soft errors) and system/application acknowledgements;
- Harmonize data element usage and cardinality requirements with LOI Release 1, and the electronic Directory of Services (eDOS) IG;
- Incorporate US Lab Realm value sets developed for clarity and consistency across all laboratory IGs; and
- Use a new publication method for value sets that allows for precision usage at point of use and provides ''at a glance'' comprehensive usage at the field and component-level across all laboratory IGs; and synced with value set activities (HL7, VSAC, etc.).

Overall, we propose to adopt Release 2 of the standard because it addresses errors and ambiguities found in Release 1 and harmonizes requirements with other laboratory standards we propose to adopt in this proposed rule. Release 2 would also make implementation of the LOI IG clearer and more consistent for health IT developers and laboratories, as well as improve interoperability. We propose to adopt Release 2 at § 170.205(l)(1).

Commenters on the Voluntary Edition proposed rule noted that for optimal interoperability we need to also adopt the most recent version of the HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Test Compendium Framework, Release 2, (also referred to as the ''electronic Directory of Services (eDOS) IG''), as it is the companion IG to the LOI IG. We agree with the commenters' assessment and propose to include the most recent version of the eDOS IG in this criterion for certification to all health care settings (*i.e.,* not confining it to only the ambulatory setting) and adopt it at § 170.205(l)(2). The most recent version of the eDOS IG will be Release 2, Version 1.2, which is scheduled to publish in the next few months. Release 2, Version 1.2 is currently under ballot reconciliation.[20] In general, the eDOS IG provides requirements and guidance for the delivery of an electronic Directory of Services (test compendium) from a laboratory (compendium producer) to an EHR or other system (compendium consumer) where it is used to produce electronic orders (LOI-conformant messages) for laboratory tests. Version 1.2 of the eDOS IG addresses errors and ambiguities in the prior version as well as harmonizes with Release 2 of the LOI IG.

We also propose, for the purposes of certification, to require a Health IT Module to be able to use, at a minimum, the version of Logical Observation Identifiers Names and Codes (LOINC®) adopted at § 170.207(c)(3) (version 2.50) as the vocabulary standard for laboratory orders. This is the most recent version of LOINC®. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of LOINC® as a minimum standards code set and our proposal to adopt version 2.50, or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

We note that the LOI Release 2 IG requires the information for a test requisition as specified in the Clinical Laboratory Improvement Amendments (CLIA), 42 CFR 493.1241(c)(1) through (c)(8), to be included in the content message. Therefore, inclusion of this standard for certification may also facilitate laboratory compliance with CLIA.

- *Computerized Provider Order Entry—Diagnostic Imaging*

2015 Edition Health IT Certification Criterion

§ 170.315(a)(3) (Computerized provider order entry—diagnostic imaging)

We propose to adopt a 2015 Edition CPOE certification criterion specific to diagnostic imaging. This proposed criterion does not reference any standards or implementation specifications, and is unchanged in comparison to the 2014 Edition CPOE—diagnostic imaging criterion adopted at § 170.314(a)(20). To note, we also propose to adopt the title of ''diagnostic imaging,'' which is the title we gave to the 2014 Edition version of this certification criterion in the 2014 Edition Release 2 final rule (79 FR 54436).

- *Drug-Drug, Drug-Allergy Interaction Checks for CPOE*

2015 Edition Health IT Certification Criterion

§ 170.315(a)(4) (Drug-drug, drug-allergy interaction checks for CPOE)

We propose to adopt a 2015 Edition ''drug-drug, drug-allergy interaction checks for CPOE'' certification criterion that is revised in comparison to the 2014 Edition ''drug-drug, drug-allergy interaction checks'' criterion (§ 170.314(a)(2)). We propose to clarify that the capabilities included in this criterion are focused on CPOE by including ''for CPOE'' in the title of this criterion.

We also propose to include in this criterion the capabilities to record user actions for drug-drug, drug-allergy interaction (DD/DAI) interventions and to enable a user to view the actions taken for DD/DAI interventions (also referred to as ''checks''). Specifically, we propose that a Health IT Module must be able to record at least one action taken and by whom in response to drug-drug or drug-allergy interaction checks. To be certified to this criterion, a Health IT Module (at a user's request) must also be able to generate either a human readable display or human readable report of actions taken and by whom in response to drug-drug or drug-allergy interaction checks.

We solicited comment in the Voluntary Edition proposed rule on whether health IT should be able to track (which means ''record'' and will be referred to as ''record'' throughout this preamble) provider (referred to as ''user'' for the purposes of this proposed certification criterion) actions for DD/DAI interventions, including recording if and when the user viewed, accepted, declined, ignored, overrode, or otherwise commented on the DD/DAI interventions. We received comments that supported recording user actions for DD/DAI interventions (79 FR 54449). We also received comments recommending that we consider including recording user actions in response to CDS interventions. We discuss those comments under the CDS certification criterion in this section (III.A.3) of the preamble.

We believe that recording user actions for DD/DAI interventions could assist with quality improvement and patient safety. While some commenters expressed concern that functionality for recording user actions would be

[20] *http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember.* Access to the current draft of the eDOS IG, Release 2, Version 1.2 is freely available for review during the public comment period by establishing an HL7 user account.

burdensome to develop, we believe the potential benefits of improved care and reduced adverse events that can come from using such functionality and being able to subsequently analyze user actions for DD/DAI interventions outweighs the development burden. To provide health IT developers with flexibility and the opportunity to innovate, we have explicitly not specified the types of actions a Health IT Module must be able to record to meet this criterion. Health IT developers would need to simply demonstrate that their Health IT Module can record at least one user action for DD/DAI checks. For example, a Health IT Module could include the capability to record whether the user viewed, accepted, declined, ignored, overrode, provided a rationale or explanation for the action taken, took some other type of action not listed here or otherwise commented on the DD/DAI check. We solicit comment on whether we should focus this proposed requirement to record at least one user action taken for DD/DAI interventions on a subset of DD/DAI interventions, such as those of highest patient safety concern, and what sources we should consider for defining this subset.

We note, however, that we do not intend with this proposed requirement to infer a specific workflow or user interface in order to achieve conformance to this criterion. While appropriate documentation in accordance with clinical, safety, and system design best practices for these DD/DAI interventions is beyond the scope of certification for this criterion, we would encourage health IT developers to consider these best practices in developing this functionality and attempt to not interrupt a provider's workflow unnecessarily to meet this criterion. This criterion also does *not* propose to establish the uses for the ''user action'' information, whom should be able to view the information, or who could adjust the capability. Further, based on stakeholder feedback, there does not appear to be a consensus method or standard for characterizing the severity of patient DD/DAI reactions. Therefore, until the stakeholder community determines if there should be a set of methods, standards, or clinical guidelines for determining the severity of a patient DD/DAI reaction, we believe that users should determine these definitions for their organization and/or setting.

While this proposed certification criterion focuses on DD/DAI checking at the point when a user enters a computerized order, we believe that there are instances when a user should be aware of a patient's DD/DAI when new medications or medication allergies are entered into the patient record. Therefore, we strongly encourage health IT developers to build in functionality, including but not limited to clinical decision support, that would inform a user of new or updated DD/DAI when the medication or medication allergy lists are updated. We also seek comment on whether we should include this functionality in certification and whether this functionality should be included in an existing certification criterion (*e.g.,* medication list, medication allergy list, clinical decision support) or a standalone criterion.

- *Demographics*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(5) (Demographics)

We propose to adopt a 2015 Edition ''demographics'' certification criterion that is revised as described below in comparison to the 2014 Edition certification criterion (§ 170.314(a)(3)).

Sex

We propose that, for certification (and testing) to this criterion, health IT must be capable of recording sex in accordance with HL7 Version 3 (''AdministrativeGender'') and a nullFlavor value attributed as follows: male (M); female (F); and unknown (UNK). This proposal serves as another means of improving interoperability through the use of consistent standards.

We propose in a later section of this rule that using HL7 Version 3 for recording sex would be required under the ''Common Clinical Data Set'' definition for certification to the 2015 Edition. Please see section III.B.3 ''Common Clinical Data Set'' of this preamble for further discussion of this associated proposal.

Race and Ethnicity

We propose that, for certification (and testing) to this criterion, a Health IT Module must be capable of recording each one of a patient's races and ethnicities in accordance with, at a minimum, the ''Race & Ethnicity—CDC'' code system in the PHIN Vocabulary Access and Distribution System (VADS), Release 3.3.9.[21] We also propose that a Health IT Module must be able to aggregate each one of a patient's races and ethnicities to the categories in the OMB standard for race and ethnicity, which we previously adopted for the 2011 Edition and 2014 Edition ''demographics'' certification criteria.

As discussed in the 2014 Edition final rule (77 FR 54208), the OMB standard for the classification of data on race and ethnicity requires that the option for selecting one or more racial designations be provided. The standard also permits the use of more than the minimum standard categories for race and ethnicity, but requires that the data can be ''rolled up'' or mapped to the minimum standard categories as well as aggregated. The ''Race & Ethnicity—CDC'' code system in PHIN VADS (at a minimum, Release 3.3.9) permits a much more granular structured recording of a patient's race and ethnicity with its inclusion of over 900 concepts for race and ethnicity. The recording and exchange of patient race and ethnicity at such a granular level can facilitate the accurate identification and analysis of health disparities based on race and ethnicity. Further, the ''Race & Ethnicity—CDC'' code system has a hierarchy that rolls up to the OMB minimum categories for race and ethnicity and, thus, supports aggregation and reporting using the OMB standard. Accordingly, we propose the adoption and inclusion of both these standards in this certification criterion as described.

For the purposes of testing and certification to this ''demographics'' criterion, we would test that a Health IT Module can record each one of a patient's races and ethnicities using any of the 900 plus concepts in the ''Race & Ethnicity—CDC'' code system. We would not, however, expect the user interface to include a drop-down menu of all 900 plus ''Race & Ethnicity—CDC'' code system concepts for race and ethnicity, as we believe doing so could have negative workflow effects. Rather, we expect that health IT developers and health care providers would work together to establish the appropriate implementation given the care setting.

We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our proposal to adopt ''Race & Ethnicity—CDC'' code system in PHIN VADS as a minimum standards code set and Release 3.3.9, or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

We propose in a later section of this proposed rule that the ''Race & Ethnicity—CDC'' code system in PHIN VADS (at a minimum, Release 3.3.9) and the OMB standard would become the race and ethnicity standards under the ''Common Clinical Data Set'' definition for certification to the 2015

[21] *https://phinvads.cdc.gov/vads/ViewCodeSystem.action?id=2.16.840.1.113883.6.238#.*

Edition. Please see section III.B.3 ''Common Clinical Data Set'' of this preamble for further discussion of this associated proposal.

Preferred Language

Based on specific HITSC recommendations from 2011, we adopted ISO 639–2 constrained by ISO 639–1 for recording preferred language in the 2014 Edition ''demographics'' certification criterion (77 FR 54208).[22] More specifically, this means that technology is required to be capable of using the alpha-3 codes of ISO 639–2 to represent the corresponding alpha-2 code in ISO–639–1. To provide further clarity, we issued FAQ 27 [23] in which we stated that where both a bibliographic code and terminology code are present for a required ISO 639–2 language, technology is expected to be capable of representing the language in accordance with the (T) terminology codes (ISO 639–2/T) for the purposes of certification. After we issued FAQ 27, we issued FAQ 43 [24] in which we acknowledge that our constrained approach to the use of ISO 639–2 unintentionally excluded multiple languages that are currently in use, such as sign language and Hmong. Additionally, ISO 639–2 is meant to support written languages, which may not be the language with which patients instinctively respond when asked for their preferred language.

To improve the situation described above, we propose to adopt the Internet Engineering Task Force (IETF) Request for Comments (RFC) 5646 [25] standard for preferred language. RFC 5646 entitled ''Tags for Identifying Languages, September 2009'' is the coding system that is commonly used to encode languages on the web and is the most current RFC for this purpose and listed as a ''best current practice.'' [26] The first part of the code relies on the shortest ISO–639 code for the language. That means a 2-character code if the language is specified in ISO 639–1 or a 3-character code from ISO 639–2 or –3, if the language is only listed in one of those two ISO standards. We are also aware that RFC 5646 supports dialects.

After consideration of comments we received on the Voluntary Edition proposed rule (79 FR 54450) and further research, we believe that RFC 5646 is the most appropriate standard to support preferred language interoperability. It is our understanding that this standard is compatible with the C–CDA Release 2.0 and that other preferred language standards in use today can be efficiently mapped to it, such as ISO 639–1, 639–2, and 639–3. Therefore, for the purposes of testing and certification to this ''demographics'' criterion, we would test that a Health IT Module can record a patient's preferred language using any of the codes in RFC 5646.

We emphasize that this requirement would apply to a Health IT Module presented for certification and not health care providers. In other words, a Health IT Module certified to this criterion would need to support the recording of preferred language in RFC 5646 and should in no way be interpreted or imply the way in which health care providers use the capability to record preferred language or the preferred language values they are presented with to select a patient's preferred language. For example, we would not expect the user interface to include a drop-down menu of all RFC 5646 codes for language, as we believe doing so could have negative workflow effects. Rather, we expect that health IT developers and health care providers would work together to establish the appropriate implementation given the care setting.

We propose in a later section of this proposed rule that RFC 5646 would also become the preferred language standard under the ''Common Clinical Data Set'' definition for certification to the 2015 Edition. Please see section III.B.3 (''Common Clinical Data Set'') of this preamble for further discussion of this associated proposal.

Preliminary Cause of Death and Date of Death

We propose to include in the 2015 Edition the capability to enable a user to electronically record, change, and access the ''date of death'' as a required capability that EHR technology designed for the inpatient setting must demonstrate. We previously included this capability as part of the 2011 Edition ''demographics'' certification criterion and inadvertently omitted it from the 2014 Edition. While we heard from commenters in response to the Voluntary Edition proposed rule that they were unaware of any developer removing this capability, we believe it is appropriate to specifically include this capability in the 2015 Edition criterion for testing and certification purposes and to align with the data required by the Meaningful Use criteria of the EHR Incentive Programs. To note, this functionality would be in addition to the inclusion in the 2015 Edition ''demographics'' certification criterion of the same capability to enable a user to electronically record, change, and access ''preliminary cause of death'' in case of mortality, as is included in the 2014 Edition ''demographics'' certification criterion.

- *Vital Signs, Body Mass Index (BMI), and Growth Charts*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(6) (Vital signs, body mass index, and growth charts)

We propose to adopt a 2015 Edition ''vital signs, BMI, and growth charts'' certification criterion that is revised in comparison to the 2014 Edition ''vital signs, BMI, and growth charts'' criterion (§ 170.314(a)(4)). Specifically, we propose to: 1) Expand the types of vital signs for recording; 2) require that each type of vital sign have a specific LOINC® code attributed to it; 3) that The Unified Code of Units of Measure, Revision 1.9, October 23, 2013 (''UCUM Version 1.9'') [27] be used to record vital sign measurements; and 4) that certain metadata accompany each vital sign, including date, time, and measuring- or authoring-type source.

Proposed Approach for Vital Signs

In the Voluntary Edition proposed rule (79 FR 10889–10890), we solicited comment on whether we should require health IT to record vital signs in standardized vocabularies. We solicited comments on whether we should require that vital signs be recorded in standardized vocabularies natively within the health IT system or only during transmission. We also solicited comment on whether we should require vital signs be recorded with specific metadata for contextual purposes.

Many commenters recommended that the industry should standardize how vital signs are represented and collected. To this end, we are aware that several stakeholder groups are working to define unique, unambiguous representations/definitions for clinical concepts along with structured metadata that together provide improved context for the system to interpret information, including vital signs. This approach can help increase data standardization at a granular level so that clinical elements and associated values/findings can be consistently represented and exchanged. For example, blood pressure is represented in current systems using a variety of formats, which creates

[22] *http://www.loc.gov/standards/iso639-2/php/code_list.php.*

[23] *http://www.healthit.gov/policy-researchers-implementers/27-question-10-12-027.*

[24] *http://www.healthit.gov/policy-researchers-implementers/43-question-11-13-043.*

[25] *http://www.rfc-editor.org/info/rfc5646.*

[26] *http://www.rfc-editor.org/info/rfc5646.*

[27] *http://unitsofmeasure.org/trac/.*

significant challenges to aggregate, compare, and exchange data across systems. This occurs despite the numeric nature of blood pressure, resulting in costly and time-consuming manual translation to integrate this data across systems.

Some commenters supported requiring standardized vocabularies for vital signs during data exchange rather than natively within the health IT system. While we agree that data should be exchanged in a standard way, we also believe that the granularity necessary to unambiguously represent this data should be implemented within health IT systems so that data is captured with the same level of specificity to enable consistent and reliable interpretation by other data users and receivers without requiring mapping. Thus, we propose that health IT demonstrate it is able to record vital signs data natively as specified below. Overall, these proposals reflect our interest in ensuring that the data a user enters into a health IT system is semantically and syntactically identical to the information coming out of the system and being exchanged. We believe this would increase the confidence that the data exchanged is what the provider intended.

The 2014 Edition ''vital signs'' certification criterion requires health IT to enable a user to electronically record, change, and access a patient's height/length, weight, and blood pressure. We propose to include BMI, heart rate, respiratory rate, temperature, oxygen saturation in arterial blood by pulse oximetry, and mean blood pressure as we understand that these vital signs are commonly captured or calculated (*i.e.,* BMI) in the routine course of clinical encounters across a wide variety of both inpatient and ambulatory settings. We also propose to further specify that health IT would need to be able to record diastolic and systolic blood pressure as separate vital signs rather than ''blood pressure'' (unspecified) as a single vital sign. We clarify that this list of vital signs is not intended to be comprehensive. Rather, these listed vital signs indicate our interest in a more specific approach to recording and exchanging vital signs data that could promote unambiguous interpretation. These vital sign concepts derive from the C–CDA standard and the Public Health Information Network Vocabulary Access and Distribution System value set for vital sign result types [28] (2.16.840.1.113883.3.88.12.80.62), which was developed by the Health IT Standards Panel.[29] Therefore, we believe the health care community has experience with collecting these vital sign concepts because they have been defined for some time as part of previous collaborative stakeholder work.

We propose to require that a Health IT Module be able to attribute a specific LOINC® code to each type of vital sign using the following identifiers:

- ''Systolic blood pressure'' with LOINC® code 8480–6;
- ''Diastolic blood pressure'' with LOINC® code 8462–4;
- ''Body height'' with LOINC® code 8302–2;
- ''Body weight measured'' with LOINC® code 3141–9;
- ''Heart rate'' with LOINC® code 8867–4;
- ''Respiratory rate'' with LOINC® code 9279–1;
- ''Body temperature'' with LOINC® code 8310–5;
- ''Oxygen saturation in arterial blood by pulse oximetry'' with LOINC® code 59408–5;
- ''Body mass index (BMI) [Ratio]'' with LOINC® code 39156–5; and
- ''Mean blood pressure'' with LOINC® code 8478–0.

We understand that the industry is commonly identifying these vital signs using LOINC® codes today.

We also propose to require that a Health IT Module enable a user to record these vital signs with at least the following metadata:

- date and time of vital sign measurement or end time of vital sign measurement with optional certification in accordance with the clock synchronization standard adopted at § 170.210(g); and
- the measuring- or authoring-type source of the vital sign measurement (such as the user who documented the vital sign or the medical device that was used to measure the vital sign).

In some cases, the provider documenting the vital sign may record the date and time of vital sign measurement manually and enter the data into a health IT system at a later time; therefore, it would not be necessary to use the clock synchronization standard. However, use of the clock synchronization standard may be useful for situations where the vital sign data comes from a device and should be synchronized with the health IT system.

For ''oxygen saturation in arterial blood by pulse oximetry,'' we propose that a Health IT Module enable a user to record ''inhaled oxygen concentration'' with LOINC® code 3150–0 as metadata associated with the vital sign. We understand that ''inhaled oxygen concentration'' is frequently provided to assist with interpretation of the ''oxygen saturation in arterial blood by pulse oximetry'' value.

For all units of measure associated with a vital sign value, we propose to require that health IT be able to record an applicable unit of measure in accordance with UCUM Version 1.9 (*e.g.,* the UCUM unit ''mm[Hg]'' for systolic blood pressure; *e.g.,* the UCUM unit ''[lb_av],'' ''g,'' ''kg,'' or ''[oz_av]'' for body weight). We note that LOINC provides a translation table [30] that enumerates the UCUM syntax for a subset of UCUM codes that are commonly used in health IT that may be a useful reference for stakeholders.

Proposed ''Optional'' Pediatric Vital Signs

We propose to offer optional certification for health IT to be able to electronically record, change, and access:

- Body mass index (BMI) [Percentile] per age and sex (with LOINC® code 59576–9) for youth 2–20 years of age; and
- Weight for length per age and sex (with LOINC® code to be established in a newer version of LOINC® prior to the publication of a subsequent final rule) and/or Head occipital-frontal circumference by tape measure (with LOINC® code 8287–5) for infants less than 3 years of age.

We propose to require that a Health IT Module enable each optional vital sign to be recorded with an applicable unit of measure in accordance with UCUM Version 1.9. CDC recommends the collection of these anthropomorphic indices for youth 2–20 years of age and infants less than 3 years of age, respectively, as part of best care practices.[31]

A Health IT Module certified to the ''BMI percentile per age and sex,'' ''weight for length per age and sex,'' or ''head occipital-frontal circumference by tape measure'' vital signs would also need to record metadata for the date and time or end time of vital sign

[28] *https://phinvads.cdc.gov/vads/ViewValueSet.action?oid=2.16.840.1.113883.3.88.12.80.62.*

[29] The Health IT Standards Panel was established in 2005 as a strategic public-private partnership in contract with the U.S. Department of Health and Human Services to achieve a widely accepted and useful set of standards to enable and support widespread interoperability among healthcare software applications. The Health IT Standards Panel's contract with HHS concluded on April 30, 2010. *http://www.hitsp.org/.*

[30] *https://loinc.org/downloads/usage/units.*

[31] *http://www.cdc.gov/growthcharts/clinical_charts.htm#Set1* and *http://www.cdc.gov/growthcharts/clinical_charts.htm#Set2.*

measurement, the measuring- or authoring-type source of the vital sign measurement, the patient's date of birth, and the patient's sex in accordance with the standard we propose to adopt at § 170.207(n)(1). We believe offering optional certification to these three vital signs can provide value in settings where pediatric and adolescent patients are provided care.

Request for Comments on Vital Signs Proposal

We intend that the LOINC® codes proposed for attribution to the vital signs in the list above are neutral to, and therefore can encompass, any clinically reasonable method of measurement that is commonly used in obtaining vital signs in the course of clinical encounters in a wide variety of contexts, including but not limited to, primary-care office/clinic visits, emergency department visits, and routine inpatient admissions processes. For example, this would mean the system would attribute ''body height'' to LOINC® code 8302–2 for the measurement of how tall or long the patient is. This measurement is collected as part of routine vital signs observation regardless of whether this clinical observation was made by measuring a standing or supine adult/child, or a supine infant, or by estimating through clinically reasonable methods the height/length of an adult or child who cannot be measured in a standing or fully supine position.

Likewise, we propose to attribute a specific LOINC® code for body temperature regardless of whether the temperature was measured by a liquid-filled, digital/electronic, or infrared (non-contact) thermometer. The choice of UCUM unit code will indicate whether the measurement was taken in English or metric units. The metadata describing the source of the measurement would provide the context of the device that was used to perform the measurement. We reiterate that the intent behind this ''vital signs'' proposal is to ensure that the data a user enters into a health IT system is semantically and syntactically identical to the information coming out of the system and being exchanged, allowing other users to unambiguously and consistently interpret the information. We anticipate that stakeholders may want to expand the list of metadata beyond the date, time, and source of vital sign measurement. We welcome comment on additional vital sign metadata that we should consider for inclusion and the best available standards for representing the metadata (*e.g.,* LOINC® or a similar standard).

Health IT users may currently capture vital signs in more granular LOINC® codes that specify the method of measurement. We therefore solicit comment on the feasibility and implementation considerations for our proposals that rely on less granular LOINC® codes for attribution to vital sign measurements and the inclusion of accompanying metadata. Additionally, we solicit comment on the following issues:

- Support for or against the proposal to require attribution of vital sign values using specific LOINC® codes and associated metadata;
- whether our proposal will accomplish the stated goal of ensuring that the vital signs data a user enters into a health IT system is semantically and syntactically identical to the information coming out of the system and being exchanged;
- whether the LOINC® codes proposed above are the correct ones for representing the vital sign concepts broadly, including any method of measurement; and
- standards for recording the source of the vital sign measurement.

We also solicit comment on whether we should require a Health IT Module to be able to record metadata specific to particular vital signs results/findings. This could provide additional contextual information (*e.g.,* position for diastolic and systolic blood pressure, whether the patient is breathing supplemental oxygen, the site of the temperature such as oral or rectal, pregnancy status for BMI, and whether the vital sign was measured or self-reported). Because the LOINC® code associated with some vital sign concepts we are proposing may include whether the vital sign was measured or self-reported (*e.g.,* body weight measured), we also request comment on which specific vital signs should include metadata on whether it was measured or self-reported. If we were to require a Health IT Module to be able to record metadata specific to particular vital signs, we solicit comment on what additional metadata should be required for certification and what standards (*e.g.,* LOINC® or a similar standard) we should consider for representing that data.

We note, with respect to arterial oxygen saturation, that we are proposing here the type of measurement that we understand to be commonly performed as part of vital signs observation across a wide variety of clinical settings. We are aware that in some clinical circumstances oxygen saturation in arterial blood by pulse oximetry is not a sufficiently precise measurement to support sound clinical decisions. We therefore invite comment as to whether we should consider defining the arterial blood oxygen saturation vital sign in a more method-agnostic way, and whether we should also require capture and exchange of more robust metadata to ensure technology could reliably identify to clinicians seeking to use the value whether it was measured by pulse oximetry or a more precise but more invasive and, in most clinical contexts, less commonly performed arterial blood gas (ABG) test.

We propose in a later section of this proposed rule that vital signs be represented in same manner for the ''Common Clinical Data Set'' definition as it applies to the certification of health IT to the 2015 Edition. Note that the optional portions of the proposed vital signs criterion would not be required for the ''Common Clinical Data Set'' (*i.e.,* BMI percentile per age and sex for youth, weight for length for infants, head occipital-frontal circumference by tape measure, calculating BMI, and plotting and displaying growth charts.) Please see section III.B.3 (''Common Clinical Data Set'') of this preamble for further discussion of this associated proposal.

- *Problem List*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(7) (Problem list)

We propose to adopt a 2015 Edition ''problem list'' certification criterion that is revised in one way as compared to the 2014 Edition ''problem list'' certification criterion (§ 170.314(a)(5)). We propose to include the September 2014 Release of the U.S. Edition of SNOMED CT® in the 2015 Edition ''problem list'' certification criterion as the baseline version permitted for certification to this criterion. The 2014 Edition ''problem list'' criterion included the July 2012 Release of SNOMED CT® (International Release and the U.S. Extension) as the baseline version permitted for certification. We also refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our proposal to adopt the September 2014 Release (U.S. Edition), or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

- *Medication List*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(8) (Medication list)

We propose to adopt a 2015 Edition ''medication list'' certification criterion that is unchanged as compared to the 2014 Edition ''medication list'' certification criterion (§ 170.314(a)(6)). To note, this proposed criterion does not reference any standards or implementation specifications.

- *Medication Allergy List*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(9) (Medication allergy list)

We propose to adopt a 2015 Edition ''medication allergy list'' certification criterion that is unchanged as compared to the 2014 Edition ''medication allergy list'' certification criterion (§ 170.314(a)(7)).

We received comments in response to the Voluntary Edition proposed rule suggesting that a ''medication allergy list'' criterion should include also other types of allergies and intolerances, such as food and environmental allergies (79 FR 54451–52). We are aware of a number of vocabularies and code sets that could support food and environmental allergies as well as medications, but believe that the industry is working on identifying ways that multiple vocabularies and code sets can be used together in an interoperable way to support coding of allergies. Therefore, at this time, there is no ready solution for using multiple vocabularies to code allergies that could be adopted for the purposes of certification.

- *Clinical Decision Support*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(10) (Clinical decision support)

Health IT is key component of advanced health models and delivery system reform. CDS is a primary means of supporting the implementation of best evidence and new knowledge at the point of care and in real time (see our definition of ''CDS intervention'' discussed at 77 FR 13847). When effective decision support is presented in a useful manner, it enhances usability and helps providers and patients avoid medical errors. Therefore, we believe that clinical decision support is a crucial feature of certified health IT.

We propose to adopt a 2015 Edition ''clinical decision support'' certification criterion that is revised in comparison to the 2014 Edition ''CDS'' criterion (§ 170.314(a)(8)). We propose to adopt and include an updated ''Infobutton'' [32] standard and two updated associated IGs. We propose to require certification only to the Infobutton standard (and an associated IG) for identifying diagnostic or therapeutic reference information. We propose to require that a Health IT Module presented for certification to this criterion be able to record users' actions in response to CDS interventions. Last, we have revised the regulation text in comparison to the 2014 Edition CDS criterion to provide more clarity for certification to this proposed criterion as well as guidance for certification to the 2014 Edition CDS criterion.

Infobutton Standard and IGs

We propose to adopt and include the updated Infobutton standard (Release 2, June 2014) [33] in the proposed 2015 Edition CDS criterion. Infobutton provides a standard mechanism for health IT systems to request context-specific clinical or health knowledge from online resources. We propose to adopt and include the HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1, August 2013 (''SOA Release 1 IG'') [34] in the CDS criterion. The SOA Release 1 IG includes additional conformance criteria, redesigns extensions, revises possible values, and includes support for an additional format for representing knowledge responses. We also propose to adopt and include in the proposed 2015 Edition CDS criterion the updated Infobutton URL-based IG (HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4, June 2014) (''URL-based Release 4 IG'').[35] The IG provides a standard mechanism for health IT to submit knowledge requests to knowledge resources over the HTTP protocol using a standard URL format.

We propose to adopt the updated Infobutton standard with the SOA Release 1 IG at § 170.204(b)(3). We propose to adopt the updated Infobutton standard with the URL-based Release 4 IG at § 170.204(b)(4). We clarify that as proposed, a Health IT Module presented for certification would need to demonstrate the ability to electronically identify for a user diagnostic and therapeutic reference information in accordance with § 170.204(b)(3) *or* (b)(4) (*i.e.,* Infobutton and the SOA Release 1 IG *or* Infobutton and the URL-based Release 4 IG).

For certification to the 2014 Edition CDS criterion, we permit a health IT to be certified if it can electronically identify for a user diagnostic and therapeutic reference information using the Infobutton standard *or* another method (§ 170.314(a)(8)(ii)). For the 2015 Edition CDS criterion, we propose to require that a Health IT Module must be able to identify linked referential CDS information using the Infobutton standard *only,* as we believe this is the best consensus-based standard available to support this use case. We have taken this approach because certification focuses on the capabilities health IT can demonstrate (where applicable, according to specific standards) and not on how it is subsequently used. Thus, with this focus we believe we can refrain from continuing a regulatory requirement (*i.e.,* requiring ''another method'' for certification) from the 2014 Edition to the 2015 Edition.

For the proposed 2015 Edition ''patient-specific education resources'' certification criterion discussed later in this section of the preamble, we propose, for the purposes of certification, to require that a Health IT Module be able to request patient-specific education resources based on a patient's preferred language. We believe this capability would assist providers in addressing and mitigating certain health disparities. We solicit comment on whether we should require this functionality as part of the CDS certification criterion for reference materials identified using the Infobutton standards, including examples of use cases for which this functionality would be appropriate. We note that if should require a Health IT Module to be able to request patient-specific education resources based on a patient's preferred language as part of the CDS criterion, the availability of resources in a patient's preferred language depends on the material supported by the content provider. Therefore, to clarify, testing and certification would focus on the ability of the Health IT Module to make the request using a preferred language and Infobutton.

CDS Intervention Response Documentation

We solicited comment in the Voluntary Edition proposed rule on whether a Health IT Module should be able to record users' responses to the DD/DAI checks that are performed,

[32] Infobutton'' is typically the shorthand name used to refer to the formal standard's name: HL7 Version 3 Standard: Context-Aware Retrieval Application (Infobutton)

[33] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=208.*

[34] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=283.*

[35] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=22.*

including if and when the user viewed, accepted, declined, ignored, overrode, or otherwise commented on the product of a DD/DAI check. We also received comments recommending we broaden our consideration to include functionality for recording user responses for all CDS interventions. We believe that this functionality could be valuable for all CDS interventions, not solely DD/DAI checks, because it could assist with enhancing CDS intervention design and implementation, quality improvement, and patient safety.

As such, we propose that the CDS criterion include functionality at § 170.315(a)(10)(vi) that would require a Health IT Module to be able to record at least one action taken and by whom when a CDS intervention is provided to a user (*e.g.,* whether the user viewed, accepted, declined, ignored, overrode, provided a rationale or explanation for the action taken, took some other type of action not listed here, or otherwise commented on the CDS intervention). We also propose that a Health IT Module be able to generate either a human readable display or human readable report of the responses and actions taken and by whom when a CDS intervention is provided.

We note that we do not believe that a Health IT Module's ability to record user responses should increase provider burden in order to just meet this criterion. For example, we would not encourage implementations that would unnecessarily (*e.g.,* for a non-clinical or safety-related reason) interrupt a provider's workflow and require the provider to document the reason just to meet this criterion. Rather, we encourage health IT developers to leverage current best practices for presenting, documenting, and facilitating the safest and most appropriate clinical options in response to CDS interventions.

Clarifying ''Automatically'' and ''Triggered'' Regulatory Text

CDS can include a broad range of decision support interventions and are not solely limited to alerts. Our 2014 Edition ''CDS'' criterion uses the terms ''automatically'' and ''triggered'' when referencing interventions. The use of ''trigger'' and ''automatic'' can be associated with CDS rules or alerts, but may not encompass all kinds of CDS interventions. For example, CDS could be seamlessly presented in the user interface (*e.g.,* a dashboard display) or selected by the user within the workflow (*e.g.,* Infobutton or documentation flowsheets). The use of ''automatically'' and ''trigger'' as related to CDS interventions in the 2014 Edition ''CDS'' caused confusion as to what types of CDS interventions were permitted. To clarify, our intent is to encompass all types of CDS interventions without being prescriptive on how the interventions are deployed (*e.g.,* automatic, triggered, selected, seamless, or queried). As such, we are not using the terms ''automatically'' and ''trigger'' as related to CDS interventions in the regulatory text for this 2015 Edition certification criterion. However, we do not propose to change the regulatory text language in the 2014 Edition ''CDS'' certification criterion as current testing and certification under the ONC Health IT Certification Program permits the other types of interventions we have described above.

2014 Edition ''Clinical Decision Support'' Certification Criterion—Corrections

We propose to revise the cross-reference in § 170.314(a)(8)(iii)(B)(*2*) (CDS configuration) to more specifically cross-reference the 2014 ToC criterion (§ 170.314(b)(1)(iii)(B)). This more specific cross reference aligns with the our other proposed revision to this criterion, which is to add a cross-reference to § 170.314(b)(9)(ii)(D). We inadvertently omitted the cross-reference to § 170.314(b)(9)(ii)(D) in the 2014 Edition Release 2 final rule. These revised cross-references would more clearly indicate that health IT certified to the 2014 Edition CDS criterion would need to enable CDS interventions when a patient's medications, medication allergies, and problems are incorporated from a transition of care/care referral summary.

- *Drug Formulary and Preferred Drug List Checks*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(11) (Drug-formulary and preferred drug list checks)

We propose to adopt a 2015 Edition ''drug formulary checks and preferred drug list'' certification criterion that is revised in comparison to the 2014 Edition ''drug formulary checks'' certification criterion (§ 170.314(a)(10)). We propose a criterion that is split based on drug formularies and preferred drug lists. For drug formularies, we propose that a Health IT Module must (1) automatically check whether a drug formulary exists for a given patient and medication and (2) receive and incorporate a formulary and benefit file according to the NCPDP Formulary and Benefit Standard v3.0 (''v3.0''). We propose to adopt v3.0 at § 170.205(n)(1), but also solicit comment on more recent versions of the NCPDP Formulary and Benefit Standard. For preferred drug lists, we propose that a Health IT Module must automatically check whether a preferred drug list exists for a given patient and medication. This situation applies where the health IT system does not use external drug formularies, such as in a hospital health IT system. We also propose, for both drug formularies and preferred drug lists, that a Health IT Module be capable of indicating the last update of a drug formulary or preferred drug list as part of certification to this criterion. We believe that health IT should indicate the last update of the drug formulary or preferred drug list so the provider knows how recently the information was last updated. We also solicit comment on the best standard for individual-level, real-time formulary benefit checking to address the patient co-pay use case, and whether we should offer health IT certification to the standard for this use case.

As described in more detail in the Voluntary Edition proposed rule (79 FR 10892), CMS finalized a proposal to recognize NCPDP Formulary and Benefit Standard v3.0 as a backwards compatible version of NCPDP Formulary and Benefit Standard 1.0 for the period of July 1, 2014 through February 28, 2015, and to retire version 1.0 and adopt version 3.0 as the official Part D e-Prescribing standard on March 1, 2015 (78 FR 74787–74789). In response to the Voluntary Edition proposed rule, we received comments supporting adoption of the NCPDP Formulary and Benefit Standard v3.0 (''v3.0'') for this edition of certification criteria. Those commenters in support of adopting v3.0 noted the potential to reduce file sizes, which is beneficial when checking thousands of drug formularies on a daily basis. We agree with those commenters that v3.0 is the best available option for standardizing the implementation of drug-formulary checks in health IT and for its potential to reduce file sizes. As noted above, the adoption of v3.0 would also align with CMS' adoption of version 3.0 as the official Part D e-Prescribing standard beginning March 1, 2015.

We are aware that more recent versions of the NCPDP Formulary and Benefit Standard. Versions 4.0 (''v4.0'') (January 2013), 4.1 (''v4.1'') (October 2013), and 42 (October 2014) (''v42'')[36] have been published and are available for industry use. At the time of this

[36] Please note a change to the naming convention to Version 42 and Version 43, as NCPDP accepted a change request to remove the period in version numbering.

proposed rule, we understand that the NCPDP is currently developing and balloting Version 43 (''v43''). Version 4.0 has minor changes compared to v3.0, including removal of values from an unused diagnosis code, typographical corrections, and a change to the standard length of the name field. Version 4.1 removes files to support electronic prior authorization (ePA) transactions since these have been added to the NCPDP SCRIPT Standard Implementation Guide v2013011 (January 2013) and later versions, makes typographical corrections, adds a new coverage type for ePA routing, and adds an RxNorm qualifier to some data elements. V42 includes changes to reduce the file size. Stakeholder feedback has indicated that v4.0, v4.1, and v42 are backwards compatible with v3.0 for the elements that are the same as compared to v3.0.

We received mixed comments in response to the Voluntary Edition proposed rule on whether it is more appropriate to adopt v4.0 instead of v3.0 (79 FR 54454). Some commenters were concerned about known problems with v3.0 and indicated v4.0 could fix these known problems. Conversely, other commenters stated that v4.0 was too unstable and new for an edition of certification criteria that was anticipated to be adopted and in use in 2014. With these comments in mind, we solicit comment on whether we should adopt v4.0, v4.1, or v42 of the NCPDP Drug and Formulary Benefit Standard instead of v.3.0 for the proposed 2015 Edition ''drug formulary checks and preferred drug list'' criterion and what unintended impacts this could have on the industry given the Part D requirements.

We believe there is value in certifying that health IT is able to receive and incorporate a formulary and benefit file in accordance with the NCPDP Formulary and Benefit Standard v3.0. Systems would be able to incorporate more updated or complete formulary and benefit files to inform providers as they make determinations about which medications to prescribe their patients. We seek to understand the potential system burden in incorporating formulary and benefit files and, therefore, seek comment on this issue.

In the Voluntary Edition proposed rule, we noted that the NCPDP Formulary and Benefit Standard v3.0 did not address individual-level, real-time formulary benefit checking. Comments in response to the Voluntary Edition proposed rule noted that the ASC X12 270/271 Health Care Eligibility Benefit Inquiry and Response standard could perform individual-level, real-time formulary benefit checking in addition to the NCPDP Telecommunication Standard. Commenters also noted that e-prescribing networks could provide this service to customers within proprietary networks. We are aware of a recently established NCPDP task group that is defining potential use cases and business requirements for real-time benefit checking.

We continue to believe in the value of providers and patients knowing what the patient's cost sharing responsibilities are at the point of care for a given medication to inform discussions about a patient's care. Therefore, for this use case, we ask commenters to identify the best standard(s) for individual-level, real-time (at the point of care) formulary benefit checking and describe how the standard addresses this use case. We also solicit comment on whether we should offer certification for this use case using the appropriate standard for individual-level, real-time formulary benefit checking and whether it should be part of the 2015 Edition ''drug formulary and preferred drug list checks'' certification criterion or a standalone certification criterion.

- *Smoking Status*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(12) (Smoking status)

We propose to adopt a 2015 Edition ''smoking status'' certification criterion that is revised in comparison to the 2014 Edition ''smoking status'' criterion (§ 170.314(a)(11)). We propose that a Health IT Module must be able to record, change, and access smoking status in *any* of the available codes for smoking status in, at a minimum, the September 2014 Release of the U.S. Edition of SNOMED CT®.[37] We have taken this more flexible approach because there is no longer a proposed meaningful use objective and measure associated with this requirement and, thus, no specific requirement for certain codes to be used toward numerator calculation.

We note, however, that the 8 smoking status SNOMED CT® codes identified in § 170.207(h)[38] remain the same codes as identified for the 2014 Edition. They are also the value set included in the Common Clinical Data Set for the 2015 Edition and the only codes permitted for representing smoking status for electronic transmission in a summary care record for the purposes of certification. Therefore, a Health IT Module certified to certification criteria that reference the Common Clinical Data Set (*i.e.,* the ToC, data portability, VDT, Consolidated CDA creation performance, and application access to the Common Clinical Data Set certification criteria) would need to be able to code smoking status in only the 8 smoking status codes, which may mean mapping other smoking status codes to the 8 codes.

We also note that we would not expect the user interface to include a drop-down menu of all available SNOMED CT® smoking status codes, as we believe doing so could have negative workflow effects. Rather, we expect that health IT developers and health care providers would work together to establish the appropriate implementation given the care setting.

We propose to include the 2015 Edition ''smoking status'' certification criterion in the 2015 Edition Base EHR definition. Please see section III.B.1 of this preamble for further discussion of this associated proposal.

- *Image Results*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(13) (Image results)

We propose to adopt a 2015 Edition ''image results'' certification criterion that is unchanged in comparison to the 2014 Edition ''image results'' criterion (§ 170.314(a)(12)).

- *Family Health History*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(14) (Family health history)
2015 Edition Health IT Certification Criterion
§ 170.315(a)(15) (Family health history—pedigree)

We propose to adopt two 2015 Edition ''family health history'' (FHH) certification criteria. Both proposed criteria are revised in comparison to the 2014 Edition FHH certification criterion (§ 170.314(a)(13)). The proposed 2015 Edition FHH certification criterion at § 170.315(a)(14) would require

[37] We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our proposal to adopt the September 2014 Release (U.S. Edition), or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

[38] These 8 codes are: Current every day smoker, 449868002; current some day smoker, 428041000124106; former smoker, 8517006; never smoker, 266919005; smoker—current status unknown, 77176002; unknown if ever smoked, 266927001; heavy tobacco smoker, 428071000124103; and light tobacco smoker, 428061000124105.

technology to enable a user to record, change, and access a patient's FHH electronically according to, at a minimum, the concepts or expressions for familial conditions included in the September 2014 Release of the U.S. Edition of SNOMED CT®. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our proposal to adopt the September 2014 Release (U.S. Edition), or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

The proposed 2015 Edition FHH—pedigree certification criterion at § 170.315(a)(15) would require technology to enable a user to create and incorporate a patient's FHH according to HL7 Pedigree standard and the HL7 Pedigree IG, HL7 Version 3 Implementation Guide: Family History/Pedigree Interoperability, Release 1.[39] We believe that this approach gives the most flexibility to health IT developers and providers to develop, adopt, and implement technology that supports their clinical documentation needs, while still enabling interoperability. For example, some providers may only need technology that supports FHH coding in SNOMED CT®. Other providers may also want technology that supports genomic coding, which HL7 Pedigree can support. The adoption of two separate criteria can more effectively support different use cases and clearly identify the capabilities to which health IT has been certified.

As part of the 2014 Edition final rule, we incorrectly assigned the HL7 Pedigree standard to § 170.207 where we adopt ''vocabulary'' standards. Accordingly, for the 2015 Edition, we have placed the HL7 Pedigree standard and its IG in § 170.205(m)(1) to more accurately place it in the ''content'' exchange standards section of the CFR.

- *Patient List Creation*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(16) (Patient list creation)

We propose to adopt a 2015 Edition ''patient list creation'' certification criterion that is unchanged in comparison to the 2014 Edition ''patient list creation'' criterion (§ 170.314(a)(14)). We propose to incorporate our guidance provided in FAQ 39 [40] into the 2015 Edition ''patient list creation'' criterion. Specifically, the text of the 2015 Edition ''patient list creation'' certification criterion provides that a Health IT Module must demonstrate its capability to use at least one of the more specific data categories included in the ''demographics'' certification criterion (§ 170.315(a)(5)) (*e.g.,* sex or date of birth).

- *Patient-Specific Education Resources*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(17) (Patient-specific education resources)

We propose to adopt a 2015 Edition ''patient-specific education resources'' certification criterion that is revised in comparison to the 2014 Edition ''patient-specific education resources'' certification criterion (§ 170.314(a)(15)). We propose that certification would only focus on the use of Infobutton for this certification criterion instead of Infobutton *and* any means other than Infobutton as required by the 2014 Edition criterion. We have reviewed the regulatory burden posed by the 2014 Edition criterion and determined that there is diminished value in continuing to frame the 2015 Edition certification criterion in this way. We continue to believe, however, that the Infobutton capability is important to be available to providers to have and use to identify patient-specific education resources.

We propose to adopt the updated Infobutton standard (Release 2 and the associated updated IGs (SOA-based IG and URL-based IG)). These are discussed in more detail under the ''CDS'' certification criterion earlier in this section of the preamble. We also note that we no longer include a requirement that health IT be capable of electronically identifying patient-specific education resources based on ''laboratory values/results.'' We understand from stakeholder feedback on the 2014 Edition version of this criterion and our own research that the Infobutton standard cannot fully support this level of data specificity. For example, Infobutton could likely provide something useful for results that are a concept like ''E.coli,'' but not necessarily a numerical laboratory result.

We also propose that a Health IT Module be able to request patient-specific education resources based on a patient's preferred language as this would assist providers in addressing and mitigating certain health disparities. More specifically, we propose that a Health IT Module must be able to *request* that patient-specific education resources be identified (using Infobutton) in accordance with RFC 5646. We are aware, however, that Infobutton only supports a value set of ISO 639–1 for preferred language and, therefore, testing and certification of preferred language for this certification criterion would not go beyond the value set of ISO 639–1. To note, we also understand that the language of patient education resources returned through Infobutton is dependent on what the source can support. Thus, we reiterate that testing and certification would focus on the ability of the Health IT Module to make the request using a preferred language and Infobutton.

- *Electronic Medication Administration Record*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(18) (Electronic medication administration record)

We propose to adopt a 2015 Edition electronic medication administration record (eMAR) certification criterion that is unchanged in comparison to the 2014 Edition ''eMAR'' criterion (§ 170.314(a)(16)).

- *Patient Health Information Capture*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(19) (Patient health information capture)

We propose to adopt a new 2015 Edition ''patient health information capture'' certification criterion that would ''replace'' the 2014 Edition ''advance directives'' certification criterion (§ 170.314(a)(17)) for the purposes of certification to the 2015 Edition. The HITPC recommended, as part of their EHR Incentive Programs Stage 3 recommendations, that we adopt a certification criterion for ''advance directives'' that would require a Health IT Module to be capable of storing an advance directive and/or including more information about the advance directive, such as a link to the advance directive or instructions regarding where to find the advance directive or more information about it.[41] We agree with this recommendation in that more functionality should be demonstrated for certification as it relates to advance directives. Further, we believe that the functionality described by the HITPC can be more broadly applicable and, thus, have named this certification criterion to reflect functionality that can be applied to various patient health information documents. For example,

[39] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=301.*

[40] *http://www.healthit.gov/policy-researchers-implementers/39-question-04-13–039.*

[41] *http://www.healthit.gov/facas/sites/faca/files/HITPC_MUWG_Stage3_Recs_2014-04-01.pdf.*

we believe such capabilities could be applicable to birth plans as well as advance directives.

For certification to this criterion, we propose that a Health IT Module would need to properly identify health information documents for users (*e.g.,* label health information documents as advance directives and birth plans). A Health IT Module would also need to be able to demonstrate that it could enable a user to record (capture and store) and access (ability to examine or review) health information documents.

We further propose that a Health IT Module would need to be able to reference health information documents, which means providing narrative information on where to locate a specific health information document. A Health IT Module would also need to demonstrate that it can link to patient health information documents. ''Linking'' would require a Health IT Module to demonstrate it could link to an internet site storing a health information document. While an intranet link to a health information document might suffice for provider use, a Health IT Module would still need to demonstrate the ability to link to an external site via the internet for the purposes of certification.

We also propose that a Health IT Module would be required to demonstrate that it could enable a user to record and access information directly and electronically shared by a patient. This could come from multiple sources, including patient information provided directly from a mobile device. To note, we have not proposed any specific standards for this criterion related to receiving and accepting information directly and electronically shared by a patient.

We clarify that these capabilities may not be applicable to every patient health information document, but a Health IT Module would need to be able to perform all of these capabilities electronically for certification to this criterion.

- *Implantable Device List*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(20) (Implantable device list)

We propose to adopt a new 2015 Edition certification criterion focused on the ability of a Health IT Module to record, change, and access a list of unique device identifiers (UDIs) [42] corresponding to a patient's implantable devices (''implantable device list''), parse certain data from a UDI, retrieve the ''Device Description'' attribute associated with a UDI in the Global Unique Device Identification Database (GUDID), and make accessible to a user both the parsed and retrieved data. The proposed criterion represents a first step towards enabling health IT to facilitate the widespread availability and use of unique device identifiers to prevent device-related adverse events, enhance clinical decision-making related to devices, improve the ability of clinicians to respond to device recalls and device-related safety information, and achieve other important benefits, consistent with the fundamental aims of the HITECH Act [43] and the HHS Health IT Patient Safety Action and Surveillance Plan.[44]

FDA issued the Unique Device Identification System final rule on September 24, 2013.[45] The rule implements a statutory directive to establish a ''unique device identification system'' for medical devices that will enable adequate identification of devices through distribution and use.[46] It accomplishes this objective by requiring device labelers (usually the device manufacturer) to include a UDI on the label and packages of most medical devices subject to FDA jurisdiction. In addition, for each device with a UDI, the labeler must submit a standard set of identifying data elements to the FDA-administered GUDID, which will be publicly accessible.[47] Full implementation of the UDI system for devices that are implantable, life-saving, and life-sustaining is required by September 2015.[48]

We first proposed to adopt a certification criterion for implantable devices in the Voluntary Edition proposed rule (79 FR 10894). We received a large volume of comments on our proposal, many of which supported the adoption of a UDI-related certification criterion focused on implantable device list functionality. Some supporters of our proposal suggested that we wait to adopt it in our next rulemaking cycle in order to allow relevant standards and use cases to mature. Other commenters, mostly health IT developers, suggested that the proposed criterion would be applicable only to health IT systems designed for surgical or specific inpatient settings in which devices are implanted, and therefore suggested that we reduce the scope of the criterion to those settings.[49] For the reasons stated in the 2014 Edition Release 2 final rule,[50] we finalized only a small subset of the criteria we had originally proposed in the Voluntary Edition proposed rule. These criteria focused on adding flexibility and making improvements to the 2014 Edition. Consistent with this reduced scope, we did not finalize an implantable device list criterion at that time, stating instead our intention to propose such a criterion in our next rulemaking that would provide additional detail and clarity, as well as respond to concerns raised by commenters.

We continue to believe that incorporating UDIs in health IT is important and necessary to realize the significant promise of UDIs and FDA's

[42] A UDI is a unique numeric or alphanumeric code that consists of two parts: (1) a device identifier (DI), a mandatory, fixed portion of a UDI that identifies the labeler and the specific version or model of a device, and (2) a production identifier (PI), a conditional, variable portion of a UDI that identifies one or more of the following when included on the label of a device: the lot or batch number within which a device was manufactured; the serial number of a specific device; the expiration date of a specific device; the date a specific device was manufactured; the distinct identification code required by 21 CFR 1271.290(c) for a human cell, tissue, or cellular and tissue-based product (HCT/P) regulated as a device. *http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/.*

[43] Specifically, the certification criterion supports the National Coordinator's responsibility under the HITECH Act to ensure that the nation's health IT infrastructure supports activities that reduce medical errors, improve health care quality, improve public health activities, and facilitate the early identification and rapid response to public health threats and emergencies. 42 U.S.C. 300jj–11(b)(2) & (7).

[44] ONC, *HHS Health IT Patient Safety Action and Surveillance Plan* (July 2013), *http://www.healthit.gov/policy-researchers-implementers/health-it-and-patient-safety* (hereinafter ''Health IT Safety Plan''). The first objective of the Health IT Safety Plan is to use health IT to make care safer. *See id.* at 7. The Plan specifically contemplates that ONC will update its standards and certification criteria to improve safety-related capabilities and add new capabilities that enhance patient safety.

[45] 78 FR 58786.

[46] 21 U.S.C. 360i(f).

[47] See FDA, Global Unique Device Identification Database (GUDID) Guidance for Industry and Food and Drug Administration Staff (June 27, 2014), available at *http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM369248.pdf.*

[48] Pursuant to 21 U.S.C. 360i(f), FDA must implement the Unique Device Identification System Final Rule with respect to devices that are implantable, life-saving, and life sustaining not later than 2 years after the rule was finalized. Other implementation and compliance dates are detailed in the final rule. Compliance dates for UDI implementation will be phased in based on the existing risk-based classification of medical devices: September 2014 for devices classified by FDA at the highest risk level (Class III); September 2015 for implantable, life-supporting or life-sustaining devices; September 2016 for moderate risk (Class II) devices; and September 2018 for low risk (Class I) devices.

[49] For a detailed summary of the comments we received on our earlier implantable device list proposal, see the 2014 Edition, Release 2, final rule (79 FR 54458).

[50] 79 FR 54458.

Unique Device Identification System to protect patient safety and improve health care quality and efficiency. Crucially, recording and exchanging UDIs in patients' electronic health records would enable this information to travel with patients as they move among providers and throughout the health care system. With access to this information at the point of care, clinicians can accurately identify a patient's implantable devices and prevent adverse events resulting from misidentification or non-identification of the device and its associated safety characteristics (such as MRI compatibility and latex content). Health IT could also be leveraged in conjunction with automated identification and data capture (AIDC) or other technologies to streamline the capture and exchange of UDIs and associated data for patients' devices. As UDIs become ubiquitous, UDI capabilities in health IT could facilitate better post-market surveillance of devices, better and more accurate reporting of device-related events, and more effective corrective and preventative action in response to device recalls and alerts.

Fully implementing UDIs will take time and require addressing a number of challenges. A key challenge is that UDIs may initially be captured in any of a variety of clinical, inventory, registry, or other IT systems. Robust adoption and use of UDIs will require bridging these different components and changing IT and administrative processes to, among other things, ensure that UDIs are properly captured and associated with patients' electronic health records.

In December 2014, the Brookings Institution with collaboration from FDA published a detailed roadmap for effective UDI implementation.[51] Significantly, the roadmap's recommendations stated that ''while the path to full implementation is complex, there are relatively straightforward steps that can be done now'' to begin realizing the benefits of UDI implementation across the health care system. The roadmap's recommendations specifically urged ONC to support the incorporation of UDIs into certification criteria for health IT.

We agree that a key initial step towards solving these challenges is incorporating UDIs in certified health IT. We believe now is the appropriate time to take that first step. Major efforts have been underway for some time to harmonize and pilot health IT standards and specifications in support of a variety of UDI use cases, and substantial progress has been achieved to standardize the electronic exchange of UDIs.[52] In addition, FDA plans to implement the GUDID in early 2015 and require UDIs for all implantable devices by September 2015.[53] In light of this progress on technical standards and FDA's timeline for UDI implementation, we believe it is feasible for health IT developers to begin implementing the baseline functionality necessary to use and exchange UDIs, and in particular for UDIs associated with patient's implantable devices. Once implanted, these devices cannot be inspected with the naked eye and are therefore more susceptible to misidentification and resulting patient harm.

To meet this criterion, a Health IT Module would have to enable a user to record, change, and access a patient's implantable device list, which would consist solely of one or more UDIs associated with a patient's implantable devices. The Health IT Module would also have to be able to parse the following data elements from a UDI:

- Device Identifier;
- Batch/lot number;
- Expiration date;
- Production date; and
- Serial number.

In addition to parsing the UDI, a Health IT Module presented for certification would have to be able to retrieve the optional ''device description'' data element associated with the Device Identifier in the GUDID, if the data element has been populated. This could be accomplished using the GUDID's web interface, web services, downloadable module, or any other method of retrieval permitted under FDA's GUDID guidance.

For each UDI in a patient's implantable device list, a Health IT Module presented for certification would have to enable a user to access the UDI and the data elements identified above (including the ''device description,'' if it exists). Also, in addition to enabling a user to record and access UDIs for a patient's implantable devices and as noted above, a Health IT Module would be required to provide the capability to change UDIs from a patient's implantable device list in order to meet this criterion. This functionality would allow a user to delete erroneous or duplicative entries from a patient's implantable device list and update the list in the event that a device were removed from the patient. We seek comment on whether such functionality is necessary and whether there is a safer or more effective way to maintain the accuracy of this information.

We believe that, in addition to capturing UDIs, health IT should facilitate the exchange of UDIs in order to increase the overall availability and reliability of information about patients' implantable and other devices. Therefore, we propose in a later section of this rule to include the 2015 Edition ''implantable device list'' certification criterion in the 2015 Edition Base EHR definition and propose to include a patient's unique device identifier(s) as data within the Common Clinical Data Set definition for certification to the 2015 Edition. Please see section III.B of this preamble for further discussion of these associated proposals.

We have also proposed to modify § 170.102 to include new definitions for ''Device Identifier,'' ''Implantable Device,'' ''Global Unique Device Identification Database (GUDID),'' ''Production Identifier,'' and ''Unique Device Identifier.'' This will prevent any ambiguity in interpretation and ensure that each term's specific meaning reflects the same meaning given to them in the Unique Device Identification System final rule and in 21 CFR 801.3. Capitalization was purposefully applied

[51] The Brookings Institution, *Unique Device Identifiers (UDIs): A Roadmap for Effective Implementation* (December 2014) (available at *http://www.brookings.http://www.brookings.edu/~/media/research/files/papers/2014/12/05%20medical%20device%20tracking%20system/udi%20final%2012052014*).

[52] For example, the Brookings Institution and FDA convened a UDI Implementation Work Group comprising device manufacturers, payers, health IT developers, academics, clinicians, and other stakeholders to explore opportunities and challenges associated with capturing UDIs in claims, identifying steps for implementation and integration of UDIs within EHRs and other health care IT infrastructure, and utilizing UDIs as a tool for improved patient and provider connectivity. *http://www.brookings.edu/about/centers/health/projects/development-and-use-of-medical-devices/udi.* The Work Group held a series of expert workshops and in December 2014 published a detailed roadmap for effective UDI implementation. The Brookings Institution, *Unique Device Identifiers (UDIs): A Roadmap for Effective Implementation* (December 2014) (available at http://www.brookings.http://www.brookings.edu/~/media/research/files/papers/2014/12/05%20medical%20device%20tracking%20system/udi%20final%2012052014). Concurrently, the HL7 Technical Steering Committee has established a UDI Task Force to ensure that UDI is implemented in a consistent and interoperable manner across the suite of HL7 standards. See *http://hl7tsc.org/wiki/index.php?title=TSC_Minutes_and_Agendas.* And through an S&I Framework Structured Data Capture Initiative, ONC, AHRQ, FDA, and NLM are collaborating with industry stakeholders to include UDI data for devices in health IT adverse event reporting. See *http://wiki.siframework.org/Structured+Data+Capture+Initiative.* AHRQ has already incorporated UDI and associated data attributes in its Common Formats for adverse event reporting. See AHRQ Data Dictionary, Common Formats Hospital Version 1.2, at 87, available at *https://www.psoppc.org/c/document_library/get_file?p_l_id=375680&folderId=431263&name=DLFE-15061.pdf.*

[53] *http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm427496.htm*; see also 21 U.S.C. 360i(f).

to each word in these defined phrases in order to signal to readers that they have specific meanings. Please see section III.B of this preamble for further discussion of these associated proposals.

In several respects the scope of this proposed implantable device list criterion is narrower than the criterion we proposed in the Voluntary Edition proposed rule. We received comments in response to the Voluntary Edition proposed rule recommending clear standards and use cases for an ''implantable device list'' criterion. With consideration of these comments, unlike in the Voluntary Edition proposed rule, we do not propose that health IT certified to the 2015 Edition ''implantable device list'' criterion be required to exchange or display contextual information (such as a procedure note) associated with a UDI because we believe additional standards and use case development will be needed to support these capabilities. We request comment on whether we have overlooked the need for or feasibility of requiring this functionality.

We also do not propose any requirements on health IT to facilitate the ''capture'' of UDIs at the point of care. As discussed above, UDIs may initially be captured in any of a variety of clinical and non-clinical contexts, many of which are beyond the current scope of health IT certified under the ONC Health IT Certification Program. Prescribing a requirement for capturing UDIs in certified health IT would also be complicated by the range of data capture tools permitted under the UDI final rule, including several different types of AIDC technology. Moreover, as several commenters pointed out in response to our proposal in the Voluntary Edition proposed rule, only a subset of certified health IT users—generally surgeons or other clinicians who perform or assist with operations involving implantable devices—would have a need for such data capture functionality, and presumably health IT developers who specialize in health IT for these settings can develop appropriate solutions for these users.

Given the scope of our program and the current state of UDI adoption, we do not believe that it would be useful to address these ''upstream'' issues at this time through rulemaking. Hence our proposal focuses on: (1) Ensuring that certified health IT can record and exchange UDIs for implantable devices as part of a patient's core electronic health record using appropriate standards for interoperability and exchange so that regardless of how UDIs are captured, they can be readily integrated with patients' electronic health records; (2) providing all users of certified health IT with the ability to access basic information about patients' implantable devices, thereby promoting greater awareness of and stimulating additional demand for UDIs and UDI-related capabilities in health IT; and (3) encouraging health IT developers to begin implementing GUDID functionality. We believe that focusing on these three areas of baseline UDI functionality will provide the greatest value to our stakeholders and efforts to promote adoption of UDIs and realize the significant benefits of UDIs and FDA's Unique Device Identification System described in this proposal.

- *Social, Psychological, and Behavioral Data*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(21) (Social, psychological, and behavioral data)

We propose a new 2015 Edition ''social, psychological, and behavioral data'' certification criterion that would require a Health IT Module to be capable of enabling a user to record, change, and access a patient's social, psychological, and behavioral data based on SNOMED CT® and LOINC® codes. This would include the ability to record a patient's decision not to provide the information.

An individual's health is shaped largely by life circumstances that fall outside the traditional health care system and include social, psychological, and behavioral factors. These factors include, but are not limited to, family support systems, stress, housing, nutrition, income, and education. This proposed certification criterion to further the collection and use of such patient data is not intended to be comprehensive; rather, it reflects efforts to further HHS priorities to transform health delivery, to reduce health disparities, and to achieve the overarching goals of the National Quality Strategy. In particular, the proposed certification criterion supports efforts to reduce disparities and efforts to collect patient social, psychological, and behavioral data for improved health care, such as by aligning with recommendations from HHS and the Institute of Medicine.[54]

We believe that offering certification that would require a Health IT Module to enable a user to record, change, and access a patient's social, psychological, and behavioral data would assist a wide array of stakeholders (*e.g.,* providers, consumers, payors, community-based organizations, and state and local governments) in better understanding how this data may adversely affect health. Ultimately, this can lead to better health outcomes for these populations through improved patient care, quality improvement, health equity, and clinical decision support based on individual factors.

We also believe the self-reporting of information by individuals in response to the questions included in these social, psychological, and behavioral measures (*i.e.,* the question and answer sets below) could be utilized for the EHR Incentive Programs Stage 3 which proposes an objective on patient engagement, including patient-generated health data. For more information, please refer to the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register**.

We have heard from many stakeholders recommending that we prioritize the use of available measures and instruments for the structured recording of social, psychological, and behavioral data, and have followed those recommendations here. The measures (questions and answers sets below) will have LOINC® codes (or in the case of sexual orientation and gender identity, SNOMED CT® codes for the answers—but no specific questions) used to identify them. Therefore, we propose, for certification to this criterion, that social, psychological, and behavioral data be coded in accordance with, at a minimum, version 2.50 of LOINC® as attributed in the table below.[55] Please note that some question-answer sets for specific domains do not currently have a LOINC® code in place; in these instances it is expected that LOINC® codes will be established in a newer version of LOINC® prior to the

[54] U.S. Department of Health and Human Services, Office of Minority Health, 2011, *HHS Action Plan to Reduce Racial and Ethnic Disparities: A Nation Free of Disparities in Health and Health Care* (available at: *http://www.minorityhealth.hhs.gov/npa/files/Plans/HHS/HHS_Plan_complete.pdf*); U.S. Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation, 2011, *Implementation Guidance on Data Collection Standards for Race, Ethnicity, Sex, Primary Language, and Disability Status* (available at: *http://aspe.hhs.gov/datacncl/standards/ACA/4302/index.pdf*); and Institute of Medicine (IOM), November 2014, Washington, DC, The National Academies Press, 2014, *Capturing Social and Behavioral Domains and Measures in Electronic Health Records: Phase 2* (available at: *http://iom.edu/Reports/2014/EHRdomains2.aspx*).

[55] We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of LOINC® as a minimum standards code set and our proposal to adopt version 2.50, or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

publication of a subsequent final rule. Please further note that we propose to include sexual orientation and gender identity within this certification criterion as described after this table.

Domain	Question(s) [LOINC® name]	Answer(s) [LOINC® answer code]	LOINC® Codes for question-answer list combination	LOINC® Answer list ID
Financial Resource Strain (Overall financial resource strain from CARDIA).	How hard is it for you to pay for the very basics like food, housing, medical care, and heating? Would you say it is . . .	For example: Very hard, Somewhat hard, Not hard, at all.[56]	LOINC® code pending.	LOINC® code pending.
Education (Educational attainment).	What is the highest level of school you have completed or the highest degree you have received? [57]	[0] Never attended/kindergarten only [1] 1st grade [2] 2nd grade [3] 3rd grade [4] 4th grade [5] 5th grade [6] 6th grade. [7] 7th grade. [8] 8th grade. [9] 9th grade. [10] 10th grade. [11] 11th grade. [12] 12th grade, no diploma. [13] High school graduate. [14] GED or equivalent. [15] Some college, no degree. [16] Associate degree: occupational, technical, or vocational program. [17] Associate degree; academic program. [18] Bachelor's degree (e.g., BA, AB, BS). [19] Master's degree (e.g., MA, MS, MEng, MEd, MSW, MBA). [20] Professional school degree (example: MD, DDS, DVM, JD). [21] Doctoral degree (example: PhD, EdD). [77] Refused. [99] Don't know.	63504–5	LL1069–5.
Stress (from Elo et al) [58]	Stress means a situation in which a person feels tense, restless, nervous, or anxious, or is unable to sleep at night because his/her mind is troubled all the time. Do you feel this kind of stress these days?	For example: Likert scale ranging from 1—indicating not at all, 2—a little bit, 3—somewhat, 4—quite a bit, to 5—indicating very much.	LOINC® code pending.	LOINC® code pending.
Depression (PHQ–2)	[Patient Health Questionnaire 2 item (PHQ–2) [Reported]].	N/A	55757–9	N/A.
	Little interest or pleasure in doing things in last 2 weeks [Reported.PHQ].	[0] Not at all, [1] Several days, [2] More than half the days, [3] Nearly every day.	44250–9	LL358–3.
	Feeling down, depressed or hopeless in last 2 weeks [Reported.PHQ].	[0] Not at all, [1] Several days, [2] More than half the days, [3] Nearly every day.	44255–8	LL358–3.
	[Patient Health Questionnaire 2 item (PHQ–2) total score [Reported]].	For example: 0–6	5578–7	Answer is in UCUM units.[59]
Physical Activity (Exercise Vital Signs).	How many days of moderate to strenuous exercise, like a brisk walk, did you do in the last 7 days? [SAMHSA].	For example: 1,2,3,4,5,6,7, etc.	68515–6	Answer is in UCUM units.[60]
	On those days that you engage in moderate to strenuous exercise, how many minutes, on average, do you exercise? [SAMHSA].	For example: 10, 20, etc.	68516–4	Answer is in UCUM units.
Alcohol Use (AUDIT–C)	[Alcohol Use Disorder Identification Test—Consumption [AUDIT–C].	N/A	72109–2	N/A.

Domain	Question(s) [LOINC® name]	Answer(s) [LOINC® answer code]	LOINC® Codes for question-answer list combination	LOINC® Answer list ID
	How often do you have a drink containing alcohol? [SAMHSA].	[a] Never [b] Monthly or less [c] 2–4 times a month [d] 2–3 times a week [e] 4 or more times a week	68518–0	LL2179–1.
	How many standard drinks containing alcohol do you have on a typical day? [SAMHSA].	[a] 1 or 2 [b] 3 or 4 [c] 5 or 6 [d] 7 to 9 [e] 10 or more	68519–8	LL2180–9.
	How often do you have six or more drinks on one occasion? [SAMHSA].	[a] Never [b] Less than monthly [c] Monthly [d] Weekly [e] Daily or almost daily	68520–6	LL2181–7.
	[Total score [AUDIT–C]]	N/A[61]		N/A.
Social Connection and Isolation (NHANES III).	Are you married or living together with someone in a partnership at the time of questioning? In a typical week, how many times do you talk on the telephone with family, friends, or neighbors? How often do you get together with friends or relatives? How often do you attend church or religious services? How often do you attend meetings of the clubs or organizations you belong to?	For example, these categories form an ordinal scale assessing the number of types of social relationships on which a person is connected and not isolated, and has standard scoring. Individuals receive one point for each of the following: Being married or living together with someone in a partnership at the time of questioning, averaging three or more social interactions per week (assessed with questions one and two, above), reporting attending church or other religious services more than four times per year (assessed with question three, above), and reporting that they belong to a club or organization (assess with question four, above). A score of 0 represents the highest level of social isolation and a score of 4 represents the lowest level of social isolation.[62]	LOINC® code pending.	LOINC® code pending.
Exposure to violence: Intimate partner violence (HARK 4Q).	Within the last year, have you been humiliated or emotionally abused in other ways by your partner or ex-partner? Within the last year, have you been afraid of your partner or ex-partner? Within the last year, have you been raped or forced to have any kind of sexual activity by your partner or ex-partner? Within the last year, have you been kicked, hit, slapped, or otherwise physically hurt by your partner or ex-partner?	Pending	LOINC® code pending.	LOINC® code pending.

We propose to require that a Health IT Module enable a user to record, change, and access a patient's sexual orientation and gender identity as part of this certification criterion. We propose that sexual orientation be coded in accordance with, at a minimum, the September 2014 Release of the U.S. Edition of SNOMED CT®[63] and HL7 Version 3 attributed as follows:

[56] The answer is then scored from a scale of 1 (very hard) to 3 (not at all), and unknown answers are scored as a negative number.

[57] LOINC® Component used for the table.

[58] Elo, A.-L., A. Leppänen, and A. Jahkola. 2003. Validity of a single-item measure of stress symptoms. *Scandanavian Journal of Work, Environment & Health* 29(6):444–451.

[59] Note that LOINC® provides a translation table at *https://loinc.org/downloads/usage/units* that enumerates the UCUM syntax for a subset of UCUM codes that are commonly used in health IT that may be a useful reference for stakeholders.

[60] Note that LOINC® provides a translation table at *https://loinc.org/downloads/usage/units* that enumerates the UCUM syntax for a subset of UCUM codes that are commonly used in health IT that may be a useful reference for stakeholders.

[61] The Alcohol Use Disorders Identification Test C (AUDIT–C) is scored on a scale of 0 to 12. Each of the three AUDIT–C questions has 5 answer choices with points ranging from 0 to 4. A screen is considered positive for unhealthy alcohol use or hazardous drinking if the AUDIT–C score is 4 or more points for men or 3 or more points for women.

[62] Pantell et al., 2013.

Sexual orientation	Code
Homosexual	SNOMED CT® 38628009.
Heterosexual	SNOMED CT® 20430005.
Bisexual	SNOMED CT® 42035005.
Other	HL7 V3 nullFlavor OTH.
Asked but unknown	HL7 V3 nullFlavor ASKU.
Unknown	HL7 V3 nullFlavor UNK.

We propose that gender identity be coded in accordance with, at a minimum, the September 2014 Release of the U.S. Edition of SNOMED CT®[64] and HL7 Version 3 attributed as follows:

Gender identity	Code
Identifies as male gender.	SNOMED CT® 446151000124109.*
Identifies as female gender.	SNOMED CT® 446141000124107.*
Female-to-male transsexual.	SNOMED CT® 407377005.
Male-to-female transsexual.	SNOMED CT® 407376001.
Identifies as non-conforming gender.	SNOMED CT® 446131000124102.*
Other	HL7 V3 nullFlavor OTH.
Asked but unknown	HL7 V3 nullFlavor ASKU

*These new concepts will appear in the March 2015 release of the U.S. Edition of SNOMED CT® and are now viewable at *https://uscrs.nlm.nih.gov/main.xhtml.*

We note that the functionality under consideration to record the data discussed above has no bearing on whether a patient chooses to provide this information or whether a health care provider chooses to record the information or would be required to do so through the EHR Incentive Programs or other programs. However, we believe the structured recording of these types of data as described is the best available method for reliably capturing and maintaining accurate reflections of this information. For this proposed certification criterion, we seek comment on whether:

- The appropriate measures have been included for the listed social, psychological, and behavioral data;
- There should be standardized questions associated with the collection of sexual orientation and gender identity data (and if so, what vocabulary standard would be best suited for coded these standardized questions);
- We should set a minimum number of data measures for certification (*e.g.,* at a minimum: One, 3, or all); and
- These measures should be part of one certification criterion or separate certification criteria. We note that our proposal for an ‘‘Open Data Certified Health IT Products List,’’ as discussed in section IV.D.3 of this preamble, would result in more granular identification of certified health IT. Specific to this criterion, the CHPL would include information regarding each of the data measures (*e.g.,* education, depression, and sexual orientation) that were certified as part of a Health IT Module's certification to this criterion.

Work Information—Industry/Occupation Data

The Institute of Medicine identified patients' work information as valuable data that could be recorded by health IT and used by both health care providers and public health agencies.[65] Similarly, the 2012 HHS Environmental Justice Strategy and Implementation Plan echoed the potential benefits of having work information in EHR technology.[66] The combination of industry and occupation (I/O) information provides opportunities for health care providers to improve patient health outcomes—for health issues wholly or partially caused by work and for health conditions whose management is affected by work. For example, ‘‘Usual’’ (longest-held) I/O information can be key for health care improvement and population-based health investigations, and is already a required data element for cancer reporting.[67] Health care providers also can use current I/O information to assess symptoms in the context of work activities and environments, inform patients of risks, obtain information to assist in return-to-work determinations, and evaluate the health and informational needs of groups of patients.

Since publication of the Voluntary Edition proposed rule (79 FR 10924) in which we requested comment on I/O information for the purposes of certification, we have considered health IT developer feedback on the need to adopt consensus standards for capturing I/O information in health IT and continue to work with the National Institute for Occupational Health and Safety (NIOSH) to explore avenues to record I/O data in health IT. NIOSH also continues to work with various industry stakeholders and health IT developers to assess the incorporation of patient I/O fields into commercial EHRs, develop occupationally related CDS, and to investigate practices and systems to achieve accurate, automated coding of I/O information. Given the value of I/O information as noted above and the progress being made by NIOSH and others, we are making a refined request for comments as part of a future edition of certification criteria. We invite commenters to consider what additional support might be needed for health IT developers, implementers, and users to effectively include a certification criterion that would require health IT to enable a user to record, change, and access (all electronically) the following data elements in structured format:

- Patients' employment status and primary activities (*e.g.,* volunteer work);
- Patients' current I/O, linked to one another and with time-stamp, including start date;
- Patients' usual I/O, linked to one another and with time-stamp, including start year and duration in years; and
- Patients' history of occupation with a time and date stamp for when the history was collected (to note, this is focused on the capability to record a history, not a requirement that a history must be recorded or that a patient history be recorded for a certain historical period of time).

We solicit public comment on the experience health IT developers and health care providers have had in recording, coding, and using I/O data. This would include any innovation that is making I/O data more useful for providers.

To better understand the health care needs associated with work data, we specifically solicit public comment from *health care providers, provider*

[63] We refer readers to section III.A.2.d (‘‘Minimum Standards’’ Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our proposal to adopt the September 2014 Release (U.S. Edition), or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

[64] We refer readers to section III.A.2.d (‘‘Minimum Standards’’ Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our proposal to adopt the September 2014 Release (U.S. Edition), or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

[65] IOM (Institute of Medicine). 2011. ‘‘Incorporating Occupational Information in Electronic Health Records: A Letter Report’’. Available at: *http://www.nap.edu/catalog.php?record_id=13207.*

[66] U.S. Department of Health and Human Services. February, 2012. 2012 HHS Environmental Justice Strategy and Implementation Plan. Available at: *http://www.hhs.gov/environmentaljustice/strategy.html.*

[67] CDC (2) (Centers for Disease Control and Prevention). 2012. Implementation Guide for Ambulatory Healthcare Provider Reporting to Central Cancer Registries, HL7 Clinical Document Architecture (CDA) Release 1.0, August 2012. Available at: *http://www.cdc.gov/phin/library/guides/Implementation_Guide_for_Ambulatory_Healthcare_Provider_Reporting_to_Central_Cancer_Registries_August_2012.pdf.*

organizations, and patients on the following:

- The usefulness for providers to be able to access current and usual I/O and related data in the EHR, including whether additional data elements, such as work schedule, are useful.
- The usefulness of a history of positions provided as current I/O, with data from each position time-stamped, linked, retained, and accessible as part of the longitudinal patient care (medical) record.
- Narrative text (vs. codes) for both current and usual I/O.
- CDC_Census codes for both current and usual I/O; available through PHIN VADS at *https://phinvads.cdc.gov/vads/SearchVocab.action.*
- SNOMED CT® codes for occupation (current codes or potentially developed codes).
- Other standards and codes that may be in use by the health IT industry for both current and usual I/O.

U.S. Uniformed/Military Service Data

In the Voluntary Edition proposed rule (79 FR 10924), we outlined rationale for a potential certification criterion that would assess the capability of health IT to enable a user to record, change, and access U.S. military service or all uniformed service (including commissioned officers of the U.S. Public Health Service (USPHS) and the National Oceanographic and Atmospheric Administration (NOAA) as they too are eligible for military health services, veterans benefits, and related services). We reiterate the rationale here as we continue to believe it is persuasive for adopting such a certification criterion. In recent years, U.S. Military service members have been returning from service in Iraq and Afghanistan and other various combat duty stations. A portion of these service members are returning with traumatic brain injuries, major limb injuries, and diagnoses of post-traumatic stress disorder as reported by the Department of Defense and Department of Veterans Affairs. We believe recording U.S. uniformed/military service information can have many benefits. It can help in identifying epidemiological risks for patients such as those noted above. It can assist in ensuring that a patient receives all the health care benefits he or she is entitled to by alerting medical professionals to the patient's service history, which can facilitate the coordination of benefits. This information can also increase the ability to assemble a longitudinal record of care for a U.S. service member, such as by requesting or merging of a patient's electronic health record stored by the Department of Defense, Veteran's Health Administration, and/or another health care provider.

In response to the request for comment on a ‘‘U.S. uniformed/military service’’ certification criterion in the Voluntary Edition proposed rule, commenters indicated that vocabulary standards for capturing such history may not be mature enough yet. Specifically, commenters noted that SNOMED CT ® currently has relevant codes, such as ‘‘history relating to military service,’’ and ‘‘duration of military service,’’ but not codes to cover all potential military service statuses, capture military service in an unambiguous way (*e.g.,* capturing current employed as well as history of military service) and military service in foreign locales. To improve coding of military and all uniformed history, we believe a promising path forward would be to add codes to the U.S. Extension of SNOMED–CT ®. Therefore, we request comment on the following:

- Whether a potential certification criterion should be focused solely on U.S. military service or all uniformed service members (*e.g.,* commissioned officers of the USPHS and NOAA);
- Whether the U.S. Extension of SNOMED–CT ® is the most appropriate vocabulary code set or whether other vocabulary code sets may be appropriate; and
- The concepts/values we should use to capture U.S. military service or all uniformed service status. We ask commenters to consider the work of NIOSH on I/O information as it relates to capturing military service.

Other Social, Psychological, and Behavioral Data

We seek comment on whether there are additional social, psychological, and behavioral data that we should include for certification as well as the best available standards for representing such data.

- *Decision Support—Knowledge Artifact*

2015 Edition Health IT Certification Criterion

§ 170.315(a)(22) (Decision support—knowledge artifact)

We propose a new ‘‘decision support—knowledge artifact’’ certification criterion in the 2015 Edition for technology to electronically send and receive clinical decision support knowledge artifacts in accordance with a Health eDecisions (HeD) standard.

A previous ONC-sponsored S&I initiative, HeD, defined two use cases (UC) with the goals of expressing CDS interventions in a standardized format for sharing (UC 1) and requesting/receiving knowledge artifacts from a CDS service provider (UC 2). We discuss UC 2 further in the proposal for a 2015 Edition ‘‘decision support—service’’ certification criterion in this section of the preamble. HeD UC 1 defined the functional requirements needed to build a standard schema for the contents of three ‘‘CDS Knowledge Artifact’’ [68] types: event condition action (ECA) rules, order sets, and documentation templates.[69] UC 1 was based on the scenario of a ‘‘CDS Knowledge Artifact supplier’’ making a computable CDS Knowledge Artifact available to a ‘‘CDS Artifact integrator.’’ For example, in accordance with the HeD standard, health IT could automatically integrate medication order sets based on best practice clinical guidelines in a machine-readable format without the need for human interpretation.

In the Voluntary Edition proposed rule, we proposed to adopt the HL7 Implementation Guide: Clinical Decision Support Knowledge Artifact Implementation Guide, Release 1 (January 2013) (‘‘HeD standard’’).[70] We stated that the HeD standard would greatly assist the industry in producing and sharing machine-readable files for representations of clinical guidance. We did not adopt the HeD standard as we agreed with commenters that more clarity is needed regarding the HeD proposals (79 FR 54453).

As the HeD initiative has completed, a new S&I initiative has launched, the Clinical Quality Framework (CQF), which builds on the HeD work and expands the scope to harmonize both CDS and electronic clinical quality measurement (eCQM) standards. The CQF initiative has created an updated and more modular HeD implementation guide for sharing CDS artifacts, HL7 Version 3 Standard: Clinical Decision Support Knowledge Artifact Specification, Release 1.2 DSTU (July 2014).[71] The modularity allows for portions of the HeD standard Release 1.2 to be updated without requiring updates

[68] A CDS Knowledge Artifact is the encoding of structured CDS content as a rule to support clinical decision making in many areas of the health care system, including quality and utilization measures, disease outbreaks, comparative effectiveness analysis, efficacy of drug treatments, and monitoring health trends.

[69] HL7 Implementation Guide: Clinical Decision Support Knowledge Artifact Implementation Guide, Release 1 (January 2013) (‘‘HeD standard'').

[70] *http://wiki.siframework.org/file/detail/implementation_guide_working_final_042413_lse_uploaded-1.docx.*

[71] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=337.*

to the entire standard. As the CQF work continues, this more recent standard will be leveraged heavily to produce a harmonized clinical quality expression language for both CDS and eCQMs.

We continue to believe that the HeD standard would greatly assist the industry in producing and sharing machine readable files for representations of clinical guidance. We therefore propose to adopt the HL7 Version 3 Standard: Clinical Decision Support Knowledge Artifact Specification, Release 1.2 DSTU (July 2014) (''HeD standard Release 1.2'') at § 170.204(d)(1) and offer testing and certification for health IT demonstrate it can electronically send and receive a CDS artifact formatted in the HeD standard Release 1.2.

We solicited comment in the Voluntary Edition proposed rule on what we should test and certify to when it comes to testing and certification for acceptance and incorporation of CDS Knowledge Artifacts (79 FR 54453). Commenters suggested that we focus testing on a few types of CDS Knowledge Artifacts, but not on all possible types included in the HeD standard. We note that HHS is developing publicly available CDS interventions in HL7 draft standard formats,[72] including the HeD standard Release 1.2, that will be available at *www.ushik.org.* We welcome comment on specific types of CDS Knowledge Artifacts on which we should focus testing and certification to the HeD standard Release 1.2. We also invite comments on versions of standards we should consider as alternative options, or for future versions of this certification criterion, given the ongoing work to harmonize CDS and quality measurement standards as discussed under the ''CQM—record and export'' certification criterion later in this section of the preamble.

- *Decision Support—Service*

2015 Edition Health IT Certification Criterion
§ 170.315(a)(23) (Decision support—service)

We propose a new ''decision support—service'' certification criterion in the 2015 Edition for technology to electronically make an information request with patient data and receive in return electronic clinical guidance in accordance with the standard in accordance with an HeD standard.

A previous ONC-sponsored S&I initiative, HeD, defined two use cases (UC) with the goals of expressing CDS interventions in a standardized format for sharing (HeD UC 1) and requesting/receiving knowledge artifacts from a CDS service provider (HeD UC 2). We discuss HeD UC 1 further in the proposal for a 2015 Edition ''decision support—knowledge artifact'' certification criterion above. HeD UC 2 defines the interface requirements needed to send patient data and receive CDS guidance based on one scenario: a request for clinical guidance made to a CDS guidance supplier. The HeD S&I initiative considered the following interactions with a CDS guidance supplier: Drug dosing calculation; immunization forecasting; disease management; quality measure evaluation; transition of care support; test appropriateness scores (*e.g.,* radiology tests); prediction rule evaluation (*e.g.,* APACHE score, AHRQ Pneumonia Severity Index); and severity of illness assessment (*e.g.,* Charlson Index). The HeD initiative created the HL7 Implementation Guide: Decision Support Service, Release 1—US Realm DSTU (January 2014) (''Decision Support Service IG''),[73] which defines SOAP and REST web service interfaces for CDS guidance services.

We proposed to adopt the Decision Support Service IG in the Voluntary Edition proposed rule because the implementation of this IG would promote systems whereby a health care provider can send a query about a patient to a CDS guidance supplier and receive CDS guidance back in near real-time. Although we received general support for adopting the Decision Support Service IG, we did not adopt it because the 2014 Edition Release 2 final rule focused on the adoption and revision of a small number of 2014 Edition certification criteria that add flexibility and make improvements to the existing set of 2014 Edition certification criteria.

We are aware of a more recent release of the Decision Support Service IG, HL7 Implementation Guide: Decision Support Service, Release 1.1 (March 2014), US Realm DSTU Specification (''Release 1.1'').[74] Release 1.1 utilizes the latest available version of the HL7 Virtual Medical Record specification. Given the general support we received in the Voluntary Edition proposed rule, we propose to adopt the HL7 Implementation Guide: Decision Support Service, Release 1.1 (March 2014), US Realm DSTU Specification at § 170.204(e)(1) and offer testing and certification for health IT to demonstrate the ability to send and receive electronic clinical guidance according to the interface requirements defined in Release 1.1. We also invite comments on versions of standards we could consider as alternative options, or for future versions of this certification criterion, given the ongoing work to harmonize CDS and quality measurement standards as discussed under the ''CQM—record and export'' certification criterion later in this section of the preamble.

- *Transitions of Care*

2015 Edition Health IT Certification Criterion
§ 170.315(b)(1) (Transitions of care)

We propose to adopt a 2015 Edition certification criterion for ''transitions of care'' (ToC) that is a continuation and extension of the ToC certification criterion adopted as part of the 2014 Edition Release 2 final rule at § 170.314(b)(8). This proposed criterion also reflects the corresponding structural and clarifying changes that we adopted in the 2014 Edition Release 2 final rule that correspond to ''clinical information reconciliation and incorporation'' certification criterion also adopted as part of the 2014 Edition final rule.

Accordingly, the 2015 Edition ToC certification criterion we propose to adopt would include many of the same capabilities adopted at § 170.314(b)(8) with the exception of the following revisions and additions.

Updated C–CDA Standard

As expressed in the 2014 Edition final rule, the C–CDA standard is now the single standard permitted for certification and the representation of summary care records. It is also referenced in other proposed 2015 Edition certification criteria. Industry stakeholders have continued to work to improve and refine the C–CDA standard since the 2014 Edition final rule, including publishing additional guidance for its consistent implementation.[75] An updated version, HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft

[72] This site may also include CDS interventions formatted to the Quality Improvement and Clinical Knowledge Model (QUICK) standard which we discuss in the preamble for the ''Clinical quality measures—record and export'' certification criterion.

[73] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=334.*

[74] *http://www.hl7.org/documentcenter/public/standards/dstu/HL7_DSS_IG%20_R1_1_2014MAR.zip.*

[75] *http://wiki.siframework.org/Companion+Guide+to+Consolidated+CDA+for+MU2.*

Standard for Trial Use, Release 2.0,[76] which was balloted through 2014, includes the following changes, which we believe provide important clarifications and enhancements:

- Addition of new structural elements: new document sections and data entry templates:
  - ○ New Document Templates for: Care Plan; Referral Note; Transfer Summary.
  - ○ New Sections for: Goals; Health Concerns; Health Status Evaluation/Outcomes; Mental Status; Nutrition; Physical Findings of Skin.
  - ○ New organizers and many new entries (*e.g.* Wound Observation).
- Some sections/entries were deprecated (*i.e.,* should no longer be used).
- Updates to (versioning of) template/section/entry object identifiers (OIDs).
  - ○ This includes a new chapter describing HL7's approach to template versioning.
- Tighter data constraints/requirements.
  - ○ For example, some data elements with a ''MAY'' requirement now have a ''SHOULD'' requirement. Likewise, some with a ''SHOULD'' requirement now have a ''MUST'' requirement.
- Updated Vocabulary/Value Set constraints.
  - ○ For example: two SNOMED CT ® codes were added to the Current Smoking Status value set and the Tobacco Use value set to support the 2014 Edition vocabulary requirements for patient smoking status.
  - ○ NLM's Value Set Authority Center (VSAC) was named as reference for Value Sets used in C–CDA.

In the Voluntary Edition proposed rule, we proposed to adopt the C–CDA Release 2.0 standard and reference its use in the other certification criteria in which this standard would have also been applicable. At the time of that proposal, the C–CDA Release 2.0 had not yet completed its balloting cycle within HL7 and stakeholder comments on the Voluntary Edition proposed rule expressed concern related to the C–CDA Release 2.0 standard's stability. Given that the C–CDA Release 2.0 has completed balloting and is now published as the next C–CDA version, we believe that the continued attention it received through HL7 balloting has resulted in a standard that is the best available for adoption in this proposed rule and for future implementation in the coming years. Thus, we propose to adopt C–CDA Release 2.0 at § 170.205(a)(4) as part of this certification criterion. We note that compliance with the C–CDA Release 2 cannot include the use of the ''unstructured document'' document-level template for certification to this criterion.

To address a technical implementation challenge sometimes referred to as ''bilateral asynchronous cutover,'' (which is meant to convey the complexity of continued interoperability among exchange partners as each upgrades their health IT at different times and with different standards capabilities), we propose that the 2015 Edition ToC certification criterion reference both the C–CDA Release 1.1 and Release 2.0 standards. In other words, a Health IT Module presented for certification to this criterion would need to demonstrate its conformance and capability to create and parse both versions (Release 1.1 and 2.0) of the C–CDA standards. Under this proposal, the sending Health IT Module would send two documents (one conforming to C–CDA R1.1 and other conforming to C–CDA R2.0) and the receiving Health IT Module would receive both versions of the documents and choose the appropriate version for downstream processing.

While we recognize that this proposal is not ideal, we have proposed this more conservative approach as a way to mitigate the potential that there would be interoperability challenges for ToC as different health care providers adopt Health IT Modules certified to the 2015 Edition criterion at different times that include C–CDA Release 2.0 capabilities. However, we request public comment, especially from health IT developers with experience implementing the C–CDA, on an alternative approach related to the creation of C–CDA-formatted documents. The alternative approach would be focused on C–CDA creation and receipt capabilities related to whether the health IT system could produce one, ''dually compliant,'' C–CDA that addresses both C–CDA versions at once. We understand that this approach is possible, may be preferred from an implementation perspective, and could help prevent potential data duplication errors that could result if a Health IT Module is required to be able to produce two separate C–CDA files (one in each version) as part of certification.

Our proposal to adopt C–CDA Release 2.0 is applicable to all of the other certification criteria in which the C–CDA is referenced. Similarly, unless C–CDA Release 2.0 is explicitly indicated as the sole standard in a certification criterion, we propose to reference both C–CDA versions in each of these criteria for the reasons just discussed.

Valid/Invalid C–CDA System Performance

As we considered stakeholder feedback and reviewed the additional public dialogue surrounding the variability of CEHRT in recognizing valid/invalid documents formatted according to the C–CDA 1.1 standard, including structured content by different health IT developers,[77] we recognized that an expanded ToC certification criterion with a specific capability focused principally on health IT system behavior and performance related to recognizing valid/invalid C–CDAs would be beneficial. Thus, we propose to include within the 2015 Edition ToC certification criterion a specific focus on this technical system behavior. We believe this type of error checking and resilience is an important and necessary technical prerequisite in order to ensure that as data in the system is parsed from a C–CDA for incorporation as part of the ''clinical information reconciliation and incorporation'' certification criterion the user can be assured that the system has appropriately interpreted the C–CDA it received. Further, we believe this level of rigorous testing will better enable Health IT Modules to properly recognize C–CDA-based documents and prepare the necessary information for reconciliation and other workflow needs.

We propose that this specific aspect of the certification criterion would focus on and require the following technical outcomes be met. The Health IT Module would need to demonstrate the ability to detect valid and invalid C–CDA documents, including document, section, and entry level templates for data elements specified in 2014 and 2015 edition. Specifically, this would include:

- The ability of the Health IT Module to detect invalid C–CDA documents. Thus, any data in the submitted C–CDA document that does not conform to either the C–CDA 1.1 or 2.0 standard (in addition to data coding requirements specified by this regulation) would be considered invalid;
- The ability to identify valid C–CDA document templates (*e.g.,* CCD, Discharge Summary, Progress Note) and process the required data elements, section and entries, specific to the document templates and this regulation.
- The ability to detect invalid vocabularies and codes not specified in

[76] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=379.* Access to the IG is freely available for review during the public comment period by establishing an HL7 user account.

[77] D'Amore JD, et al. J Am Med Inform Assoc 2014;21:1060–1068.

either the C–CDA 1.1 or 2.0 standard or required by this regulation (*e.g.,* using a SNOMED CT ® code where a LOINC ® code is required or using a code which does not exist in the specified value set).

- The ability to correctly interpret empty sections and nullFlavor combinations per the C–CDA 1.1 or 2.0 standard. For example, we anticipate testing could assess a Health IT Module's ability to continue to process a C–CDA when a nullFlavor is used at the section template level.

We expect these capabilities would be tested by providing several C–CDA documents with valid and invalid data. We do not expect Health IT Modules presented for certification to have a common C–CDA handling process, however, we do expect that they would have a baseline capability to identify valid and invalid C–CDA documents and prepare the necessary data for clinical information reconciliation and incorporation. Further, we expect that Health IT Modules will have some mechanism to track errors encountered when assessing received C–CDA's and we have proposed that health IT be able to track the errors encountered and allow for a user to be notified of errors or review the errors produced. The Health IT Module would not need to support both and how this technical outcome is accomplished is entirely up to the health IT developer.

We direct readers to the proposed ''Consolidated CDA creation performance'' certification criterion (§ 170.315(g)(6)) under which we seek comment on a potential requirement for this certification criterion or the ''Consolidated CDA creation performance'' certification criterion that would evaluate the completeness of the data included in a C–CDA in order to ensure that the data recorded by health IT is equivalent to the data included in a created C–CDA.

XDM Package Processing

As indicated in the earlier paragraphs, a Health IT Module presented for certification to this certification criterion will need to support one of the edge protocols referenced in the Edge IG version 1.1 (*i.e.,* the ''IHE XDR profile for Limited Metadata Document Sources'' edge protocol or an SMTP-focused edge protocol (SMTP alone or SMTP in combination with either IMAP4 or POP3)). However industry feedback has indicated that the use of XDM packages has grown within the stakeholder community using Direct, which most often happens when Edge System A using XDR sends content and metadata to its HISP–A, who in turn packages that content and metadata into an XDM ZIP and sends it within a Direct message to HISP–B, which then ultimately sends the message containing the XDM package to Edge System B using an SMTP-based edge.

Therefore, if Edge System B does not support XDM package processing, interoperability could be impacted when HISP–B forwards XDM packages to Edge System B via the SMTP protocol. To mitigate this potential incompatibility, we propose to include a specific capability in this certification criterion that would require a Health IT Module presented for certification that is also being certified to the SMTP-based edge to demonstrate its ability to accept and process an XDM package it receives, which would include extracting relevant metadata and document(s). That is, this additional requirement only applies to a Health IT Module presented for certification with an SMTP-based edge implementation and not an XDR edge implementation). Additionally, because we expect XDM packaging to be created in accordance with the specifications included in IHE IT Infrastructure Technical Framework Volume 2b (ITI TF–2b),[78] we propose to adopt this as the standard (at § 170.205(p)(1)) for assessing whether the XDM package was successfully processed.

Common Clinical Data Set

We propose to include an updated Common Clinical Data Set for the 2015 Edition that includes references to new and updated vocabulary standards code sets. Please also see the Common Clinical Data Set definition proposal in section III.B.3 of this preamble.

Encounter Diagnoses

For encounter diagnoses, we are carrying over the requirement from the 2014 Edition ''ToC'' certification criterion that a Health IT Module must enable a user to create a transition of care/referral summary that also includes encounter diagnoses using either SNOMED CT ® (September 2014 Release of the U.S. Edition as a baseline for the 2015 Edition) or ICD–10 codes.

''Create'' and Patient Matching Data Quality

In 2011, both the HITPC and HITSC made recommendations to ONC on patient matching. The HITPC made recommendations in the following five categories: Standardized formats for demographic data fields; internally evaluating matching accuracy; accountability; developing, promoting and disseminating best practices; and supporting the role of the individual/patient.[79] The HITSC made the following four recommendations: Detailing patient attributes that could be used for matching (in order to understand the standards that are needed); data quality; formats for these data elements; and what data are returned from a match request.[80] The standards recommended by the HITSC are as follows:

- *Basic Attributes:* Given Name; Last Name; Date of Birth; Administrative Gender.[81]
- *Other Attributes:* Insurance Policy Number; Medical Record Number; Social Security Number (or last 4 digits); Street Address; Telephone Number; Zip Code.
- *Potential Attributes:* Email Address; Voluntary Identifiers; Facial Images; Other Biometrics.

In July 2013, ONC launched an initiative to reinvigorate public discussion around patient matching, to perform a more detailed analysis of patient matching practices, and to identify the standards, services, and policies that would be needed to implement the HITPC and HITSC's recommendations. The initiative's first phase focused on a common set of patient attributes that could be leveraged from current data and standards referenced in our certification criteria. Given the initial findings, we proposed to include a limited set of standardized data as a part of the ''Create'' portion of the ToC criterion in the Voluntary Edition proposed rule to improve the quality of the data included in outbound summary care records. Overall, the vast majority of commenters supported the proposed policy that standardized patient attributes should be required for use in as part of the transitions of care certification criterion. Commenters overwhelmingly supported the inclusion of the proposed constrained specifications for last name/family name, maiden name, suffix, first/given name, middle/second name, maiden name, date of birth, current address and historical address, phone number, and sex in support of patient matching. However, given our approach in the 2014 Edition Release 2 final rule

[78] *http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol2b_FT_2010-08-10.pdf.*

[79] *http://www.healthit.gov/sites/default/files/hitpc-transmittal-letter-priv-sectigerteam-020211.pdf.*

[80] *http://www.healthit.gov/FACAS/sites/default/files/standards-certification/8_17_2011Transmittal_HITSC_Patient_Matching.pdf.*

[81] Despite its inclusion of the word ''gender,'' ''Administrative Gender'' is generally used in standards to represent a patient's ''sex,'' such as male or female. See: *http://ushik.ahrq.gov/ViewItemDetails?system=hitsp&itemKey=83680000.*

to only adopt a small subset of the proposed certification criteria to provide flexibility, clarity, and enhance health information exchange, we decided not adopted this proposal.

We again propose to include a limited set of standardized data as a part of the ''Create'' portion of the ToC criterion in the 2015 Edition to improve the quality of the data included in outbound summary care records. To be clear, this proposal does *not* require a Health IT Module to capture the data upon data entry, but rather at the point when the data is exchanged (an approach commonly used for matching in HL7 transactions, IHE specifications,[82] C–CDA specification, and the eHealth Exchange). The proposed standardized data include: first name, last name, middle name (including middle initial), suffix, date of birth, place of birth, maiden name, phone number, and sex. In the bulleted list below, we identify more constrained specifications for some of the standardized data we propose. Based on our own research, we do not believe that the proposed constraints to these data conflict with the C–CDA. That being said, some proposed constraints may further restrict the variability as permitted by existing specifications and others may create new restrictions that do not currently exist within the C–CDA. We propose that:

- For ''last name/family name'' the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0 [83] (which addresses whether suffix is included in the last name field) be followed.
- For ''suffix,'' that the suffix should follow the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0 (JR, SR, I, II, III, IV, V, RN, MD, Ph.D., ESQ) [84] and that if no suffix exists, the field should be marked as null.
- For ''date of birth,'' that the year, month and date of birth should be required fields while hour, minute and second should be optional fields. If hour, minute and second are provided then either time zone offset should be included unless place of birth (city, region, country) is provided; in the latter local time is assumed. If date of birth is unknown, the field should be marked as null.
- For ''phone numbers,'' the ITU format specified in ITU–T E.123 [85] and ITU–T E.164 [86] be followed and that the capture of home, business, and cell phone numbers be allowed.[87] Further, that if multiple phone numbers are present in the patient's record, all should be included in the C–CDA and transmitted.
- For ''sex'' we propose to require developers to follow the HL7 Version 3 Value Set for Administrative Gender and a nullFlavor value attributed as follows: M (Male), F (Female), and UNK (Unknown).

While the Patient Matching Initiative's recommendations included standardizing current and historical address, we have not included a specific standardized constraint for that data at this time due to a lack of consensus around the proper standard. In response to the Voluntary Edition proposed rule, commenters also suggested that we delay support for international standards for address until future editions of certification criteria. To reiterate, the data we propose for patient matching would establish a foundation based on leveraging current data and standards in certification criteria. We welcome comments on this approach and encourage health IT developers to consider and support the use other patient data that would improve patient matching for clinical care and many types of clinical research.

Direct Best Practices

In the past couple of years we have heard feedback from stakeholders regarding health IT developers limiting the transmission or receipt of different file types via Direct. We wish to remind all stakeholders of the following best practices for the sharing of information and enabling the broadest participation in information exchange with Direct: *http://wiki.directproject.org/Best+Practices+for+Content+and+Workflow.*

Certification Criterion for C–CDA and Common Clinical Data Set Certification

We note that no proposed 2015 Edition health IT certification criteria includes just the C–CDA Release 2.0 and/or the Common Clinical Data Set, particularly with the 2015 Edition not including a proposed ''clinical summary'' certification criterion as discussed later on in this preamble. Health IT certified to simply the C–CDA Release 2.0 with or without certification to the Common Clinical Data Set may be beneficial for other purposes, including participation in HHS payment programs. We request comment on whether we should adopt a separate 2015 Edition health IT certification criterion for the voluntary testing and certification of health IT to the capability to create a summary record formatted to the C–CDA Release 2.0 with or without the ability to meet the requirements of the Common Clinical Data Set definition.

C–CDA Data Provenance Request for Comment

As the exchange of health data increases, so does the demand to track the provenance of this data over time and with each exchange instance. Confidence in the authenticity, trustworthiness, and reliability of the data being shared is fundamental to robust privacy, safety, and security enhanced health information exchange. The term ''provenance'' in the context of health IT refers to evidence and attributes describing the origin of electronic health information as it is captured in a health system and subsequently persisted in a way that supports its lifespan. As described in the President's Council of Advisors on Science and Technology (PCAST) Report ''Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans'' [88], provenance includes information about the data's source and the processing that the data has undergone. The report refers to ''tagged data elements'' as units of data accompanied by a ''metadata tag'' that describes the attributes, provenance, and required security protections of the data.

In April 2014, ONC launched the Data Provenance Initiative within the Standards and Interoperability (S&I) Framework to identify the standards necessary to capture and exchange provenance data, including provenance at time of creation, modification, and time of exchange.[89] The stakeholder community represented a wide variety of organizations including health IT developers; federal, state, and local agencies; healthcare professionals; research organizations; payers; labs; and individuals within academia. In the fall of 2014, the HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) (DSTU) [90] was published. This IG

[82] *http://www.ihe.net/Technical_Frameworks/.*

[83] *http://www.caqh.org/pdf/CLEAN5010/258-v5010.pdf.*

[84] *http://www.caqh.org/pdf/CLEAN5010/258-v5010.pdf.*

[85] *http://www.itu.int/rec/T-REC-E.123-200102-I/e.*

[86] *http://www.itu.int/rec/T-REC-E.164-201011-I/en.*

[87] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=186.*

[88] PCAST Report to the President: Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward, *http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.*

[89] *http://wiki.siframework.org/Data+Provenance+Initiative.*

[90] *http://wiki.hl7.org/index.php?title=HL7_Data_Provenance_Project_Space* and *http://*

clarifies existing content from various standards within HL7 [91] and describes how provenance information for a CDA document in a health IT system should be applied, and what vocabulary should be used for the metadata. This includes provenance metadata in the CDA at the header, section and entry levels. We seek comment on the maturity and appropriateness of this IG for the tagging of health information with provenance metadata in connection with the C–CDA. Additionally, we seek comment on the usefulness of this IG in connection with certification criteria, such as ToC and VDT certification criteria.

- *Clinical Information Reconciliation and Incorporation*

2015 Edition Health IT Certification Criterion
§ 170.315(b)(2) (Clinical information reconciliation and incorporation)

We propose to adopt a 2015 Edition ''clinical information reconciliation and incorporation'' certification criterion that is a revised (but largely similar to the 2014 Edition Release 2) version of the ''clinical information reconciliation and incorporation'' criterion adopted at § 170.314(b)(9).

Incorporation System Performance

As we considered public comments made after the 2014 Edition final rule and reviewed the additional public dialogue surrounding the variability of certified health IT in incorporating C–CDAs including structured content by different health IT developers [92], we recognized the need to expand the existing ''clinical information reconciliation and incorporation'' certification criterion to focus on health IT system behavior and performance related to incorporating C–CDAs including structured content. We believe that testing a Health IT Module's capability to reconcile and incorporate, at a minimum: problems, medications, and medication allergies from multiple C–CDAs will improve the overall clinical effectiveness.

We expect that testing for this specific system performance would include the ability to incorporate valid C–CDAs with variations of data elements to be reconciled (*e.g.*, documents with no medications, documents having variations of medication timing data). In addition we believe we can further strengthen this certification criterion by proposing to require that a C–CDA be created based on the reconciliation and incorporation process in order to validate the incorporation results. We anticipate that the generated C–CDA would be verified using test tools for conformance and can be checked against the information that was provided to incorporate.

Accordingly, we propose that the following technical system behavior and performance also be addressed as part of the clinical information reconciliation and incorporation certification criterion: The Health IT Module must demonstrate the ability to reconcile problem, medication, and medication allergy data from valid C–CDAs (both Release 1.1. and 2.0) with variations of data elements to be reconciled and then generate a conformant C–CDA document based on the reconciled information. For example, a test could include assessing a Health IT Module's capability to reconcile and incorporate medication information with different timing information.

- *Electronic Prescribing (e-Prescribing)*

2015 Edition Health IT Certification Criterion
§ 170.315(b)(3) (Electronic prescribing)

We propose to adopt a 2015 Edition certification criterion for e-prescribing that is revised in comparison to the 2014 Edition ''e-prescribing'' criterion (§ 170.314(b)(3)). First, for the purposes of certification, we propose to require a Health IT Module to be able to receive and respond to additional NCPDP SCRIPT Standard Implementation Guide Version 10.6 (v10.6) transactions or segments, namely Change Prescription, Refill Prescription, Cancel Prescription, Fill Status, and Medication History. Second, for the purposes of certification, we propose to require that a Health IT Module demonstrate that directions for medication use transmitted as e-prescriptions are codified in a structured format. Third, for the purposes of certification, we propose to require a Health IT Module be able to limit a user to e-prescribing all medications in the metric unit standard only, follow NCPDP-recommended conventions for use of leading zeroes before a decimal, and avoid use of trailing zeroes after a decimal when e-prescribed.

e-Prescribing Transactions or Segments

For 2014 Edition testing and certification to this criterion, a Health IT Module presented for certification must demonstrate that it can create a new prescription according to the NCPDP SCRIPT v10.6 New Prescription transaction (NEWRX). Stakeholders have recommended we consider expanding testing to a greater number of NCPDP SCRIPT v10.6 transactions and segments in order to better facilitate prescriber and pharmacist communications to provide better care for patients. Stakeholders have indicated that there is variable uptake and inconsistent implementation of the transactions in the NCPDP SCRIPT Standard v10.6 despite their added value for patient safety and improved communication between prescribers and pharmacists. In consideration of stakeholder input, we propose to include additional NCPDP SCRIPT v10.6 transactions in addition to the New Prescription transaction for health IT testing and certification. We propose that testing and certification would require a Health IT Module to demonstrate the ability to send and receive end-to-end prescriber-to-receiver/sender-to-prescriber transactions (bidirectional transactions). The transactions and reasons for inclusion for testing and certification are outlined in Table 3 below.

gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseBrowse&frs_package_id=240.

[91] Standards including HL7 Clinical Documentation Architecture Release 2 (CDA R2), HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, and HL7 Version 2 Vocabulary & Terminology Standards (all are normative standards).

[92] D'Amore JD, et al. J Am Med Inform Assoc 2014; 21:1060–1068.

Table 3—Proposed Additional[93] NCPDP SCRIPT v10.6 Transactions for Testing and Certification to e-Prescribing Certification Criterion

NCPDP SCRIPT v10.6 transaction or segment	Use case(s)	Problem addressed/value in testing for certification
Change Prescription (RXCHG, CHGRES).	• Allows a pharmacist to request a change of a new prescription or a "fillable" prescription. • Allows a prescriber to respond to pharmacy requests to change a prescription.	Facilitates more efficient, standardized electronic communication between prescribers and pharmacists for changing prescriptions.
Cancel Prescription (CANRX, CANRES).	• Notifies the pharmacist that a previously sent prescription should be canceled and not filled.	Facilitates more efficient, standardized electronic communication between prescribers and pharmacists for cancelling prescriptions. • Sends the prescriber the results of a prescription cancellation request.
Refill Prescription (REFREQ, REFRES).	• Allows the pharmacist to request approval for additional refills of a prescription beyond those originally prescribed. • Allows the prescriber to grant the pharmacist permission to provide a patient additional refills or decline to do so.	Facilitates more efficient, standardized electronic communication between prescribers and pharmacists for refilling prescriptions.
Fill Status (RXFILL)	Allows the pharmacist to notify the prescriber about the status of a prescription in three cases: 1) to notify of a dispensed prescription, 2) to notify of a partially dispensed prescription, 3) to notify of a prescription not dispensed.	Allows the prescriber to know whether a patient has picked up a prescription, and if so, whether in full or in part. This information can inform assessments of medication adherence.
Medication History (RXHREQ, RXHRES).	• Allows a requesting entity to generate a patient-specific medication history request. • The responding entity can respond with a patient's medication history, including source, fill number, follow-up contact, date range, as information is available.	Allows a requesting entity to receive the medication history of a patient. A prescriber may use this information to perform medication utilization review, medication reconciliation, or other medication management to promote patient safety.

We solicit comment on including the proposed transactions and segments for testing and certification to this certification criterion as outlined in Table 3, and on the problems addressed/value in testing for certification. We also solicit comment on the following issues:

- Other NCPDP SCRIPT v10.6 transactions that should be considered for testing and certification, and for what use cases/value;
- What factors we should consider for end-to-end prescriber-to-receiver testing.

We also propose to adopt and include the February 2, 2015 monthly version of RxNorm in this criterion as the baseline version minimum standards code set for coding medications (see section III.A.2.d (''Minimum Standards'' Code Sets) of this preamble).

Structured and Codified ''Sig''

Medications can be e-prescribed using a free text format, and typically the instructions include the medication name, dose, route of administration, frequency of administration, and other special instructions. This set of prescribing instructions is referred to as the ''Sig.'' In a free text format, non-standard or conflicting language may be used that is not understood by the pharmacist filling the prescription. Where systems do facilitate creation of the Sig, some systems may auto-concatenate the field length and thus the tail end of the Sig is lost. This has implications for communication between prescribers and pharmacists as well as for patient safety. Prescribers and pharmacists may have to engage in back-and-forth communication to clarify what is intended in the Sig instructions. Therefore, there is an opportunity to streamline prescriber-pharmacist communication, allow more time for direct activities of patient care, and reduce confusion during the pharmacy verification and dispensing processes.

We are aware that the NCPDP SCRIPT v10.6 standard includes structured Sig segments that are used to codify the prescribing directions in a structured format.[94] Providing Sig instructions in a structured format promotes accurate, consistent, and clear communication of the prescribing information as intended by the prescriber.

In one study of the structured and codified Sig within NCPDP SCRIPT v10.5, the Sig format fully represented 95% of ambulatory prescriptions tested.[95] While we believe that the results of this study give an indication of the scope of the structured and codified Sig within NCPDP SCRIPT v10.5, we note that the Sig standard was tested in the lab environment and not with live end-users. Stakeholders have also indicated the limitations of the structured and codified Sig within NCPDP SCRIPT v10.6 to represent all Sig instructions, particularly complex Sigs requiring multi-step directions. For example, stakeholders have noted that the Sig segment within the NCPDP SCRIPT v10.6 standard limits the field length to 140 characters whereas later versions of the NCPDP SCRIPT standard (from v201311 onward) have expanded the character length to 1000. Despite these potential limitations, we see standardizing and codifying the majority of routine prescriptions as a means to promote patient safety as well as reduce disruptions to prescriber workflow through a reduction in pharmacy call-backs.

We note the flexibility to create complex unstructured Sigs remains through use of existing e-prescribing workflow and appropriate use of the free text field. There is, however, low uptake of structured Sig according to the NCPDP SCRIPT v10.6 standard, which includes a combination of mandatory and conditional structured Sig segments.

We believe that medication Sig instructions should be codified in a

[93] We are proposing to keep the ''New Prescription'' transaction for testing and certification.

[94] NCPDP's Structured and Codified Sig Format Implementation Guide v1.2 is adopted within SCRIPT v10.6.

[95] Liu H, Burkhart Q and Bell DS. Evaluation of the NCPDP Structured and Codified Sig Format for e-prescriptions. J Am Med Inform Assoc. 2011 Sep–Oct;18(5):645–51.

structured format for the benefits outlined above. Therefore, we propose to require that a Health IT Module enable a user to enter, receive, and transmit codified Sig instructions in a structured format in accordance with NCPDP Structured and Codified Sig Format Implementation Guide v1.2 which is embedded within NCPDP SCRIPT v10.6 for certification to the e-prescribing criterion in the 2015 Edition.[96] We propose that this requirement apply to the New Prescription, Change Prescription, Refill Prescription, Cancel Prescription, Fill Status, and Medication History prescription transactions or segments as we understand that the NCPDP Structured and Codified Sig Format can be used for all NCPDP SCRIPT v10.6 prescription transactions that include the medication field. We also propose to require that a Health IT Module include all structured Sig segment components enumerated in NCPDP SCRIPT v10.6 (*i.e.,* Repeating Sig, Code System, Sig Free Text String, Dose, Dose Calculation, Vehicle, Route of Administration, Site of Administration, Sig Timing, Duration, Maximum Dose Restriction, Indication and Stop composites).

We are aware that NCPDP has recently published recommendations for implementation of the structured and Codified Sig format for a subset of component composites that represent the most common Sig segments in the NCPDP SCRIPT Implementation Recommendations Version 1.29.[97] We therefore welcome comment on this proposal, including whether we should require testing and certification to a subset of the structured and codified Sig format component composites that represent the most common Sig instructions rather than the full NCPDP Structured and Codified Sig Format Implementation Guide v1.2. As previously noted, prescribers would still be able to be able to create unstructured Sigs through the use of the free text field, and our proposal only discusses the capability of technology to enable a user to enter, receive, and transmit codified Sig instructions using the NCPDP Structured and Codified Sig Format.

Medication Dosing

In the Voluntary Edition proposed rule, we solicited comment on whether we should propose health IT certification for oral liquid medication dosing to the metric standard (*e.g.,* mL or milliliters) for patient safety reasons (79 FR 10926–10927). Use of the metric standard offers more precision in medication dose than the Imperial standard (*e.g.,* teaspoons), which can decrease preventable adverse drug events. A number of health care and standards developing organizations, including the AAP[98] and NCPDP,[99] support the use of the metric standard for dosing volumetric medications. Additionally, the FDA's Safe Use Initiative is working with CDC, NCPDP, and other stakeholders to encourage adoption of the NCPDP's recommendations for standardizing dosing designations on prescription container labels of oral liquid medications.[100] Recent research has demonstrated that parents who used milliliter-only dosing instruments were less likely to make dosing errors than parents who used teaspoons or tablespoon units.[101]

We received a number of comments to the comment solicitation. Many commenters noted that the structured Sig segment of the NCPDP SCRIPT Standard v10.6 supports use of the metric standard for liquid medication dosing. One ONC–ACB commented that in their experience, vendors have struggled to properly codify medication dosing information within the C–CDA in terms of consistency across all health IT systems. Many provider organizations and patient advocacy organizations were in support of requiring use of the metric standard for oral liquid medication dosing. Additionally, many commenters were in favor of providing the metric standard as one option to record liquid medication doses. We also received comments recommending the proper use of leading and trailing zeroes in dosing designations. NCPDP has recommended that dose amounts should always use leading zeroes before the decimal point for amounts less than one, and should not use trailing zeroes after a decimal point for oral liquid medications.[102]

Our intent is for health IT to be able to more precisely dose prescriptions in order to reduce dosing errors and improve patient safety. We also believe that use of the metric standard could improve patient safety and potentially reduce dosing errors for all medications in addition to oral liquid medications. We therefore propose, for certification to this criterion, that a Health IT Module be capable of limiting a user's ability to electronically prescribe all medications in only the metric standard. Prescription labels contain the dosing instructions specified by the prescriber. Thus, if the prescriber doses using the metric standard, the label will contain dosing instructions in the metric standard and potentially reduce dosing errors during administration. We also propose to require that a Health IT Module be capable of always inserting leading zeroes before the decimal point for amounts less than one when a user electronically prescribes medications as well as not allow trailing zeroes after a decimal point. We welcome comment on these proposals, including the feasibility of implementing the metric standard for e-prescribing all medications.

- *Incorporate Laboratory Tests and Values/Results*

2015 Edition Health IT Certification Criterion

§ 170.315(b)(4) (Incorporate laboratory tests and values/results)

We propose to adopt a 2015 Edition ''incorporate laboratory tests and values/results'' certification criterion that is revised in comparison to the 2014 Edition ''incorporate laboratory tests and values/results'' criterion (§ 170.314(b)(5)). We propose to adopt and include the HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Draft Standard for Trial Use, Release 2, US Realm (''LRI Release 2'') in the proposed 2015 Edition ''transmission of laboratory test reports'' criterion for the ambulatory setting. LRI Release 2 is currently under ballot reconciliation with HL7 and should be published in the next few months.[103] LRI Release 2 would:

- Implement common formats across US Realm IGs for consistent reader

[96] NCPDP's Structured and Codified Sig Format Implementation Guide v1.2 is within the NCPDP SCRIPT v10.6 standard.

[97] *http://www.ncpdp.org/NCPDP/media/pdf/SCRIPTImplementationRecommendationsV1-29.pdf.*

[98] AAP Council on Clinical Information Technology Executive Committee, 2011–2012. Policy Statement—Electronic Prescribing in Pediatrics: Toward Safer and More Effective Medication Management. Pediatrics 2013; 131;824.

[99] *http://www.ncpdp.org/NCPDP/media/pdf/wp/DosingDesignations-OralLiquid-Medication Labels.pdf.*

[100] *http://www.fda.gov/Drugs/DrugSafety/SafeUseInitiative/ucm188762.htm#overdoses.*

[101] Unit of Measurement Used and Parent Medication Dosing Errors. Pediatrics 134:2 August 1, 2014. Pp. e354–e361.

[102] *http://www.ncpdp.org/NCPDP/media/pdf/wp/DosingDesignations-OralLiquid-MedicationLabels.pdf.*

[103] *http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember.* Access to the current draft of the LRI Release 2 IG is freely available for review during the public comment period by establishing an HL7 user account.

experience (*e.g.,* sequence of sections, formatting, layout, and terminology);

- Incorporates all previous errata, LRI Release 1 DSTU comments and change requests;
- Adopt HL7 version 2.8 fields developed to fill gaps identified in the development of Release 1;
- Include harmonized data type ''flavors'' for use across the US Realm Lab IGs;
- Introduce initial requirements for error reporting conditions and severity (hard/soft errors) and system/application acknowledgements;
- Harmonize data element usage and cardinality requirements with LOI Release 1, and the electronic Directory of Services (eDOS) IG;
- Incorporate US Lab Realm value sets developed for clarity and consistency across all laboratory IGs; and
- Use a new publication method for value sets that allows for precision usage at point of use and provides ''at a glance'' comprehensive usage at the field and component-level across all laboratory IGs; and synced with value set activities (HL7, VSAC, etc.).

Overall, we propose to adopt LRI Release 2 because it addresses errors and ambiguities found in LRI Release 1 and harmonizes interoperability requirements with other laboratory standards we propose to adopt in this proposed rule (*e.g.,* the HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders from EHR, DSTU Release 2, US Realm, 2013 [104]).

As compared to the 2014 Edition certification criterion, we also propose more specific requirements for how a Health IT Module must be capable of electronically displaying the information included in a test report. This specificity would improve the consistency with how laboratory tests and values/results are displayed, which would also assist with laboratory compliance with CLIA. To meet this criterion, a Health IT Module would be required to display the following information included in laboratory test reports it receives: (1) the information for a test report as specified in 42 CFR 493.1291(a)(1) through (a)(3) and (c)(1) through (c)(7); the information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); the information for alerts and delays as specified in 42 CFR 493.1291(g) and (h); and the information for corrected reports as specified in 42 CFR 493.1291(k)(2).

We also propose, for the purposes of certification, to require a Health IT Module to be able to use, at a minimum, the version of Logical Observation Identifiers Names and Codes (LOINC®) adopted at § 170.207(c)(3) (version 2.50) as the vocabulary standard for laboratory orders. This is the most recent version of LOINC®. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of LOINC® as a minimum standards code set and our proposal to adopt version 2.50, or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

We propose to adopt the updated LRI Release 2 at § 170.205(j)(2), which requires the modification of the regulatory text hierarchy in § 170.205(j) to designate the standard referenced by the 2014 Edition version of this certification criterion at § 170.205(j) to be at § 170.205(j)(1). This regulatory structuring of the IGs would make the CFR easier for readers to follow.

EHR–S Functional Requirements LRI IG/Testing and Certification Requirements

We seek comment on the HL7 EHR–S Functional Requirements for the V2.5.1 Implementation Guide: S&I Framework Lab Results Interface R2, Release 1, US Realm, Draft Standard for Trial Use, Release 1 (''EHR–S IG''). The EHR–S IG is currently under ballot reconciliation with HL7.[105] The focus of the EHR–S IG is the definition of EHR system functional requirements related to the receipt of laboratory results that are compliant with the LRI Release 2. The EHR–S IG also includes additional requirements as set forth in CLIA as well as clinical best practices beyond the scope of LRI Release 2.

We specifically seek comment on the clarity and completeness of the EHR–S IG in describing the requirements related to the receipt and incorporation of laboratory results for measuring conformance of a Health IT Module to LRI Release 2. In addition, we seek comment on how a Health IT Module should be tested and certified consistently and uniformly for the incorporation of laboratory results data. For example, should testing and certification require the Health IT Module to demonstration the ability to associate the laboratory result with an order or patient, to recall the result for display or for submission to another technology, and/or to use the result for automated clinical decision support interventions? Further, what, if any, specific capabilities currently included in the EHR–S IG should be part of testing and certification for this criterion?

- Transmission of Laboratory Test Reports

2015 Edition Health IT Certification Criterion
§ 170.315(b)(5) (Transmission of laboratory test reports)

We propose to adopt a 2015 Edition ''transmission of laboratory test reports'' certification criterion that is revised in comparison to the 2014 Edition ''transmission of electronic laboratory tests and values/results to ambulatory providers'' criterion (§ 170.314(b)(6)). We have renamed this criterion to more clearly indicate its availability for the certification of health IT used by any laboratory. We propose to adopt and include the HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Draft Standard for Trial Use, Release 2, US Realm (''LRI Release 2'') in the proposed 2015 Edition ''transmission of laboratory test reports'' criterion. LRI Release 2 is currently under ballot reconciliation with HL7 and should be published in the next few months.[106] We propose to adopt this standard for the same reasons discussed in the 2015 Edition ''incorporate laboratory tests and values/results'' above. We refer readers to the description of the LRI Release 2 IG and our rationale for its adoption discussed in that criterion.

As also discussed in the 2015 Edition ''incorporate laboratory tests and values/results'' above, the LRI Release 2 IG requires the information for a test report as specified at 42 CFR 493.1291(a)(1) through (3), (c)(1) through (c)(7), (d), (g), (h) and (k)(2) to be included in the content message. Therefore, inclusion of this standard for certification should not only facilitate improved interoperability of electronically sent laboratory test reports (as discussed in more detail in the 2015 Edition ''incorporate laboratory tests and values/results'' criterion), but also facilitate laboratory compliance with CLIA as it relates to the incorporation and display of test results in a receiving system.

We also propose, for the purposes of certification, to require a Health IT

[104] We have proposed to adopt this implementation guide for the 2015 Edition ''CPOE for laboratory orders'' certification criterion.

[105] *http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember.* Access to the current draft of the EHR–S IG is freely available for review during the public comment period by establishing an HL7 user account.

[106] Access to the current draft of the LRI Release 2 IG is freely available for review during the public comment period by establishing an HL7 user account.

Module to be able to use, at a minimum, the version of Logical Observation Identifiers Names and Codes (LOINC®) adopted at § 170.207(c)(3) (version 2.50) as the vocabulary standard for laboratory orders. This is the most recent version of LOINC®. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of LOINC® as a minimum standards code set and our proposal to adopt version 2.50, or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

We propose to adopt the updated LRI Release 2 at § 170.205(j)(2), which requires the modification of the regulatory text hierarchy in § 170.205(j) to designate the standard referenced by the 2014 Edition version of this certification criterion at § 170.205(j) to be at § 170.205(j)(1). This regulatory structuring of the IGs would make the CFR easier for readers to follow.

- *Data Portability*

2015 Edition Health IT Certification Criterion

§ 170.315(b)(6) (Data portability)

We propose to adopt a 2015 Edition ''data portability'' certification criterion that is revised in comparison to the 2014 Edition ''data portability'' certification criterion (§ 170.314(b)(7)). Similar to the 2014 Edition version, we propose to include the 2015 Edition ''data portability'' criterion in the Base EHR definition (*i.e.,* the 2015 Base EHR definition).

For the 2014 Edition ''data portability'' criterion, we expressed that the criterion was intended to enable an EP, eligible hospital, or CAH to create a set of export summaries for all patients in EHR technology formatted according to the C–CDA that includes each patient's most recent clinical information. (77 FR 54193). We also included this criterion in the Base EHR definition as a way to ensure that the capability was delivered to EPs, eligible hospitals, or CAHs. By including the criterion in the Base EHR definition, an EP, eligible hospital, or CAH must have EHR technology certified to this criterion in order to possess EHR technology that meets the CEHRT definition.

In the years since the 2014 Edition final rule was issued (September 2012) and the subsequent implementation and use of this capability by EPs, eligible hospitals, and CAHs, we have received two types of feedback. From health IT developers, we have received requests for clarification about this certification criterion's scope. For example, requests for clarifications about the data that must be produced and from how far back in time the data must be produced. Whereas from providers (and the implementation professionals and third party developers with which they work), we have generally received more substantive critiques about the overall usefulness of the capability and the ways in which health IT developers met the certification criterion's requirements but did not necessarily deliver on its intent. Such ''user'' comments conveyed that some health IT developers provided a capability that was difficult or non-intuitive to use, difficult to find to even use (*e.g.,* ''hidden''), and in some cases either required developer personnel to assist the provider in executing the capability or limited its execution to only being done by the developer at the provider's request. We have also received feedback that the scope of testing has not rigorously assessed the ability of health IT to create large quantities of export summaries. As a result, some providers have reported challenges and poor performance associated with this capability.

We believe that this feedback from CEHRT users indicates that the data portability certification criterion adopted in the 2014 Edition has not provided the data accessibility to providers we believed would occur as a result of its adoption. It also indicates that some health IT developers have (intentionally or unintentionally) obstructed the certification criterion's true intent—to give providers easy access and an easy ability to export clinical data about their patients for use in a different EHR technology or even a third party system for the purpose of their choosing.

To address provider critiques as well as to provide additional developer requested clarity, we propose a revised 2015 Edition ''data portability'' certification criterion as compared to the 2014 Edition version. The proposed data portability certification criterion at § 170.315(b)(6) approaches data portability from a slightly different angle than the 2014 Edition version and focuses on the following specific capabilities.

1. As a general rule, we emphasize that this capability would need to be user-focused and user driven. A user must be able to set the configuration options included within the more detailed aspects of the criterion and a user must be able to execute these capabilities at any time the user chooses and without subsequent developer assistance to operate. We expect that testing of a Health IT Module presented for certification to this criterion would include a demonstration that the Health IT Module enables a user to independently execute this capability without assistance from the health IT developer beyond normal orientation/training.

2. The criterion would require that a user be able to configure the Health IT Module to create an export summary for a given patient or set of export summaries for as many patients selected. It would also require that these export summaries be able to be created according to any of the following document-template types included in the C–CDA R2.0 (also proposed as the content standard in this criterion): CCD; Consultation Note; History and Physical; Progress Note; Care Plan; Transfer Summary; and Referral Note. We also propose that the Discharge Summary document template be included for a Health IT Module developed for the inpatient setting.

3. From a data perspective, we propose that the minimum data that a Health IT Module must be capable of including in an export summary are: the data represented by the Common Clinical Data Set and:

- Encounter diagnoses (according to the standard specified in § 170.207(i) (ICD–10–CM) or, at a minimum, the version of the standard at § 170.207(a)(4) (September 2014 Release of the U.S. Edition of SNOMED CT®) [107];
- Cognitive status;
- Functional status;
- For the ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information; and
- For the inpatient setting only. Discharge instructions.

4. We propose that a user would need to be able to be able to configure the technology to set the time period within which data would be used to create the export summary or summaries. And that this must include the ability to enter in a start and end date range as well as the ability to set a date at least three years into the past from the current date.

5. We propose that a user would need to be able to configure the technology to create an export summary or summaries based on the following user selected events:

- A relative date or time (*e.g.,* the first of every month);

[107] We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of SNOMED CT® as a minimum standards code set and our proposal to adopt the September 2014 Release (U.S. Edition), or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

- A specific date or time (*e.g.,* on 10/24/2015); and
- When a user signs a note or an order.

6. We propose that a user would need to able to configure and set the storage location to which the export summary or export summaries are intended to be saved.

Again, we emphasize that all these capabilities would need to be able to be configured and executed by a user without the aid of additional health IT developer personnel and without the need to request developer action. Further, we also reiterate that we have expanded the nature and focus of this criterion to more precisely address provided critiques as well as to expand the anticipated and potential uses providers can deploy based on this more configuration focused criterion.

- Data Segmentation for Privacy

We propose to adopt two new certification criteria that would focus on the capability to separately track (''segment'') individually identifiable health information that is protected by rules that are more privacy-restrictive than the HIPAA Privacy Rule. This type of health information is sometimes referred to as sensitive health information. The HIPAA Privacy Rule serves as the federal baseline for health information privacy protections. It also generally permits the use or disclosure of protected health information (PHI) for limited specific purposes (such as treatment and payment) without a patient's permission.[108]

The HIPAA Privacy Rule does not override (or preempt) more privacy-protective federal and state privacy laws. A number of federal and state health information privacy laws and regulations are more privacy-protective than the HIPAA Privacy Rule. Typically, these rules require a patient's permission (often referred to as ''consent'' in these rules) in writing in order for the individually identifiable health information regulated by those laws to be shared. One example is the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 CFR part 2) (''part 2'') that apply to information about treatment for substance abuse from federally funded programs.[109] There are also federal laws protecting certain types of health information coming from covered U.S. Department of Veterans Affairs facilities and programs (38 U.S.C. 7332). These laws and comparable state laws were established, in part, to address the social stigma associated with certain medical conditions by encouraging people to get treatment and providing them a higher degree of control over how their health information may be shared. These laws place certain responsibilities on providers to maintain the confidentiality of such information. More restrictive state laws also protect certain categories of individually identifiable health information, such as information regarding minors or teenagers, intimate partner/sexual violence, genetic information, and HIV-related information.[110] These laws and regulations remain in effect and changes to these laws and regulations are not within the scope of this proposed rule.[111] However, with these laws in mind, the proposals that follow seek to encourage the development and use of a technical capability that permits users to comply with these existing laws and regulations. These proposals are also in line with the *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Version 1.0.*[112] HHS is committed to encouraging the development and use of policy and technology to advance patients' rights to access, to amend, and to make choices for the disclosure of their electronic individually identifiable health information. HHS also noted support for the development of standards and technology to facilitate patients' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, or HIV) in an electronic environment.[113]

Technological advances are creating opportunities to share data and allow patient preferences to electronically persist in health IT. In 2012, ONC launched the Data Segmentation for Privacy (DS4P) initiative through ONC's Standards and Interoperability (S&I) Framework.[114] The DS4P initiative aimed to provide technical solutions and pilot implementations to help meet existing legal requirements in an increasingly electronic environment.[115] The DS4P initiative worked to enable the implementation and management of varying disclosure policies in an electronic health information environment in an interoperable manner. Overall, the DS4P initiative and its subsequent pilots focused on the exchange of health information in the context of 42 CFR part 2 and sought to develop technical standards that would enable a provider to adopt health IT that could segment electronic sensitive health information regulated by more restrictive laws and make compliance with laws like Part 2 more efficient. Since the sunset of the DS4P initiative in April 2014, there have been live implementations and public testimony regarding the success and practical application of the DS4P standard. Organizations including the Substance Abuse and Mental Health Services Administration (SAMHSA), the U.S. Department of Veterans Affairs (VA), and private companies that participated in the initiative have moved to production use of DS4P. For example, a stakeholder who implemented the DS4P part 2 solution noted that the DS4P technical capability implemented in parts of Florida has saved some hospitals millions of dollars associated with the cost of care because the patients they treat with substance use issues or behavioral health issues were able to send an electronic referral and get a discharge performed earlier in the process.[116] Another technology stakeholder incorporated the DS4P technical functionality into its behavioral health and general hospital health IT solutions released this year. Most recently, SAMHSA developed an open source technology for patient consent management that uses the DS4P standard.[117] In September 2014, this technical solution was deployed into a live environment at a public health department.

The technical specifications are outlined in the HL7 Version 3 Implementation Guide: DS4P, Release 1

[108] *http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/.*

[109] *http://www.healthit.gov/sites/default/files/privacy-security/gwu-data-segmentation-final-cover-letter.pdf.*

[110] *http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.*

[111] For a policy discussion, see Substance Abuse and Mental Health Services Administration (SAMHSA)'s recent public listening session pertaining to the federal confidentiality of regulations: *https://www.federalregister.gov/articles/2014/05/12/2014-10913/confidentiality-of-alcohol-and-drug-abuse-patient-records.*

[112] *http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.*

[113] *http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.*

[114] *http://wiki.siframework.org/Data+Segmentation+for+Privacy+Use+Cases.*

[115] For more information about enabling privacy through data segmentation technology, see *http://www.healthit.gov/providers-professionals/enabling-privacy.*

[116] See Health IT Policy Committee's (HITPC) Privacy and Security Tiger Team Public Meeting, Transcript, (Apr. 16, 2014), p. 14, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-04-16.pdf.*

[117] *http://www.healthit.gov/providers-professionals/ds4p-initiative.*

(DS4P IG), Part 1: CDA R2 and Privacy Metadata.[118] The DS4P IG describes the technical means of applying security labels (privacy metadata) which can be used to enact any security or privacy law, regulation, or policy so that the appropriate access control decisions will be made regarding downstream use, access or disclosure for specially protected data so that appropriate metadata tags are applied.

Conceptually, the DS4P approach utilizes metadata applied in layers (*e.g.* metadata applied to the header, section, or entry levels of a C–CDA document). The DS4P technical approach defaults to privacy metadata tagging at the document level. If an organization chooses to apply additional privacy metadata tagging within a document, that optional technical capability is also described within the IG for CDA. If a receiving system is unable to process section or entry level privacy metadata, the default is tagging at the document level. The approach relies on certain electronic actions being taken by both the sending system and the receiving system. The sending system must:

1. Identify information that requires enhanced protection or is subject to further restrictions;
2. Verify that the patient's privacy consent decision allows for the disclosure of health information;[119] and
3. Add privacy metadata to the health information being disclosed.

In turn, the receiving system must:

1. Be able to process the privacy metadata associated with the received health information; and
2. Verify the patient's consent before re-disclosure, if the receiving system has a need to re-disclose the information.

Data segmentation technology emerged to enable health care providers' use of technology to comply with existing privacy laws, regulations, and policies. The term ''data segmentation'' is often used to describe the electronic labeling or tagging of a patient's health information in a way that allows patients or providers to electronically share parts,[120] but not all, of a patient record. For example, data segmentation technology can be applied to the sharing of electronic sensitive health information, because that information is afforded greater protections under various state and federal laws,[121] as is discussed above. In this proposed rule, we propose to offer two certification criteria that would allow for health IT to be presented for testing and certification to the DS4P standard. We view the proposed offering of certification to these criteria as an initial step on technical standards towards the ability of an interoperable health care system to compute and persist the applicable permitted access, use or disclosure; whether regulated by state or federal laws regarding sensitive health information or by an individual's documented choices about downstream access to, or use or disclosure to others of, the identifiable individual's health information. The application of the DS4P standard at the document level is an initial step. We understand and acknowledge additional challenges surrounding the prevalence of unstructured data, sensitive images, and potential issues around use of sensitive health information by CDS systems. The adoption of document level data segmentation for structured documents will not solve these issues, but will help move technology in the direction where these issues can be addressed.

For example, today, electronic sensitive health information is not typically kept in the same repository as non-sensitive data. If security labels were applied to C–CDA documents at the time they are created (see ''data segmentation for privacy—send'' certification criterion), the receiving system would have more choices about how to store and use that sensitive information. If the receiving system had the capability to grant access to the tagged documents by using the security labels as part of the access control decision, then co-mingling the tagged, sensitive health information with the non-sensitive data becomes more achievable.

In July 2014, the HITPC provided recommendations on the use of DS4P technology to enable the electronic implementation and management of disclosure policies that originate from the patient, the law, or an organization, in an interoperable manner, so that electronic sensitive health information may be appropriately shared.[122] The HITPC noted a clear need to provide coordinated care for individuals with mental health and/or behavioral health issues. The HITPC recognized that the ability of patients to withhold consent to disclose information remains a concern for providers. In particular, providers want to provide the best care for patients, but they have concerns about incomplete records due to both professional obligation and liability considerations. While the need for providers to act on incomplete information is not necessarily new, the use of health IT may create an expectation of more complete information.[123] In recognition of the consumer, business, clinical, and technical complexities, the HITPC suggested a framework of two glide paths for the exchange of 42 CFR part 2-protected data, based on whether the subject is sending or receiving information.[124] As a first step in the glide path, the HITPC recommended that we include Level 1 (document level tagging) send and receive functionality.[125] Document level is the most basic level of privacy metadata tagging described in the DS4P standard. The following two proposals would implement the HITPC's recommendations.

- *Data Segmentation for Privacy—Send*

2015 Edition Health IT Certification Criterion
§ 170.315(b)(7) (Data segmentation for privacy—send)

A provider currently cannot send sensitive patient information electronically without some technical capability to indicate information is subject to restrictions, such as a prohibition on re-disclosure without consent, consistent with 42 CFR part 2. The sending provider also must have confidence that the receiver can properly handle electronically sent 42 CFR part 2-covered data. Because neither of these functionalities are currently supported in certification, sensitive health information such as 42 CFR part 2-covered data is often only

[118] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=354.* Completed Normative Ballot in January 2014 and was successfully reconciled in February 2014. HL7 approved the final standard for publication and ANSI approved in May 2014.

[119] *http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange.*

[120] The HL7 approved standard does allow for tagging at the data element level, but this proposed rule is suggesting just applying the DS4P to the document level.

[121] *http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.*

[122] See Health IT Policy Committee (HITPC) Recommendation Letter to ONC, July 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf;* see also HITPC's Privacy and Security Tiger Team Public Meeting, Transcript, May 12, 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-12.pdf;* Public Meeting, Transcript, May 27, 2014, *http://www.healthit.gov/facas/sites/faca/files/PSTT_Transcript_Final_2014-05-27.pdf.*

[123] Id.

[124] For more details on the two glide paths for part 2-protected data, see *http://www.healthit.gov/facas/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf.*

[125] Id. See also, related HITPC recommendations pertaining to data segmentation submitted to ONC in September 2010: *http://www.healthit.gov/sites/faca/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf.*

shared via paper and fax. We propose, consistent with the HITPC recommendations, that for certification to this criterion, a Health IT Module must be able to send documents using document level tagging (Level 1) in accordance with the DS4P IG. Document level tagging enables health IT to send the 42 CFR part 2-covered data along with the appropriate privacy metadata tagging and keep it sequestered from other data. The DS4P IG, which includes Level 1 functionality, provides guidance to allow, with proper authorization, a system to send a C–CDA with tags indicating any restrictions (such as a prohibition on re-disclosure without consent). While the DS4P IG specifies the technical means for applying privacy metadata tagging to C–CDA documents, it also optionally supports use of privacy metadata tagging within the document (at the section and entry levels). We only propose to require the document level functionality for sending as part of certification to this criterion.

- *Data Segmentation for Privacy—Receive*

2015 Edition Health IT Certification Criterion
§ 170.315(b)(8) (Data segmentation for privacy—receive)

In general, 42 CFR part 2-covered data is not currently provided electronically to healthcare providers through electronic exchange. Instead, the status quo remains to share 42 CFR part 2-covered data via paper and fax. In line with the HITPC recommendations, we propose a certification criterion that would require a Health IT Module to be able to receive 42 CFR part 2-covered data in accordance with the DS4P IG. DS4P at the document level (Level 1) of the recommendations allows recipient health IT to receive, recognize, and view documents with privacy metadata tagging indicating certain restrictions from 42 CFR part 2 providers with the document sequestered from other health IT data. A recipient provider could use document level tagging to sequester the document from other documents received and help prevent unauthorized re-disclosure, while allowing the sensitive data to flow more freely to authorized recipients. Thus, consistent with the HITPC recommendations, we propose that a Health IT Module be able to receive documents tagged with privacy metadata tagging (Level 1).

- *Care Plan*

2015 Edition Health IT Certification Criterion
§ 170.315(b)(9) (Care plan)

We propose to adopt a new 2015 Edition certification criterion that would reflect a Health IT Module's ability to enable a user to record, change, access, create and receive care plan information in accordance with the ''Care Plan document template'' in the C–CDA Release 2.0 standard.

The S&I Framework Longitudinal Coordination of Care (LCC) Longitudinal Care Plan Sub-Work Group defined a ''care plan'' as ''the synthesis and reconciliation of the multiple plans of care produced by each provider to address specific health concerns. It serves as the blueprint shared by all participants to guide the individual's care. As such, it provides the structure required to coordinate care across multiple sites, providers, and episodes of care.'' [126] The care plan helps multiple providers and caregivers align and coordinate care, which is especially valuable for patients living with chronic conditions and/or disabilities. It also provides a structure to promote the consideration of a patient's future goals and expectations in addition to managing their currently active health issues.

The C–CDA Release 2.0 contains a Care Plan document template that reflects these principles and provides a structured format for documenting information such as the goals, health concerns, health status evaluations and outcomes, and interventions. Note that the Care Plan document template is distinct from the ''Plan of Care Section'' in previous versions of the C–CDA. The Care Plan document template represents the synthesis of multiple plans of care (for treatment) for a patient, whereas the Plan of Care Section represented one provider's plan of care (for treatment). To make this distinction clear, the C–CDA Release 2.0 has renamed the previous ''Plan of Care Section'' as the ''Plan of Treatment Section (V2).''

Given the value for improved coordination of care, we propose a new 2015 Edition certification criterion for ''care plan'' that would require a Health IT Module to enable a user to record, change, access, create, and receive care plan information in accordance with the ''Care Plan document template'' in the HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes.[127] The IG provides guidance for implementing CDA documents, including the Care Plan document template. The ''transitions of care'' certification criterion proposed elsewhere in this section of the preamble would require a Health IT Module enable a user to send and receive transitions of care/referral summaries according to the C–CDA Release 2.0, which would include the Care Plan document template. Therefore, this criterion would focus only on a Health IT Module's ability to enable a user to record, change, access, create, and receive care plan information. We welcome comment on our proposal, including whether we should require certain ''Sections'' that are currently deemed optional as part of the Care Plan document template for certification to this criterion. For example, we invite comment on whether we should require the optional ''Health Status Evaluations and Outcomes Section'' and ''Interventions Section (V2)'' as part of certification to this criterion, and if so, for what value/use case.

- *Clinical Quality Measures—Record and Export*

2015 Edition Health IT Certification Criterion
§ 170.315(c)(1) (Clinical quality measures—record and export)

We propose to adopt a 2015 Edition certification criterion for ''clinical quality measures (CQM)—record and export'' that is revised in comparison to the 2014 Edition ''CQM—capture and export'' certification criterion (§ 170.314(c)(1)). In order to align with our use of the term ''record'' used in other 2014 and 2015 Edition certification criteria, we propose to call this certification criterion ''CQM—record and export.'' We explain the term ''record'' in the 2014 Edition final rule at 77 FR 54168.[128] We propose to require that a system user be able to export CQM data at any time the user chooses and without subsequent developer assistance to operate. We also propose to require that this certification criterion be part of the set of criteria necessary to satisfy the ''2015 Edition Base EHR'' definition (see also section III.B.1 of this preamble for a discussion of the proposed 2015 Edition Base EHR definition). Last, we solicit comment on the version of standards we should adopt for this certification criterion.

Standards for Clinical Quality Measures

In the 2014 Edition ''CQM—capture and export'' certification criterion, we require that technology must be able to export a data file formatted in

[126] *http://wiki.siframework.org/file/view/Care%20Plan%20Glossary_v25.doc/404538528/Care%20Plan%20Glossary_v25.doc.*

[127] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=379.*

[128] ''Record'' is used to mean the ability to capture and store information in technology.

accordance with the HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture (QRDA), DSTU Release 2 (July 2012) standard. We understand that the industry is working to harmonize both clinical quality measurement and CDS standards through initiatives such as the Clinical Quality Framework (CQF) S&I initiative. CDS guides a clinician to follow a standard plan of care, while CQMs measure adherence to a standard plan of care. Thus, these two areas are closely related and would benefit from standard ways to reference patient data within health IT as well as common logic to define a sub-population. The CQF S&I initiative is working to define a shared format, terminology, and logic between CQMs and CDS for improved efficiency, cost, and quality of care.

In order to harmonize CQM and CDS standards, the industry is using pieces of existing CQM standards (*e.g.,* Health Quality Measures Format (HQMF), QRDA Categories I and III, and the Quality Data Model (QDM)) and CDS standards (*e.g.,* Clinical Decision Support Knowledge Artifact Specification (also known as HeD Schema) and the Virtual Medical Record). HL7 issued an errata (September 2014)[129] that reflects updates based on an incremental version of the harmonized CQM and CDS standards (*i.e.,* QDM-based HQMF Release 2.1).[130] This errata is meant to be used in conjunction with the July 2012 QRDA IG we adopted in the 2014 Edition. Our understanding is that the fully harmonized CQM and CDS standards will be based on the Quality Improvement and Clinical Knowledge (QUICK) data model,[131] and that the industry expects to ballot a QUICK FHIR-based DSTU serving the same function as the HQMF standard at the May 2015 HL7 meeting. Subsequent standards for electronically processing and reporting CQMs and CDS would then be expected to be built on the QUICK data model, including a QRDA-like standard based on the anticipated QUICK FHIR-based DSTU.

Given the timing of this proposed rule and the expected deliverables for harmonized CQM and CDS standards as described above, we solicit comment on the version of QRDA or the QRDA-like standards we should adopt for this certification criterion. Specifically, we solicit comment on the following three options:

- HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture (QRDA), DSTU Release 2 (July 2012);
- HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture (QRDA), DSTU Release 2 (July 2012) and the September 2014 Errata; or
- A QRDA-like standard based on the anticipated QUICK FHIR-based DSTU.CQM standards we should adopt for this certification criterion.

We anticipate that the QUICK data model will not be available to review during the public comment period of this NPRM, and welcome stakeholder input on the usefulness of adopting the current (July 2012) QRDA standard alone or in conjunction with the September 2014 errata given that we anticipate there will be harmonized CQM and CDS standards available in mid-2015. We also seek to understand the tradeoffs stakeholders perceive in adopting each standard provided that the EHR Incentive Programs Stage 3 proposed rule is proposing that technology certified to the 2015 Edition would not be required until January 1, 2018, but that technology certified to the 2015 Edition ''CQM—record and export'' certification criterion would be needed for EPs, eligible hospitals, and CAHs participating in the EHR Incentive Programs Stage 3 objectives and measures in 2017. Thus, we welcome input on recommended QRDA standards for the ''CQM—record and export'' certification criterion factoring in where the industry may be with adoption of CQM and CDS standards over the next few years.

User Ability To Export CQM Data

We have received stakeholder feedback that some systems certified to the 2014 Edition ''CQM—capture and export'' certification criterion do not provide users with the ability to export data ''on demand'' nor to export batches of multiple patients simultaneously. Rather, some users of certified health IT must request this functionality from the health IT developer. Our intent is that users should be able to export CQM data formatted to the QRDA standard at any time the user chooses for one or multiple patients and without additional assistance. Thus, as proposed, when a Health IT Module is presented for certification to this criterion, we would expect that testing of the Health IT Module would include demonstration of a user's ability to export CQM data without subsequent health IT developer assistance beyond normal orientation/training.

- *Clinical Quality Measures—Import and Calculate*

2015 Edition Health IT Certification Criteria

§ 170.315(c)(2) (Clinical quality measures—import and calculate)

We propose to adopt a 2015 Edition certification criterion for ''clinical quality measures (CQM)—import and calculate'' that is revised in comparison to the 2014 Edition ''CQM—import and calculate'' certification criterion (§ 170.314(c)(2)). We propose to require that a system user be able to import CQM data at any time the user chooses and without subsequent health IT developer assistance to operate. We also no longer include an exemption that would allow a Health IT Module presented for certification to all three CQM certification criteria (§§ 170.315(c)(1), (c)(2), and (c)(3)) to not have to demonstrate the data import capability. Last, we solicit comment on our intended direction for testing and certifying health IT and the version of standards we should adopt for this certification criterion.

User Ability To Import CQM Data

We have received stakeholder feedback that some systems certified to the 2014 Edition ''CQM—import and calculate'' certification criterion do not provide users the ability to import data ''on demand,'' and rather users must request this functionality from the system developer or vendor. Our intent is that users should be able to import CQM data formatted to the QRDA standard for one or multiple patients at any time the user chooses and without additional assistance. Thus, when a Health IT Module is presented for certification to this criterion, we would expect that testing of the Health IT Module would include demonstration of a user's ability to import CQM data without subsequent health IT developer assistance beyond normal orientation/training.

Import of CQM Data

For the 2014 Edition, we do not require systems that certify to § 170.314(c)(1) (CQM—capture and export), § 170.314(c)(2) (CQM—import and calculate), and § 170.314(c)(3) (CQM—electronic submission) to have to demonstrate that they can import data files in accordance with the QRDA

[129] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35.* Please note that in order to access the errata, the user should download the ''HL7 Implementation Guide for CDA Release 2: Quality Reporting Document Architecture—Category I, DSTU Release 2 (US Realm)'' package.

[130] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=97.*

[131] *http://www.hl7.org/special/Committees/projman/searchableProjectIndex.cfm?action=edit&ProjectNumber=1045.*

standard. In 2012, we adopted this policy because we did not believe that systems that could perform capture, export, and electronic submission functions would need to import CQM data as they were in essence ''self-contained'' (77 FR 54231). However, we have received stakeholder input recommending that all systems should be able to import CQM data and that there could be instances were a provider using one technology to record CQM data could not subsequently import such data into a different technology. We agree with this feedback. Therefore, this exemption will no longer carry forward as part of the proposed 2015 Edition version of this certification criterion. This means that a Health IT Module presented for certification to this certification criterion (§ 170.315(c)(2)) would need to be able to demonstrate the ability to import data in order to be certified to this certification criterion even if they also certify to provide ''record and export'' and ''electronic submission/report'' functions.

Testing of Import and Calculate Functionalities

The testing procedures for the 2014 Edition ''CQM—import and calculate'' certification criterion only test that technology can import a small number of test records and use those for calculation of CQM results. We have received feedback that technology should be able to import a larger number of test records and that we should test this ability to reflect real-world needs for technology. With the import of a large number of records, technology also needs to be able to de-duplicate records for accurate calculation of CQM results. Therefore for testing and certification to the proposed 2015 Edition ''CQM—import and calculate'' certification criterion, we intend for testing to include that technology can import a larger number of test records compared to testing for the 2014 Edition and automatically de-duplicate them for accurate CQM calculation. We welcome comment on our proposed intentions to test a larger number of test records compared to the 2014 Edition test procedure and that a Health IT Module could eliminate duplicate records. We also request comment on the number of test records we should consider testing a Health IT Module for performing import and calculate functions.

Standards for Clinical Quality Measures

We describe above in the preamble for the proposed 2015 Edition ''CQM—record and export'' certification criterion our understanding of the industry's timeline and expected deliverables for harmonized CQM and CDS standards. Given the discussion above, we also solicit comment on the QRDA standards we should consider adopting for this 2015 Edition ''CQM—import and calculate'' certification criterion.

- *Clinical Quality Measures—Report*

2015 Edition Health IT Certification Criteria
§ 170.315(c)(3) [Reserved]

In the 2014 Edition, we adopted a ''CQM—electronic submission'' certification criterion that requires technology to enable a user to electronically create a data file for transmission of CQM data in accordance with QRDA Category I and III standards and ''that can be electronically accepted by CMS'' (§ 170.314(c)(3)). We have received stakeholder feedback recommending we better align our certification policy and standards for electronically-specified CQM (eCQM) reporting with other CMS programs that include eCQMs, such as the Physician Quality Reporting System (PQRS) and Hospital Inpatient Quality Reporting (IQR) programs. The PQRS and Hospital IQR programs update their measure specifications on an annual basis through rulemaking in the Physician Fee Schedule (PFS) and Inpatient Prospective Payment Systems (IPPS) rules respectively.

To better align with the reporting requirements of other CMS programs, we intend to propose certification policy for reporting of CQMs in or with annual PQRS and/or Hospital IQR program rulemaking. We anticipate we will propose standards for reporting of CQMs that reflect CMS' requirements for the ''form and manner'' of CQM reporting (*e.g.,* CMS program-specific QRDA standards), allowing for annual updates of these requirements as necessary. Under this approach, the ''CQM—report'' certification policy and associated standards for the 2015 Edition that support achieving EHR Incentive Program requirements would be proposed jointly with the calendar year (CY) 2016 PFS and/or IPPS proposed rules. We anticipate these proposed and final rules will be published in CY 2015. We clarify that we anticipate removing ''electronic'' from the name of this certification criterion. As described in the preamble, we expect that all functions proposed in the 2015 Edition certification criteria are performed or demonstrated electronically. Thus, it is not necessary to specifically include this requirement in the title of this certification criterion. We also anticipate naming this certification criterion ''report'' instead of ''submission'' to better align with the language we use in other certification criteria that also require demonstration of the same functionality to submit data.

- *Clinical Quality Measures—Filter*

2015 Edition Health IT Certification Criterion
§ 170.315(c)(4) (Clinical quality measures—filter)

We propose to adopt a new 2015 Edition certification criterion for CQM filtering. In the Voluntary Edition proposed rule, we proposed a new certification criterion that would require health IT to be able to record structured data for the purposes of being able to filter CQM results to create different patient population groupings by one or more of a combination of certain patient characteristics[132] (79 FR 10903–04). We proposed this capability to support eCQM reporting where the reporting entity is not an individual provider but rather a group practice or an accountable care organization (ACO). We also proposed certain patient characteristics that would support identification of health disparities, help providers identify gaps in quality, and support a provider in delivering more effective care to sub-groups of their patients. We did not adopt this certification criterion in the 2014 Edition Release 2 final rule as we received comments recommending we further refine the use cases and perform more analysis of which data elements are being captured in standardized ways (79 FR 54462).

CMS offers various options for providers to report quality data as part of a group instead of individually reporting as individual providers. For example, the PQRS offers the Group Practice Reporting Option (GPRO) that allows for assessment and payment (or adjustment) based on reporting of data on quality measures at the group level. Similarly, there are group reporting options, including the GRPO under the PQRS for reporting data used to assess quality for purposes of the Value Modifier under the Medicare Physician Fee Schedule. Another CMS group reporting option is the Comprehensive Primary Care (CPC) initiative. In the CPC initiative, participating primary

[132] Practice site and address; Tax Identification Number (TIN), National Provider Identifier (NPI), and TIN/NPI combination; diagnosis; primary and secondary health insurance, including identification of Medicare and Medicaid dual eligible; demographics including age, sex, preferred language, education level, and socioeconomic status.

care practices receive care management fees to support enhanced, coordinated services. In the CPC initiative, each physical site location is counted as a ''practice.'' A group practice may encompass several primary care sites, of which some, but not all, are participating in CPC. Because the unit of analysis in CPC is the practice site, CMS requires all CPC participants to report CQMs at the level of the practice rather than at the level of the individual provider. Each CPC practice's quality results, which include performance on patient experience and claims measures as well as CQMs, are tied to the distribution of any Medicare shared savings calculated and earned at the level of the Medicare population of each region participating in the initiative.

ACO models and programs, such as the Medicare Shared Savings Program (MSSP) and CMS Pioneer ACO Model, include groups of doctors, hospitals, and other health care providers who come together voluntarily to give coordinated high quality care to their patients. In ACO models and programs, the providers that participate in the ACO share responsibility for the care and outcomes of their patients. For example, MSSP participants are rewarded if the ACO lowers the growth in its health care costs while meeting performance standards on quality of care. ACOs are required to internally report on cost and quality metrics associated with the activities of their practitioners, to promote the use of evidence-based medicine, and to support the care coordination activities of their practitioners. Understanding the practice patterns of individual practitioners for services provided on behalf of the ACO is therefore important for such organizations.

In some cases, not all providers practicing at a particular practice site location or in an ACO will be participating in the group practice or ACO reporting options. The National Provider Identifier (NPI) is insufficient by itself to attribute a provider's performance to a particular group practice or ACO, as the provider could practice in multiple health care organizations. Likewise, a health care organization may have multiple Tax Identification Numbers (TINs). Currently, data may be accessed by filtering on either the TIN or the NPI, but not in combination due, in part, to current CMS reporting requirements and limitations of health IT being used by providers. The ability to filter by a combination of NPI/TIN could allow for more specific and proper attribution of a provider's performance to the correct organization for aggregating group practice or ACO quality measure results.

Health IT should support an organization's ability to filter both individual patient level and aggregate level eCQM results by data that would support administrative reporting as well as identification of health disparities and gaps in care for patients being treated at particular group practice sites or in a given ACO. We, therefore, propose a new certification criterion for CQM filtering that would require health IT to be able to record data (according to specified standards, where applicable) and filter CQM results at both patient and aggregate levels by each one and any combination of the following data:

- TIN;
- NPI;
- Provider type;
- Patient insurance;
- Patient age;
- Patient sex in accordance with the standard specified in § 170.207(n)(1) (HL7 Version 3);
- Patient race and ethnicity in accordance with the standards specified in § 170.207(f)(1) (OMB standard) and, at a minimum, (f)(2) (''Race & Ethnicity—CDC'' code system in the PHIN VADS);
- Patient problem list data in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4) (September 2014 Release of the U.S. Edition of SNOMED CT®); and
- Practice site address.

We clarify that a Health IT Module must be able to filter by any combination of the proposed data elements (*i.e.,* by any one (*e.g.,* provider type) or a combination of any of the data elements (*e.g.,* combination of TIN and NPI or combination of all data)). We also note that this combination requirement is different than other proposed certification criteria in that it requires all combinations to be demonstrated for certification and not just one. We anticipate that if adopted, stakeholders may want to expand the list of data in this certification criterion and support the reporting needs of additional programs over time. Our intent with this proposal is to continue to work with CMS and other stakeholders to ensure that this list of data represents a common and relatively stable set across program needs in support of program alignment.

For certain data elements, we have specified vocabulary standards (as identified above) to maintain consistency in the use of adopted national standards. As part of the 2014 Edition, technology is certified to record patient race, ethnicity, and problem lists in accordance with standards. In this proposed rule, for the ''demographics'' certification criterion and other criteria, we propose to certify a Health IT Module to record patient sex, race, and ethnicity in accordance with standards we propose to adopt as part of the 2015 Edition. We also propose to certify a Health IT Module to the record patient problem lists in accordance with the latest version of the SNOMED CT® standard. Please refer to the proposed ''demographics'' and ''problem list'' certification criteria discussed earlier in this section of the preamble for a more detailed discussion about the standards. We are also aware that patient sex, race, and ethnicity are being collected as supplemental data to the Quality Reporting Data Architecture (QRDA) Category I and III files for eCQM reporting to CMS. Collection of patient date of birth is currently required as part of the 2014 Edition ''demographics'' certification criterion, and is being proposed for the 2015 Edition ''demographics'' certification criterion. Therefore, we believe there should not be a large developmental burden to enable a Health IT Module to record these data because they are already being collected through policy established in the 2014 Edition and/or are being proposed as part of 2015 Edition certification criteria discussed elsewhere in this proposed rule.

We are aware that patient insurance can be collected using a payer value set that denotes whether the patient has Medicare, Medicaid, and/or another commercial insurance. We solicit comment on other payer value sets that could be leveraged to support this proposal. We believe that provider type could also inform quality improvement if there are differences in quality measure results by different types of providers. We are aware of the Healthcare Provider Taxonomy Code Set designed to categorize the type, classification, and/or specialization of health care providers.[133] Health care providers applying for an NPI must select a Healthcare Provider Taxonomy Code or code description during the application process. We solicit comment on the appropriateness of this code set for classifying provider types as well as other standards that could be used classify provider types.

In order to support the identification of CQM results for a particular practice, we propose to include practice site address in the list of data. We note that

[133] *http://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/Taxonomy.html*

while this information may not be needed for CQM filtering at the ACO level, certification would require that health IT enables a user to record practice site address, but not dictate that a user must include this information. We believe the industry is aware of the need to identify a standard way to represent address. While such a standard is being developed, we believe that to support group or practice reporting, having the address is one of the key data elements that would allow a provider using health IT to filter CQM results at the practice or group level. We solicit comment on standards for collecting address data that could be leveraged to support this functionality.

We solicit comment on the appropriateness of the proposed data elements for CQM filtering, including whether they are being captured in standardized vocabularies. We also solicit comment on additional data elements that we should consider for inclusion and standardized vocabularies that might be leveraged for recording this information in health IT.

- *Authentication, Access Control, and Authorization*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(1) (Authentication, access control, and authorization)

We propose to adopt a 2015 Edition ‘‘authentication, access control, and authorization’’ certification criterion that is unchanged in comparison to the 2014 Edition ‘‘authentication, access control, and authorization’’ criterion (§ 170.314(d)(1)).

- *Auditable Events and Tamper-Resistance*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(2) (Auditable events and tamper-resistance)

We propose to adopt a 2015 Edition ‘‘auditable events and tamper-resistance’’ certification criterion that is unchanged in comparison to the 2014 Edition ‘‘auditable events and tamper-resistance’’ criterion (§ 170.314(d)(2)). We seek comment, however, on two issues. In August 2014, the HHS Office of Inspector General (OIG) released a report entitled ‘‘The Office of the National Coordinator for Health Information Technology's Oversight of the Testing and Certification of Electronic Health Records.’’ [134] In that report, the OIG found that ONC approved test procedures did not address common security issues, including ‘‘logging emergency access or user privilege changes.’’ The OIG therefore recommended ‘‘. . . that ONC work with NIST to strengthen EHR test procedure requirements so that the ATCBs [ONC-Authorized Testing and Certification Bodies] can ensure that EHR vendors incorporate common security and privacy features into the development of EHRs.’’ [135]

The standards adopted at § 170.210(e) and referenced by the 2014 Edition ‘‘auditable events and tamper-resistance’’ and ‘‘audit report(s)’’ certification criteria require that technology must be able to record audit log information as specified in sections 7.2 through 7.4, 7.6 and 7.7 of the standard adopted at 45 CFR 170.210(h). The standard adopted at § 170.210(h) is ASTM E2147.[136] Section 7.6 of ASTM E2147 specifies that audit log content needs to include the ‘‘type of action’’ and references six ‘‘actions:’’ Additions, deletions, change, queries, print, and copy. Section 7.7 requires that the audit log record when patient data is accessed. So while not explicitly referenced in section 7.6, the action of ‘‘access’’ or viewing of a patient's information is also required to be recorded for certification. Moreover, we clarify that an ‘‘emergency access’’ event is expected to be recorded (just like any other access) in accordance with section 7.7.

Because it does not appear that the ASTM standard indicates recording an event when an individual's user privileges are changed, we seek comment on whether we need to explicitly modify/add to the overall auditing standard adopted at 170.210(e) to require such information to be audited or if this type of event is already audited at the point of authentication (*e.g.,* when a user switches to a role with increased privileges and authenticates themselves to the system). We also seek comments on any recommended standards to be used in order to record those additional data elements.

In a 2013 report entitled ‘‘Not All Recommended Safeguards Have Been Implemented in Hospital EHR Technology (OEI–01–11–00570),’’ [137] the OIG recommended that ONC should propose a revision to this certification criterion to require that EHR technology keep the audit log operational whenever the EHR technology is available for updates or viewing or, alternatively, CMS could update its meaningful use criteria to require providers to keep the audit log operational whenever EHR technology is available for updates or viewing.[138] As a result of that report, in the Voluntary Edition proposed rule, we proposed an ‘‘auditable events and tamper resistance’’ certification criterion that would have required technology to prevent all users from being able to disable an audit log. While several commenters supported the proposal, an equal share expressed concern, including the HITSC. The HITSC recommended against implementing this proposal, indicating that the requirements of the 2014 Edition certification criterion (identifying only a limited set of users that could disable the audit log and logging when and by whom an audit log was disabled and enabled) provided sufficient parameters to determine the accountable party in the event of a security incident.[139] Other commenters contended that including an absolute prohibition would be problematic because there are valid and important reasons for users to disable the audit log, including allowing a system administrator to disable the audit log for performance fixes, stability, disaster recovery, and system updates or allowing a system administrator to disable it when there is rapid server space loss which is hindering a provider from accessing needed clinical information in a timely manner.

We reiterate our policy first espoused with the adoption of the 2014 Edition ‘‘auditable events and tamper resistance’’ certification criterion in that the ability to disable the audit log must be restricted to a limited set of users to meet this criterion. The purpose of this certification criterion is to require health IT to demonstrate through testing and certification that it has certain security capabilities built in. As we have evaluated both OIG's input and that of commenters, we believe our certification criterion is appropriately framed within the parameters of what our regulation can reasonably impose as a condition of certification. This regulation applies to health IT and not to the people who use it. Thus, how an individual provider or entity chooses to ultimately implement health IT that has been certified to this or any other certification criterion does so outside the scope of this regulation.

[134] *http://oig.hhs.gov/oas/reports/region6/61100063.pdf*

[135] *http://oig.hhs.gov/oas/reports/region6/61100063.pdf*

[136] *http://www.astm.org/Standards/E2147.htm.* The standard is also incorporated by reference at 45 CFR 170.299(c)(1) and available at the Office of the Federal Register.

[137] *https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf.*

[138] *https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf.*

[139] *http://www.healthit.gov/FACAS/sites/faca/files/Baker_PSWG_2015editionnprm_public_comment_V2.pdf.*

We also received feedback to the Voluntary Edition proposed rule that there may be some events recorded in the audit log that may be more critical to record than other events. Commenters noted that there may be a critical subset of events that should remain enabled at all times, while other events could be turned off during critical times or for system updates by a subset of users. As noted above, the standards adopted at § 170.210(e) and referenced by the 2014 Edition ''auditable events and tamper-resistance'' certification criterion requires that health IT technology must be able to record additions, deletions, changes, queries, print, copy, access. The 2014 Edition also required the log to record when the audit log is disabled and by whom and that such capability must be restricted to a limited set of identified users. As a result, we again seek comment on whether:

- There is any alternative approach that we could or should consider;
- There is a critical subset of those auditable events that we should require remain enabled at all times, and if so, additional information regarding which events should be considered critical and why; and
- Any negative consequences may arise from keeping a subset of audit log functionality enabled at all times.
- *Audit Report(s)*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(3) (Audit report(s))

We propose to adopt a 2015 Edition ''audit reports(s)'' certification criterion that is unchanged in comparison to the 2014 Edition ''audit reports(s)'' criterion (§ 170.314(d)(3)).

- *Amendments*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(4) (Amendments)

We propose to adopt a 2015 Edition ''amendments'' certification criterion that is unchanged in comparison to the 2014 Edition ''amendments'' criterion (§ 170.314(d)(4)). We note that this certification criterion only partially addresses the amendment of protected health information (PHI) requirements of 45 CFR 164.526.

- *Automatic Access Time-Out*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(5) (Automatic access time-out)

We propose to adopt a 2015 Edition ''automatic access time-out'' certification criterion that is unchanged (for the purposes of gap certification) in comparison to the 2014 Edition ''automatic log-off'' criterion (§ 170.314(d)(5)). The 2014 Edition ''automatic log-off'' criterion requires a Health IT Module to ''prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.'' In June 2014, the Privacy and Security Workgroup (PSWG) of the HITSC assessed the automatic log-off criterion.[140] While the 2014 Edition criterion refers to ''sessions,'' the PSWG noted the need to recognize that many systems are not session-based. Instead, systems may be stateless, clientless, and/or run on any device. The PSWG further noted that the risk that this criterion addresses is the potential that protected health information could be disclosed through an unattended device. The HITSC recommended that this certification criterion should not be overly prescriptive so as to inhibit system architecture flexibility.

To clarify this intent and eliminate the reference to ''session,'' the PSWG suggested to the HITSC that this criterion by refined to state ''automatically block access to protected health information after a predetermined period of inactivity through appropriate means until the original user re-authenticates or another authorized user authenticates.'' We agree in substance with the PSWG work and HITSC recommendations. Accordingly, we propose a 2015 Edition ''automatic access time-out'' certification criterion that reflects the HITSC recommendations and the work of the PSWG. Specifically, the criterion would require a Health IT Module to demonstrate that it can automatically stop user access to health information after a predetermined period of inactivity and require user authentication in order to resume or regain the access that was stopped. We note, however, that we do not believe this would have any impact on testing and certification as compared to testing and certification to the 2014 Edition ''automatic log-off'' criterion (*i.e.,* the 2015 ''automatic access time-out'' criterion would be eligible for gap certification). We welcome comments on this assessment.

- *Emergency Access*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(6) (Emergency access)

We propose to adopt a 2015 Edition ''emergency access'' certification criterion that is unchanged in comparison to the 2014 Edition ''emergency access'' criterion (§ 170.314(d)(6)).

- *End-User Device Encryption*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(7) (End-user device encryption)

We propose to adopt a 2015 Edition ''end-user device encryption'' certification criterion that is unchanged (for the purposes of gap certification) in comparison to the 2014 Edition ''end-user device encryption'' criterion (§ 170.314(d)(7)). We propose to require certification to this criterion consistent with the most recent version of Annex A: Approved Security Functions (Draft, October 8, 2014) for Federal Information Processing Standards (FIPS) Publication 140–2.[141] The purpose of this document is to provide a list of the approved security functions applicable to FIPS PUB 140–2. To maintain and update our certification requirements to the most recent NIST-approved security functions, we propose to move to the updated version of Annex A (Draft, October 8, 2014). We proposed to adopted this updated version of Annex A at § 170.210(a)(3). We note, however, that we do not believe that this would have any impact on testing and certification as compared to testing and certification to the 2014 Edition ''end-user device encryption'' criterion (*i.e.,* the 2015 ''end-user device encryption'' criterion would be eligible for gap certification). We welcome comments on this assessment.

- *Integrity*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(8) (Integrity)

We propose to adopt a 2015 Edition ''integrity'' certification criterion that is unchanged in comparison to the 2014 Edition ''integrity'' criterion (§ 170.314(d)(8)). However, we propose a change in how a Health IT Module would be tested and certified to this criterion. The 2011 and 2014 editions of this criterion have been available for individual testing and certification. We propose that the 2015 Edition ''integrity'' criterion would be tested and certified to support the context for which it was adopted—upon receipt of a summary record in order to ensure the integrity of the information exchanged

[140] *http://www.healthit.gov/facas/sites/faca/files/HITSC_PSWG_2015NPRM_Update_2014-06-17.pdf.*

[141] *http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.*

(see § 170.315(d)(8)(ii)). Therefore, we expect that this certification criterion would most frequently be paired with the ToC certification criterion for testing and certification.

In the 2014 Edition propose rule, we sought comment on whether we should leave the standard for the 2014 Edition ''integrity'' certification criterion as SHA–1 [142] or replace it with SHA–2,[143] as SHA–2 is a much stronger security requirement. In the 2014 Edition final rule (77 FR 54251), we determined that the SHA–1 standard should serve as a floor and technology could be certified to the 2014 Edition ''integrity'' certification criterion if it included hashing algorithms with security strengths *equal to or greater than* SHA–1. We also noted that the Direct Project specification requires that SHA–1 and SHA–256 (one type of SHA–2 hash algorithms) be supported, which still remains the case today.

It is our understanding that many companies, including Microsoft and Google, plan to sunset (deprecate) SHA–1 no later than January 1, 2017.[144] While the SHA–1 standard serves as the baseline standard for certification to the proposed 2015 Edition ''integrity'' certification criterion and health IT *could* be certified to a security strength greater than SHA–1 (*e.g.,* SHA–2), we seek comments on if, and when, we should set the baseline for certification to the 2015 Edition ''integrity'' certification criterion at SHA–2. For example, we could adopt and move to SHA–2 as the baseline certification requirement with the effective date of a subsequent file rule. This would likely be in late 2015 (considering the start of testing and certification), and consistent with the current trajectory of the industry in this area. Alternatively, we could set an effective date within the criterion for when the baseline for certification would shift from SHA–1 to SHA–2 (*e.g.,* beginning 2017).

- *Accounting of Disclosures*

2015 Edition Health IT Certification Criterion
§ 170.315(d)(9) (Accounting of disclosures)

We propose to adopt a 2015 Edition ''accounting of disclosures'' certification criterion that is unchanged in comparison to the 2014 Edition ''accounting of disclosures'' criterion (§ 170.314(d)(9)). We note that the 2015 Edition criterion is no longer designated ''optional'' because such a designation is no longer necessary given that we have discontinued the Complete EHR definition and Complete EHR certification beginning with the 2015 Edition health IT certification criteria.

- *View, Download, and Transmit to 3rd Party (VDT)*

2015 Edition Health IT Certification Criterion
§ 170.315(e)(1) (View, download, and transmit to 3rd party)

We propose to adopt a 2015 Edition ''VDT'' criterion that is revised in comparison to the 2014 Edition ''VDT'' criterion (§ 170.314(e)(1)).

Clarified Introductory Text for 2015 Edition VDT Certification Criterion

In the Voluntary Edition proposed rule, we proposed to make clarifying changes to the introductory text at § 170.315(e)(1) to make it clear that this health IT capability is patient-facing and for patients to use. Commenters generally supported clarifying the introductory text of VDT. Commenters stressed the importance of allowing authorized representatives the ability to perform the VDT functionality. However, due to our approach to only finalize a subset of modifications in the 2014 Edition Release 2 final rule, we chose not to make that revision in the 2014 Edition Release 2 final rule. Therefore, we again propose to revise the introductory text to lead with ''Patients (and their authorized representatives) must be able to use health IT to . . .'' We also propose to use this same phrase at the beginning of each specific capability for VDT to reinforce this point. We note that this proposed requirement included in this criterion *does not override* an individual's right to access protected health information (PHI) in a designated record set under 45 CFR 164.524.

Common Clinical Data Set, Updated C–CDA, and Diagnostic Image Reports

We propose to include an updated Common Clinical Data Set for the 2015 Edition that includes references to new and updated vocabulary standards code sets. Please also see the Common Clinical Data Set definition proposal in section III.B.3 of this preamble. For the same reasons discussed in the proposed 2015 Edition ToC certification criterion, we also propose to reference the updated version of the C–CDA (Draft Standard for Trial Use, Release 2.0) for this certification criterion; and note, for the reasons discussed under the 2015 ToC certification criterion, compliance with Release 2.0 cannot include the use of the ''unstructured document'' document-level template for certification to this criterion.

We also propose that a Health IT Module must demonstrate that it can make diagnostic image reports available to the patient in order to be certified. A diagnostic imaging report contains a consulting specialist's interpretation of image data. It is intended to convey the interpretation to the referring (ordering) physician, and becomes part of the patient's medical record. We believe it is important to include this information in a patient's record to improve care. Therefore, we propose to include diagnostic imaging reports in the certification criterion as something a Health IT Module must be able to make accessible to patients. Again, to prevent any misinterpretation, we reiterate for stakeholders that this proposed rule and proposed certification criterion apply to a Health IT Module with regard to what must be demonstrated for the Health IT Module to be certified and does not govern its use.

We request comment on whether we should require testing and certification for the availability of additional patient data through the view, download, transmit, and API (discussed below) capabilities. For example, should patient data on encounter diagnoses, cognitive status, functional status, or other information also be made available to patients (or their authorized representatives) through these capabilities? Additionally, similar to our proposals for the data portability certification criterion, we request comment on including requirements in this criterion to permit patients (or their authorized representatives) to select their health information for, as applicable, viewing, downloading, transmitting, or API based on a specific date or time (*e.g.,* on 10/24/2015), a period of time (*e.g.,* the last 3 years), or all the information available.

VDT—Application Access to Common Clinical Data Set

To complement the API capabilities in the proposed ''Application Access to Common Clinical Data Set'' criterion at § 170.315(g)(7), which are intended to be used by health IT purchasers in the context of providing application access to the Common Clinical Data Set, we also propose to require that the same capabilities be met as part of the 2015 Edition VDT certification criterion. While in some respects it could be argued that repeating these capabilities in the VDT certification criterion are duplicative, we believe the contexts under which the capabilities proposed by this criterion and proposed at

[142] *http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.*

[143] *http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.*

[144] *http://www.symantec.com/en/au/page.jsp?id=sha2-transition.*

§ 170.315(g)(7) would be used and the contexts under which certification to this criterion would be sought are distinct enough to warrant this repetition (*i.e.,* in some cases a health IT developer may seek certification solely to this criterion). In recognition of the fact that some health IT developers will choose to build a more tightly integrated system that could rely on the same underlying capabilities developed to meet § 170.315(g)(7), we clarify that health IT developers could provide the information necessary to satisfy the ''documentation'' and ''terms of use'' requirements in § 170.315(e)(1)(iii)(D) and (E) of this criterion and § 170.315(g)(7)(iv) and (v) only once so long as the information addresses any potential technical differences in the application access capabilities provided (*e.g.,* a RESTful web service for § 170.315(e)(1) versus a SOAP web service for § 170.315(g)(7)). As proposed as part of certification in conjunction with § 170.315(g)(7), we similarly propose for this criterion to require ONC–ACBs to submit a hyperlink (as part of a product certification submission to the CHPL) that would allow any interested party to access the API's documentation and terms of use. This hyperlink would first need to be provided by the health IT developer to the ONC–ACB.

Including these capabilities in the VDT certification criterion could address several aspects that currently pose challenges to individuals (and their families) accessing their health information (*e.g.,* multiple ''portals''). Additionally, we have coordinated with CMS to have the proposed meaningful use measure for VDT revised to allow for responses to data requests executed by the API functionality to count in the measure's numerator (please see the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register**). This combination of technological capability and measurement flexibility could enhance an individual's ability to converge their data in the application of their choice. Furthermore, by including these capabilities in this criterion, we ensure that health IT developers who seek certification only to this criterion but not (g)(7) because of their market focus, will equally be required to include an API available as part of their technology.

We note that readers should also review the proposed ''API'' certification criterion in this section of the preamble for requests for comments that may impact the finalization of the API proposal included in this certification criterion. For example, we request public comment on what additional requirements might be needed to ensure the fostering of an open ecosystem around APIs so that patients can share their information with the tools, applications, and platforms of their own choosing.

Activity History Log

In the Voluntary Edition proposed rule, we proposed to include two new data elements for the activity history log: transmission status and addressee. Due to the approach we took with the 2014 Edition Release 2 final rule, we did not finalize either proposal. However, we received support for our proposal to include the addressee as a data element in the history log. Therefore, we propose to include ''addressee'' as a new data element in the 2015 Edition VDT criterion related to the activity history log. Although the 2014 Edition VDT criterion requires that the action of ''transmit'' be recorded, we did not specify that the intended destination be recorded. We believe this transactional history is important for patients to be able to access, especially if a patient actively transmits their health information to a 3rd party or another health care provider.

Patient Access to Laboratory Test Reports

In February 2014, CMS, the CDC, and the Office for Civil Rights (OCR) issued a final rule that addressed the interplay between the CLIA rules, state laws governing direct patient access to their laboratory test reports, and the HIPAA Privacy Rule.[145] The final rule permits laboratories to give a patient, a patient's ''personal representative,'' or a person designated by the patient, as applicable, access to the patient's completed test reports upon the patient's or patient's personal representative's request.[146] The final rule also eliminated the exception under the HIPAA Privacy Rule to an individual's right to access his or her protected health information when it is held by a CLIA-certified or CLIA-exempt laboratory. While patients can continue to get access to their laboratory test reports from their doctors, these changes give patients a new option to obtain their test reports directly from the laboratory while maintaining strong protections for patients' privacy.

We seek to ensure that the test reports that are delivered by providers to patients through the VDT capabilities adhere to the CLIA test reporting requirements and, therefore, propose that a Health IT Module presented for certification to this criterion must demonstrate that it can provide patient laboratory test reports that include the information for a test report specified in 42 CFR 493.1291(c)(1) through (7); the information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and the information for corrected reports as specified in 42 CFR 493.1291(k)(2).

Web Content Accessibility Guidelines (WCAG)

We reaffirm for stakeholders that the proposed 2015 Edition VDT criterion includes the WCAG 2.0 Level A (Level A) conformance requirements for the ''view'' capability. This is the same requirement we include in the 2014 Edition VDT criterion. We do, however, propose to modify the regulatory text hierarchy at § 170.204(a) to designate this standard at § 170.204(a)(1) instead of § 170.204(a). This would also require the 2014 Edition VDT certification criterion to be revised to correctly reference § 170.204(a)(1). We also seek comment on whether we should adopt WCAG 2.0 Level AA (Level AA) conformance requirements for the ''view'' capability included in the 2015 Edition VDT criterion (instead of Level A).

The most recent set of guidelines (WCAG 2.0) were published in 2008[147] and are organized under 4 central principles with testable success criteria: Perceivable, Operable, Understandable, and Robust. Each guideline offers 3 levels of conformance: A, AA, and AAA. Level A conformance corresponds to the most basic requirements for displaying Web content. Level AA conformance provides for a stronger level of accessibility by requiring conformance with Level A success criteria as well as Level AA specific success criteria. WCAG 2.0 Level AAA (Level AAA) conformance comprises the highest level of accessibility within the WCAG guidelines and includes all Level A and Level AA success criteria as well as success criteria unique to Level AAA.

In the 2014 Edition final rule (77 FR 54179) we considered public comment and ultimately adopted Level A for accessibility, but indicated our interest in raising this bar over time. As part of the Voluntary Edition proposed rule, we again proposed that health IT be compliant with Level AA for the

[145] CMS is generally responsible for regulatory laboratory oversight under CLIA, while CDC provides scientific and technical advice to CMS related to CLIA and OCR administers the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

[146] *https://www.federalregister.gov/articles/2014/02/06/2014-02280/clia-program-and-hipaa-privacy-rule-patients-access-to-test-reports.*

[147] *http://www.w3.org/TR/WCAG20/.*

proposed VDT certification criterion. We received a limited and mixed response to this proposal (79 FR 54465). In particular, some health IT developers opposed the increased level citing the cost and burden to reach Level AA, while others supported the move and offered no concerns. In both cases, health IT developers noted that WCAG conformance tools are somewhat sparse and that they have had difficulty finding viable tools.

Level AA provides a stronger level of accessibility and addresses areas of importance to the disabled community that are not included in Level A. For example, success criteria unique to Level AA include specifications of minimum contrast ratios for text and images of text, and a requirement that text can be resized without assistive technology up to 200 percent without loss of content or functionality. We recognize that Level AA is a step up from Level A, but also note that is has been nearly 3 years since we adopted Level A for the purposes of certification to the ''view'' capability. Accordingly, we once again request comment on the appropriateness of moving to Level AA for certification of the ''view'' capability included in the 2015 Edition VDT certification criterion.

We understand that there are not separate guidelines for ''mobile accessibility'' and that mobile is considered by the W3C Web Accessibility Initiative to be covered by the WCAG 2.0 guidelines.[148] Further, we would note that in September 2013, the W3C published a working group note consisting of ''Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT).'' [149] We again request public comment (especially from health IT developers that have sought or considered certification to the 2014 Edition VDT certification criterion with a ''non-web'' application) on what, if any, challenges exist or have been encountered when applying the WCAG 2.0 standards.

''Transmit'' Request for Comment

In the 2014 Edition Release 2 final rule, we modified the ''transmit'' portion of the 2014 Edition VDT certification criterion to consistently allow for C–CDA ''content'' capabilities to be separately certified from ''transport'' capabilities using Direct. In so doing, we modified the transmit portion of the certification criterion to allow it to be met in one of two ways: (1) Following the Direct Project specification (for HISPs); or (2) following the Edge Protocol IG. Given this change to ''transmit'' that we have duplicated in the proposed 2015 Edition VDT certification criterion and our proposal to include an API capability as part of the proposed 2015 Edition VDT certification criterion, we request comment on whether stakeholders believe that it would be beneficial to include the Direct Project's Implementation Guide for Direct Project Trust Bundle Distribution specification [150] as part of certification to the first way described above (following the Direct Project specification (for HISPs)) for the 2015 Edition VDT certification criterion. This trust bundle specification's focuses on ''guidance on the packaging and distribution of Trust Bundles to facilitate scalable trust between Security/Trust Agents (STAs).'' As we understand, including this specification as part of certification could enable patient-facing technology to be configured to trust externally hosted bundles of S/MIME certificates. In addition, we have continued to hear concerns regarding the difficulties related to exchanging Direct messages across platforms and ''trust communities'' in the context of patient-directed transmissions. Therefore, we also request comments on whether any additional requirements are needed to support scalable trust between STAs as well as ways in which ONC, in collaboration with other industry stakeholders, could support or help coordinate a way to bridge any gaps.

C–CDA Creation Capability Request for Comment

We request public comment on a potential means to provide explicit implementation clarity and consistency as well as to further limit potential burdens on health IT developers. Specifically, should we limit the scope of C–CDA creation capability within this certification criterion to focus solely on the creation of a CCD document template based on the C–CDA Release 2.0? This approach could also have the benefit of creating clear expectations and predictability for other health IT developers who would then know the specific document template implemented for compliance with this criterion.

C–CDA Data Provenance Request for Comment

We refer readers to the request for comment under the same heading (''C–CDA Data Provenance Request for Comment'') in the ToC certification criterion earlier in this section of the preamble (section III). The request for comment focuses on the maturity of the HL7 IG for CDA Release 2: Data Provenance, Release 1 (US Realm) (DSTU) [151] and its potential use in connection with the C–CDA.

- *Clinical Summary*

We note that we are not proposing a 2015 Edition ''clinical summary'' certification criterion because past versions of this certification criterion were adopted in direct support of the EHR Incentive Programs. The proposals found in the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register** rely on patients being provided with the ability to view, download, and transmit their health information via online access. Therefore, we believe the capabilities included in the 2015 Edition ''view, download, and transmit to 3rd party'' certification criterion appropriately and sufficiently support the proposals of the EHR Incentive Programs.

- *Secure Messaging*

2015 Edition Health IT Certification Criterion
§ 170.315(e)(2) (Secure messaging)

We propose to adopt a 2015 Edition ''secure messaging'' certification criterion that is unchanged in comparison to the 2014 Edition ''secure messaging'' criterion (§ 170.314(e)(3)).

- *Transmission to Immunization Registries*

2015 Edition Health IT Certification Criterion
§ 170.315(f)(1) (Transmission to immunization registries)

We propose to adopt a 2015 Edition ''transmission to immunization registries'' certification criterion that is revised in comparison to the 2014 Edition ''transmission to immunization registries'' criterion (§ 170.314(f)(2)). We propose to adopt an updated IG, require National Drug Codes (NDC) for recording administered vaccines, require CVX codes for historical vaccines, and require a Health IT Module presented for certification to

[148] *http://www.w3.org/WAI/mobile/.*

[149] *http://www.w3.org/TR/wcag2ict/.*

[150] *http://wiki.directproject.org/file/view/Implementation+Guide+for+Direct+Project+Trust+Bundle+Distribution+v1.0.pdf.*

[151] *http://wiki.hl7.org/index.php?title=HL7_Data_Provenance_Project_Space* and *http://gforge.hl7.org/gf/project/cbcc/frs/?action=FrsReleaseBrowse&frs_package_id=240.*

this criterion to be able to display an immunization history and forecast from an immunization registry. These proposals are described in more detail below.

Implementation Guide for Transmission to Immunization Registries

The 2014 Edition certification criterion for transmission to immunization registries at § 170.314(f)(2) references the following IG for immunization messaging: HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.4. Since the publication of the 2014 Edition final rule, the CDC has issued an updated IG (HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5) (October 2014) that promotes greater interoperability between immunization registries and health IT. Release 1.5 focuses on known issues from the previous release and revises certain HL7 message elements to reduce differences between states and jurisdictions for recording specific data elements. Specifically, Release 1.5:[152]

- Is organized into profiles, including separate profiles for VXU and ACK (acknowledgement) messages;
- Clarifies and tightens conformance statements;
- Corrects ACK (acknowledgment) messages to support improved messaging back to the EHR about the success/failure of a message; and
- Includes query and response changes such as V2.7.1 MSH user constraints, minimum requirements for a response message, and corrected profiles for response to errors and no match situations.

We believe these improvements are important to the IG and will continue to support our ultimate goal for this certification criterion—bidirectional immunization data exchange. Given the improvements included in the updated IG, we propose to adopt it at § 170.205(e)(4) and include it in the 2015 Edition ''transmission to immunization registries'' certification criterion.

National Drug Codes for Administered Vaccinations

In the Voluntary Edition proposed rule, we solicited comment for future editions on whether we should replace CVX codes for representing vaccines with NDC codes,[153] and on options for recording historical immunizations (79 FR 10908–9). NDC codes offer a number of benefits compared to CVX codes because:

- They can support pharmaceutical inventory management within immunization registries and are built into the provider's workflow;
- Are built into 2D barcodes, which have been successfully piloted for vaccines, and can improve quality and efficiency of data entry of information such as vaccine lot and expiration date; and
- Can improve patient safety with better specificity of vaccine formulation.

NDC codes also include packaging information as well as support linking to the unit of use and sale, whereas CVX codes do not provide this information as efficiently. These data elements are important for supporting vaccine inventory management.

Immunization registries are tightly linked to inventory management functions. This is largely due to the administration of the Vaccines for Children (VFC) program, a federally funded program that provides vaccines at no cost to children who might not otherwise be vaccinated because of inability to pay. CDC purchases vaccines at a discount and distributes them to grantees, which are state health departments and local and territorial public health agencies. The grantees distribute the VFC vaccines at no charge to private providers' offices and public health clinics registered as VFC providers. Because of the way this program is administered, immunization registries, which are maintained by public health agencies, have been developed to include vaccine inventory functions that help the grantees and providers manage their VFC vaccine stock. Due to the coupling of inventory functions within registries, many systems that can transmit immunization information to registries are also able to support these inventory management functions. NDC codes are used by many immunization registries to order vaccines and for inventory purposes.

We believe NDC codes for vaccines may be best suited to support immunization inventory management, as well as for providing the benefits stated above for 2D barcoding and patient safety. Both the HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5 and the C–CDA Release 2.0 IG support coding of immunizations using both CVX and NDC codes. CDC also provides a publicly available mapping of NDC codes for vaccines to CVX codes.[154]

NDC codes for vaccines include a portion that identifies the product, and thus cannot be used to code historical vaccinations of unknown formulation. Historical vaccinations are self-reported vaccinations given prior to the office visit. Patients can report historical vaccinations to providers without supporting documentation, such as a written or electronic vaccination history, and therefore the provider does not know the manufacturer and/or formulation of the product. In terms of options for recording historical vaccinations of unspecified/unknown formulation, we solicited comments on two options in the Voluntary Edition proposed rule:

- Option 1: Continue to use CVX codes for historical vaccinations only;
- Option 2: Use the NDC syntax and create a new value set for the product portion of the code for vaccines of unspecified formula (*e.g.,* influenza vaccine of unspecified formula) for historical vaccinations (resulting in an ''NDC-like'' code).

The majority of commenters were opposed to Option 2 for creating an ''NDC-like'' code. Commenters believed it would add complexity to coding NDC codes and be burdensome to maintain in the long-term. We agree with commenters and therefore believe Option 1 is a more viable solution for recording historical vaccinations. We believe health IT should be able to record historical vaccinations to provide the most complete record possible for a provider to use in determining which vaccines a patient may need.

We received comments that recommended we consider moving to RxNorm® codes for immunizations. However, RxNorm® does not support inventory management nor does it support recording historical vaccinations. Therefore, we do not believe RxNorm® is the best available option for coding vaccinations at this time.

We also received public comment that, in certain circumstances, NDC codes can be reused. Commenters expressed concerned about potential confusion for vaccine products when NDC codes are reused. In consultation with FDA, we understand that FDA does not intend to allow reuse of NDC codes for vaccine products going forward. Thus, we do not believe that reuse of NDC codes will be an issue for vaccine coding.

Given the discussion above on the benefits of NDC codes for coding vaccinations and in consideration of public comment, we propose to require for certification that a Health IT Module be able to electronically create

[152] *http://www.cdc.gov/vaccines/programs/iis/technical-guidance/downloads/hl7guide-1-5-2014-11.pdf.*

[153] *http://www.fda.gov/drugs/informationondrugs/ucm142438.htm.*

[154] *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=ndc.* See also: *http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.*

immunization information for electronic transmission to immunization registries using NDC codes for vaccines administered (*i.e.,* the National Drug Code Directory—Vaccine Codes, updates through January 15, 2015 [155]). For historical vaccines, we propose to continue the use of CVX codes and propose to adopt the HL7 Standard Code Set CVX—Vaccines Administered, updates through February 2, 2015,[156] as the baseline version for certification to the 2015 Edition. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our proposal to adopt the National Drug Code Directory—Vaccine Codes as a minimum standards code set and the ''January 15, 2015 version,'' or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition. We also refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of CVX codes as a minimum standards code set and our proposal to adopt the ''February 2, 2015 version,'' or potentially a newer version if released before a subsequent final rule, as the baseline for certification to the 2015 Edition.

In addition to soliciting comments on this proposal, we solicit comment on whether we should allow use of NDC codes for administered vaccines as an option for certification, but continue to require CVX codes for administered vaccines for the 2015 Edition. Allowing for optional use of NDC codes for administered vaccines could provide health IT developers and health care providers an implementation period before we would consider requiring NDC codes for administered vaccines. We also solicit comment on whether we should require CVX plus the HL7 Standard Code Set MVX—Manufacturers of Vaccines Code Set (October 30, 2014 version) [157] as an alternative to NDC codes for administered vaccines. MVX codes identify the manufacturer of a vaccine and support recording the vaccine at the trade name level when paired with the CVX code. MVX codes do not, however, independently include the trade name, package, or unit of use/unit of sale. CVX codes plus MVX codes could provide more information than CVX codes alone, but not as much information as NDC codes. As part of this comment solicitation, we also invite comments on the implementation burden for health IT developers and health care providers of requiring CVX plus MVX codes versus NDC codes for administered vaccines.

Immunization History and Forecast

In the Voluntary Edition proposed rule, we solicited comment on the maturity of bidirectional immunization data exchange activities and whether we should propose to include bidirectional immunization exchange in our certification rules. Commenters supported inclusion of bidirectional immunization data exchange. We understand that the HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5 we are proposing to adopt for this criterion provides improvements that support bidirectional exchange between health IT and immunization registries, including segments for querying a registry, receiving information, and sending a response to the registry. Additionally, we received comments specifically recommending that immunization forecast information and CDS guidance provide results in accordance with the Advisory Committee on Immunization Practice's (ACIP) [158] recommendations.

We believe that bidirectional exchange between health IT and immunization registries is important for patient safety and improved care. Immunization registries can provide information on a patient's immunization history to complement the data in the EHR. Immunization registries also provide immunization forecasting recommendations according to the ACIP's recommendations. This information allows for the provider to access the most complete and up-to-date information on a patient's immunization history to inform discussions about what vaccines a patient may need based on nationally recommended immunization recommendations.

Provided the discussion above, we propose that, for certification to this criterion, a Health IT Module would need to enable a user to request, access, and display a patient's immunization history and forecast from an immunization registry in accordance with the HL7 Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5. We welcome comment on this proposal. We also welcome comments on whether we should include an immunization history information reconciliation capability in this criterion and the factors we should consider regarding the reconciliation of immunization history information.

Exchange of the Common Clinical Data Set—NDC and CVX Codes

For transmission of immunization information across settings using the C–CDA standard, NDC codes carry more information than CVX codes, specifically for inventory management and safety functions (*e.g.,* trade name, package, and unit of use/unit of sale). For quality reporting of immunization coverage data using the QRDA Category I standard, inventory management data may not be needed, and therefore a CVX code is sufficient for submission of quality reporting data. However, ONC is supportive of moving towards collection of vaccine administration data within the EHR with the patient's clinical data regardless of the requirements in the QRDA Category I standard. We believe it is appropriate to use mapping from NDC codes to CVX codes and a mapping table is available.[159] We understand that the C–CDA Release 2.0 can support NDC codes as a translational data element, but the CVX code is required to accompany it. The additional information NDC codes contain could assist with vaccine tracking for clinical trials and adverse events. Therefore, we propose in a later section of this rule to include the representation of immunizations in both CVX codes and NDC codes as part of the ''Common Clinical Data Set'' definition for certification to the 2015 Edition. Please see section III.B.3 ''Common Clinical Data Set'' of this preamble for further discussion of this associated proposal. We note that this means that a Health IT Module certified to certification criteria that include the Common Clinical Data Set (*e.g.,* the ToC criterion) must demonstrate the capability to represent immunizations in CVX codes and NDC codes. This approach ensures that health IT would be able to support a provider's attempt to send immunization information that includes NDC information.

Immunization Information Certification Criterion

In response to the Voluntary Edition proposed rule, we received comments recommending we discontinue the ''immunization information'' certification criterion for future editions because the necessary data elements are enumerated in the IG for reporting to immunization registries required for the

[155] *http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.*

[156] *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx.*

[157] *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=mvx.*

[158] *http://www.cdc.gov/vaccines/acip/.*

[159] *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=ndc.* See also: *http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.*

''transmission to immunization registries'' criterion. These commenters did not see any additional value in having a standalone certification criterion for ''immunization information'' as the value lies in being able to transmit the immunization message. We agree with these comments. Therefore, we are not proposing an ''immunization information'' criterion as part of the 2015 Edition. We welcome comments on this approach.

- *Transmission to Public Health Agencies—Syndromic Surveillance*

2015 Edition EHR Certification Criterion
§ 170.315(f)(2) (Transmission to public health agencies—syndromic surveillance)

We propose to adopt a 2015 Edition certification criterion for transmission of syndromic surveillance to public health agencies that is revised in comparison to the 2014 Edition version (§ 170.314(f)(3)) for the inpatient setting. We note, however, that this proposed certification criterion is unchanged (for the purposes of gap certification) for the ambulatory setting. As discussed in the 2014 Edition Release 2 final rule, we understand that ambulatory providers may be using different methods for sending syndromic surveillance information to public health agencies, including HL7 2.5.1 and query-based messages (79 FR 54439–54441). It is our understanding that these methods are still being implemented and refined within the industry and the public health community. Therefore, given the varied adoption of methods for transmitting syndromic surveillance information to public health agencies from ambulatory settings, we propose to continue to distinguish between ambulatory and emergency department, urgent care, and inpatient settings.

Emergency Department, Urgent Care, and Inpatient Settings

We propose to adopt the PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Ambulatory Care, and Inpatient Settings, Release 2.0, September 2014 (''Release 2.0'').[160] Release 2.0 provides improvements over previous versions by:

- Re-purposing of the HL7 2.5.1 messaging structure for all type of messages/trigger events, and combining all specifications in one profile;
- Re-structuring chapters, making them more concise and placing supporting information into Appendixes;
- Adding more implementation comments and better field name descriptions within segment profile attributes;
- Making examples better aligned to the business process;
- Adding new conformance statements that simplify testing of messages;
- Making more user-friendly navigation through the document (adding a more detailed Table of Contents, updating a format of implementation comments, etc.);
- Simplifying collection and management of data by addressing requests for only using a text format for the ''Chief Complaint/Reason for Visit'' Data Element; and
- Correcting errors that were discovered in Version 1.9.

We believe these improvements are important to the IG and will continue to support interoperability and data exchange of syndromic surveillance information. As we adopted Release 1.8 of the IG in 2012 for the 2014 Edition, we believe the industry has had sufficient time to implement Release 1.8 and could benefit from the updates in Release 2.0. Release 2.0 also updates errors and known issues from Release 1.9 that commenters noted in response to the Voluntary Edition proposed rule as discussed in the Voluntary Edition final rule (79 FR 54440). Given the improvements included in Release 2.0 of the IG, we propose to adopt it at § 170.205(d)(4) and include it in the 2015 Edition ''transmission to public health agencies—syndromic surveillance'' certification criterion for emergency department, urgent care, and inpatient settings.

Ambulatory Syndromic Surveillance

We propose to permit, for ambulatory setting certification, the use of any electronic means for sending syndromic surveillance data to public health agencies as well as optional certification to certain syndromic surveillance data elements. In the 2014 Edition Release 2 final rule, we adopted a certification criterion for ambulatory syndromic surveillance at § 170.314(f)(7) that permits use of any electronic means of sending syndromic surveillance data to public health agencies for ambulatory settings (79 FR 54440–01). We adopted this criterion to provide EPs under the EHR Incentive Programs to meet the Stage 2 syndromic surveillance objective with the use of CEHRT. Because there were no IGs to support HL7 2.5.1 messaging or query-based syndromic surveillance for ambulatory settings, we expanded our policy to provide more flexibility to EPs to meet the syndromic surveillance objective.

As part of the 2014 Edition criterion, we also provide the option for technology presented for certification to demonstrate that it can electronically produce syndromic surveillance information that contains patient demographics, provider specialty, provider address, problem list, vital signs, laboratory results, procedures, medications, and insurance. Public health agencies and stakeholders that piloted query-based models for transmitting ambulatory syndromic surveillance data send all of these data elements. We offered this optional list of data elements for certification to provide clarity and a path forward to health IT developers on the data elements they should focus on for creating syndrome-based public health transmissions in support of query-based models, including any potential certification requirements introduced through future rulemaking. Due to the continued lack of mature IGs at this time, we propose to take the same approach for 2015 Edition syndromic surveillance certification for the ambulatory setting.

- *Transmission to Public Health Agencies—Reportable Laboratory Tests and Values/Results*

2015 Edition Health IT Certification Criterion
§ 170.315(f)(3) (Transmission to public health agencies—reportable laboratory tests and values/results)

We propose to adopt a 2015 Edition certification criterion that is revised in comparison to the 2014 Edition ''transmission of reportable laboratory tests and values/results'' criterion (§ 170.314(f)(4)). We have named this criterion ''transmission to public health agencies—reportable laboratory tests and values/results'' to clearly convey the capabilities included in this criterion as they relate to the intended recipient of the data. We propose to include and adopt an updated IG for laboratory reporting to public health, an updated version of SNOMED CT®, and an updated version of LOINC®. We also propose to make a technical amendment to the regulation text for the 2014 Edition criterion in order to have it continue to reference the appropriate standard and implementation specifications[161] after we restructure

[160] *http://www.cdc.gov/phin/library/guides/SyndrSurvMessagGuide2_MessagingGuide_PHN.pdf*

[161] HL7 2.5.1 and HL7 Version 2.5.1: Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 with Errata

Continued

the regulatory text hierarchy at § 170.205(g) to accommodate our 2015 Edition proposal.

CDC worked in conjunction with the HL7 Public Health Emergency Response Workgroup to develop an updated IG (HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 2 (US Realm), DSTU R1.1, 2014 or ''Release 2, DSTU R1.1'') that address technical corrections and clarifications for interoperability with laboratory orders and other laboratory domain implementation guides. Specifically, ''Release 2, DSTU R1.1'':[162]

- Corrects errata;
- Updates Objective Identifiers;
- Applies conformance statements from the LRI DSTU;
- Provides technical corrections; and
- Updates usage for consistent treatment of modifier fields.

As we adopted Release 1 of the IG in 2012 for the 2014 Edition, we believe the industry has had sufficient time to implement Release 1 and could benefit from the updates in ''Release 2, DSTU R1.1.'' Given the improvements included in the updated IG (Release 2, DSTU R1.1), we propose to adopt it at § 170.205(g)(2) and include it in the 2015 Edition ''transmission of reportable laboratory tests and values/results'' certification criterion at § 170.315(f)(3). As noted above, to properly codify this proposal in regulation, we would have to modify the regulatory text hierarchy in § 170.205(g) to designate the standard and implementation specifications referenced by the 2014 Edition ''transmission of reportable laboratory tests and values/results'' certification criterion at § 170.205(g)(1) instead of its current designation at § 170.205(g).

We propose to include the September 2014 Release of the U.S. Edition of SNOMED CT® and LOINC® version 2.50 in this criterion. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of SNOMED CT® and LOINC® as minimum standards code sets and our proposals to adopt the versions cited above, or potentially newer versions if released before a subsequent final rule, as the baselines for certification to the 2015 Edition.

- Transmission to Cancer Registries

2015 Edition Health IT Certification Criterion

§ 170.315(f)(4) (Transmission to cancer registries)

We propose to adopt a 2015 Edition ''transmission to cancer registries'' certification criterion that is revised in comparison to the 2014 Edition ''transmission to cancer registries'' certification criterion (§ 170.314(f)(6)). We propose to adopt an HL7 version cancer reporting IG, adopt an updated version of SNOMED CT®, and adopt an updated version of LOINC®. We also propose to make a technical amendment to the regulation text for the 2014 Edition certification criterion so that it continues to reference the appropriate standard[163] in the regulatory text hierarchy at § 170.205(i), while accommodating our 2015 Edition proposal. Specifically, we propose to modify the 2014 Edition certification criterion to reference § 170.205(i)(1) to establish the regulatory text hierarchy necessary to accommodate the standard and IG referenced by the proposed 2015 Edition certification criterion.

The 2014 Edition ''transmission to cancer registries'' criterion at § 170.314(f)(6) references the following IG for cancer reporting: Implementation Guide for Ambulatory Healthcare Provider Reporting to Central Cancer Registries, HL7 Clinical Document Architecture (CDA), Release 1.0. Since the publication of the 2014 Edition Final Rule, CDC worked with HL7 to introduce the IG to the standards developing organization processes. In doing so, an updated IG has been developed to address technical corrections and clarifications for interoperability with EHRs and cancer registries (HL7 Implementation Guide for CDA© Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers Release 1 or ''HL7 IG Release 1''). Specifically, HL7 IG Release 1:[164]

- Aligns with C–CDA Release 2.0 templates, where possible;
- Adds new data elements, including grade, pathologic TNM stage,[165] family history of illness, height and weight, discrete radiation oncology items, planned medications, and planned procedures;
- Changes optionality for some data elements in response to cancer community input and to align with C–CDA Release 2.0 templates;
- Improves documentation and aligns conformance statements with table constraints;
- Adds some new vocabulary links and a new reportability list for ICD–10–CM;
- Fixes some within-document references;
- Fixes some LOINC® codes;
- Fixes some Code System and Value Set Object Identifiers;
- Fixes some conformance verbs;
- Improves sample XML snippets;
- Fixes some conformance verbs and data element names in Appendix B ''Ambulatory Healthcare Provider Cancer Event Report—Data Elements''; and
- Fixes a value in the value set.

These improvements will continue to promote interoperability between health IT and cancer registries for improved cancer case reporting to public health agencies. As we adopted the non-HL7 Release 1 of the IG in 2012 for the 2014 Edition, we believe the industry has had sufficient time to implement that IG and could benefit from the updates in HL7 IG Release 1. Therefore, given the improvements that will be included in HL7 IG Release 1 as described above, we propose to adopt it at § 170.205(i)(2) and include it in the proposed 2015 Edition ''transmission to cancer registries'' certification criterion.

We propose to include the September 2014 Release of the U.S. Edition of SNOMED CT® and LOINC® version 2.50 in this criterion. We refer readers to section III.A.2.d (''Minimum Standards'' Code Sets) for further discussion of our adoption of SNOMED CT® and LOINC® as minimum standards code sets and our proposals to adopt the versions cited above, or potentially newer versions if released before a subsequent final rule, as the baselines for certification to the 2015 Edition.

Cancer Case Information

In response to the Voluntary Edition proposed rule, we received comments recommending we discontinue proposing and adopting a ''cancer case information'' certification criterion for future editions because the necessary data elements are enumerated in the IG for reporting to cancer registries that we include in editions of ''transmission to cancer registries'' criteria. We agree with this assessment. Therefore, we are not proposing a 2015 Edition ''cancer case information'' certification criterion

and Clarifications and ELR 2.5.1 Clarification Document for EHR Technology Certification.

[162] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=329.*

[163] *Standard.* HL7 Clinical Document Architecture (CDA), Release 2.0, Normative Edition (incorporated by reference in § 170.299). *Implementation specifications.* Implementation Guide for Ambulatory Healthcare Provider Reporting to Central Cancer Registries, HL7 Clinical Document Architecture (CDA), Release 1.0 (incorporated by reference in § 170.299).

[164] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=383.*

[165] The TNM Classification of Malignant Tumours (TNM) is a cancer staging system that describes the extent of a person's cancer.

similar to the one we adopted for the 2014 Edition. We welcome comments on this approach.

- *Transmission to Public Health Agencies—Case Reporting*

2015 Edition Health IT Certification Criterion

§ 170.315(f)(5) (Transmission to public health agencies—case reporting)

We propose to adopt a new certification criterion in the 2015 Edition for electronic transmission of case reporting information to public health agencies.

Health IT standards continue to evolve to address new and emerging use cases for health care. The utility of health IT for supplemental purposes has been limited due to a lack of uniformity in the terminology and definitions of data elements across health IT systems. This limitation is compounded by the fact that provider workflow often records patient information in unstructured free-text well after episodes of care. Linking data in EHR systems with other data in a uniform and structured way could accelerate quality and safety improvement, population health, and research.

Toward this end, the S&I Structured Data Capture [166] (SDC) initiative is a multi-stakeholder group working on standards-based architecture so that a set of structured data can be accessed from health IT and stored for merger with comparable data for other relevant purposes. The SDC initiative is developing a set of standards that will enable health IT to capture and store structured data. These standards will build upon and incorporate existing standards, including the IHE Retrieve Form for Data Capture (RFD) profile. As part of this work, the SDC initiative has developed a surveillance case report form for public health reporting of notifiable diseases as part of the IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation (September 5, 2014) standard.[167] The case report form can be further specified and used to electronically report vital statistics, vaccine adverse event reporting, school/camp/daycare physical, early hearing detection and intervention/newborn hearing screening, and cancer registry reporting, among other public health reporting data.

We believe that case reporting from health care providers to public health agencies could be more real-time, structured, and efficient through the use of the standard case report form that the SDC initiative has developed. Therefore, we propose to adopt a certification criterion for electronic transmission of case reporting information to public health that would require a Health IT Module to be able to electronically create case reporting information for electronic transmission in accordance with the IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation (September 5, 2014) standard, which we propose to adopt at § 170.205(q)(1). As mentioned above, this standard and our proposal include compliance with other existing standards. One such standard is the CDA Release 2.0, which is a foundational standard for use in sending and receiving case reporting information.

To note, for testing to this criterion, a Health IT Module would need to demonstrate that it can create and send a constrained transition of care document to a public health agency, accept a URL in return, be able to direct end users to the URL, and adhere to the security requirements for the transmission of this information.

We recognize that the Fast Health Interoperability Resource (FHIR®) REST API and FHIR-based standard specifications will likely play a role in an interoperable health IT architecture. FHIR resources that implement SDC concepts and support the use of case reporting to public health would likely play a role in that scenario. The current HL7 FHIR Implementation Guide: Structure Data Capture (SDC), Release 1 [168] is a ''draft for comment'' with a DSTU ballot planned for mid-2015. Given this trajectory, we solicit comment on whether we should consider adopting the HL7 FHIR Implementation Guide: SDC DSTU that will be balloted in mid-2015 in place of, or together with, the IHE Quality, Research, and Public Health Technical Framework Supplement. We are aware of a proposed HL7 working group known as the Healthcare Standards Integration Workgroup that will collaborate on FHIR resources considered co-owned with the IHE–HL7 Joint Workgroup [169] within IHE. The implementation guides created from the S&I SDC Initiative is part of this joint workgroup's area of responsibility. Therefore, we intend to work with these coordinated efforts to ensure a complementary and coordinated approach for case reporting using SDC.

- *Transmission to Public Health Agencies—Antimicrobial Use and Resistance Reporting*

2015 Edition Health IT Certification Criterion

§ 170.315(f)(6) (Transmission to public health agencies—antimicrobial use and resistance reporting)

We propose to adopt a new 2015 Edition certification criterion for transmission of antimicrobial use and resistance data to public health agencies that would require a Health IT Module to be able to electronically create antimicrobial use and resistance reporting information for electronic transmission in accordance with specific sections of the HL7 Implementation Guide for CDA ® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm (August 2013).

Collection and analysis of data on antimicrobial use and antimicrobial resistance are important components of antimicrobial stewardship programs throughout the nation and efforts by health care organizations and public health agencies aimed at detecting, preventing, and responding to resistant pathogens. Surveillance provides vital data for use by health care facilities, local, state, and federal agencies, research and development teams, policymakers, and the public. Electronic submission of antimicrobial use and antimicrobial resistance data to a public health registry can promote timely, accurate, and complete reporting, particularly if data is extracted from health IT systems and delivered using well established data exchange standards to a public health registry. The HL7 Implementation Guide for CDA ® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1—US Realm—August 2013 [170] (''HAI IG'') is an ANSI-approved standard for electronic reporting of antimicrobial use and antimicrobial resistance data to the CDC's National Healthcare Safety Network (NHSN), the largest health care-associated infection (HAI) reporting system in the United States with over 9,000 health care facilities participating. The HAI IG provides details for reporting from EPs, eligible hospitals, and CAHs.

We propose to test and certify a Health IT Module for conformance with the following sections of the IG:

[166] *http://wiki.siframework.org/Structured+Data+Capture+Initiative.*

[167] *http://www.ihe.net/uploadedFiles/Documents/QRPH/IHE_QRPH_Suppl_SDC.pdf.*

[168] *http://hl7.org/implement/standards/FHIR-Develop/sdc.html.*

[169] *http://wiki.ihe.net/index.php?title=IHE-HL7_Joint_Workgroup.*

[170] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=20.*

- HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 (pages 69–72);
- Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1 (pages 54–56); and
- Antimicrobial Use (AUP) Summary Report (Numerator and Denominator) specific document template in Section 2.1.1.2 (pages 56–58).

We propose to adopt these specific sections of the IG in § 170.205(r)(1). Note that the specific document templates referenced above include conformance to named constraints in other parts of the IG, and we would expect a Health IT Module presented for certification to this criterion to conform to all named constraints within the specified document template.

- *Transmission to Public Health Agencies—Health Care Surveys*

2015 Edition Health IT Certification Criterion
§ 170.315(f)(7) (Transmission to public health agencies—health care surveys)

We propose to adopt a new 2015 Edition certification criterion for transmission of health care surveys to public health agencies. We propose to adopt a certification criterion for transmission of health care survey information to public health agencies that would require a Health IT Module to be able to create health care survey information for electronic transmission in accordance with the HL7 Implementation Guide for CDA ® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, Draft Standard for Trial Use (December 2014),[171] which we propose to adopt at § 170.205(s)(1).

The National Ambulatory Medical Care Survey (NAMCS) is a national survey designed to meet the need for objective, reliable information about the provision and use of ambulatory medical care services in the U.S. Findings are based on a sample of visits to non-federal employed office-based physicians who are primarily engaged in direct patient care.

The National Hospital Ambulatory Medical Care Survey (NHAMCS) is designed to collect data on the utilization and provision of ambulatory care services in hospital emergency and outpatient departments. Findings are based on a national sample of visits to the emergency departments and outpatient departments of general and short-stay hospitals.

The kinds of data contained in this survey are:

- Patient demographics such as date of birth, sex, race and ethnicity;
- Vital signs such as height, weight and blood pressure;
- Reason for visit or chief complaint;
- Diagnoses associated with the visit;
- Chronic conditions that the patient has at the time of the visit;
- Procedures provided or ordered;
- Diagnostic tests ordered or provided;
- New or continued medications at the time of the visit; and
- Other variables such as tobacco use, whether the provider is the patient's primary care provider, how many times has the patient been seen in the practice in the past 12 months, which type of providers were seen at the visit, amount of time spent with the provider, and visit disposition.

Automating the survey process using the CDA standard streamlines the collection of data and increases the sample pool by allowing all providers who want to participate in the surveys to do so. The HL7 Implementation Guide for CDA ® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, Draft Standard for Trial Use (December 2014) defines the electronic submission of the data to the CDC. We clarify that the IG is intended for the transmission of survey data for both the NAMCS (*e.g.,* for ambulatory medical care settings) and NHAMCS (*e.g.,* for hospital ambulatory settings including emergency departments and outpatient departments). Templates included in this IG align with the C–CDA standard. Additionally, the templates in this IG expand on the scope of the original NAMCS and NHAMCS survey data elements and do not constrain the data collected to the narrow lists on the survey instruments; rather they allow any service, procedure or diagnosis that has been recorded.

- *Automated Numerator Recording*

2015 Edition Health IT Certification Criterion
§ 170.315(g)(1) (Automated numerator recording)

We propose to adopt a 2015 Edition ''automated numerator recording'' certification criterion that is unchanged in comparison to the 2014 Edition ''automated numerator recording'' criterion. We note, however, that the test procedure for this criterion would be different from the 2014 Edition ''automated numerator recording'' certification criterion in order to remain consistent with the applicable objectives and measures required under the EHR Incentive Programs.

- *Automated Measure Calculation*

2015 Edition Health IT Certification Criterion
§ 170.315(g)(2) (Automated measure calculation)

We propose to adopt a 2015 Edition ''automated measure calculation'' certification criterion that is unchanged in comparison to the 2014 Edition ''automated measure calculation'' criterion. We propose to apply the guidance provided for the 2014 Edition ''automated measure calculation'' certification criterion in the 2014 Edition final rule in that a Health IT Module must be able to support all CMS-acceptable approaches for measuring a numerator and denominator in order for the Health IT Module to meet the proposed 2015 Edition ''automated measure calculation'' certification criterion.[172] We also propose that the interpretation of the 2014 Edition ''automated measure calculation'' certification criterion in FAQ 32 [173] would apply to the proposed 2015 Edition ''automated measure calculation'' certification criterion.

We note that the test procedure for this criterion would be different from the 2014 Edition ''automated measure calculation'' certification criterion in order to remain consistent with the applicable objectives and measures required under the EHR Incentive Programs.

- *Safety-Enhanced Design*

2015 Edition Health IT Certification Criterion
§ 170.315(g)(3) (Safety-enhanced design)

We propose to adopt a 2015 Edition ''safety-enhanced design'' (SED) certification criterion that is revised in comparison to the 2014 Edition ''safety-enhanced design'' criterion. We propose to add certification criteria to this criterion that we believe include capabilities that pose a risk for patient harm and, therefore, an opportunity for error prevention. We propose to provide further compliance clarity for the data elements described in NISTIR 7742 [174] that are required to be submitted as part of the summative usability test results and to specifically include these data

[171] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=385.*

[172] 77 FR 54244–54245.

[173] *http://www.healthit.gov/policy-researchers-implementers/32-question-11-12-032.*

[174] *http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907312.* NISTIT 7742 is a valid and reliable publication for user-centered design processes.

elements as part of the certification criterion.

Certification Criteria Identified in the SED Criterion for UCD Processes

We propose to include seventeen (17) certification criteria (seven are new) in the 2015 Edition SED certification criterion, as listed below (emphasis added for new criteria). For each of the referenced certification criteria and their corresponding capabilities presented for certification, user-centered design (UCD) processes must have been applied in order satisfy this certification criterion.

- § 170.315(a)(1) Computerized provider order entry—medications
- § 170.315(a)(2) Computerized provider order entry—laboratory
- § 170.315(a)(3) Computerized provider order entry—diagnostic imaging
- § 170.315(a)(4) Drug-drug, drug-allergy interaction checks
- *§ 170.315(a)(5) Demographics*
- *§ 170.315(a)(6) Vital signs, BMI, and growth charts*
- *§ 170.315(a)(7) Problem list*
- § 170.315(a)(8) Medication list
- § 170.315(a)(9) Medication allergy list
- § 170.315(a)(10) Clinical decision support
- § 170.315(a)(18) Electronic medication administration record
- *§ 170.315(a)(20) Implantable device list*
- *§ 170.315(a)(22) Decision support—knowledge artifact*
- *§ 170.315(a)(23) Decision support—service*
- § 170.315(b)(2) Clinical information reconciliation and incorporation
- § 170.315(b)(3) Electronic prescribing
- *§ 170.315(b)(4) Incorporate laboratory tests/results*

The continued submission of summative usability test results promotes transparency and can foster health IT developer competition, spur innovation, and enhance patient safety. With this in mind, we also seek comment on whether there are other certification criteria that we omitted from this proposed SED criterion that commenters believe should be included.

NISTIR 7742 Submission Requirements

In the 2014 Edition final rule, we specified that the information listed below from the NISTIR 7742 ''Customized Common Industry Format Template for Electronic Health Record Usability Testing'' (NIST 7742)[175] was required to be submitted for each and every one of the criteria specified in the 2014 Edition SED criterion (77 FR 54188). For the 2015 Edition SED criterion, we propose to include the information below in the regulation text of the 2015 Edition SED criterion to provide more clarity and specificity for the information requested to be provided to demonstrate compliance with this certification criterion. The findings that would be required to be submitted for each and every one of the criteria specified in the 2015 Edition SED criterion (and become part of the test results publicly available on the Certified Health IT Product List (CHPL)) are:

- Name and version of the product
- Date and location of the test
- Test environment
- Description of the intended users
- Total number of participants
- Description of participants as follows:
  - Sex
  - Age
  - Education
  - Occupation/role
  - Professional experience
  - Computer experience
  - Product experience
- Description of the user tasks that were tested and association of each task to corresponding certification criteria
- List of the specific metrics captured during the testing
  - Task Success (%)
  - Task Failures (%)
  - Task Standard Deviations (%)
  - Task Performance Time
  - User Satisfaction Rating (Scale with 1 as very difficult and 5 as very easy)
- Test results for each task using metrics listed above
- Results and data analysis narrative:
  - Major test finding
  - Effectiveness
  - Efficiency
  - Satisfaction
  - Areas for improvement

There are illustrative tables on pages 11 and 20 in NISTIR 7742 that provide examples of the presentation of test participants and test results data. We specify that all of the data elements and sections specified above must be completed, including ''major findings'' and ''areas for improvement.'' Pages 18 and 19 of the NISTIR 7742 contain a table with suggested instructions for data scoring specifically noting that for task success, a task is counted as successful if the participant was able to achieve the correct outcome without assistance and within the time allotted on a per task basis. Likewise, for task satisfaction a 5 point Likert scale is recommended with scores ranging from ''1—very difficult'' to ''5—very easy.''

The NISTIR 7742 includes several sections: Executive Summary, Introduction, Method, and Results. In each of these sections, there are required data elements—and some of these elements call for the reporting of the number of study participants, their level of experience with EHR technology and other pertinent details.

We recommend following NISTIR 7804[176] ''Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records'' for human factors validation testing of the final product to be certified. In accordance with this guidance, we recommend a minimum of 15 representative test participants for each category of anticipated clinical end users who conduct critical tasks where the user interface design could impact patient safety (*e.g.,* physicians, nurse practitioners, physician assistants, nurses, etc.). The cohort of users who are selected as participants will vary with the product and its intended users; however, the cohort should not include employees of the developer company. We specify the submission of demographic characteristics of the test participants comparable to the table on page 11 of NISTIR 7742 because it is important that the test participant characteristics reflect the audience of current and future users. In accordance with NISTIR 7804 (page 8), we recommend that the test scenarios be based upon an analysis of critical use risks for patient safety which can be mitigated or eliminated by improvements to the user interface design.

In lieu of simply providing guidance on the number of, and user cohort for, test participants, we request comment on whether we should establish a minimum number(s) and user cohort(s) for test participants for the purposes of testing and certification to the 2015 Edition under the ONC Health IT Certification Program.

New Requirements and Compliance Guidance

As we noted in the 2014 Edition final rule (77 FR 54188), examples of method(s) that could be employed for UCD include ISO 9241–11, ISO 13407, ISO 16982, ISO/IEC 62366, ISO 9241–210 and NISTIR 7741. The UCD process selected by a health IT developer need not be listed in the examples provided in order to be acceptable. We do, however, strongly advise health IT developers to select an industry standard process because compliance

[175] *http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907312.*

[176] *http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909701.*

with this certification criterion requires submission of the name, description, and citation (URL and/or publication citation) of the process that was selected. In the event that a health IT developer selects a UCD process that is not an industry standard (that is, not developed by a voluntary consensus standards organization), but is based on one or more industry standard processes, the developer may name the process(es) and provide an outline of the process in addition to a short description as well as an explanation of the reason(s) why use of any of the existing UCD standards was impractical.

Health IT developers can perform many iterations of the usability testing, but the submission that is ultimately provided for summative usability testing and certification must be an expression of a final iteration. In addition, we expect the test scenarios used to be submitted as part of the test results. Last, we note that we do not expect developers to include trade secrets or proprietary information in the test results.

Request for Comment on Summative Testing

We understand that some health IT developers are concerned that the summative testing report may not adequately reflect the design research that has been performed throughout a product's lifecycle. We request public comment regarding options that we might consider in addition to—or as alternatives to—summative testing. For example, if formative testing reflects a thorough process that has tested and improved the usability of a product, could a standardized report of the formative testing be submitted for one or more of the 17 certification criteria for which summative testing is now required? What would be the requirements for this formative testing report, and how would purchasers evaluate these reports?

Retesting and Certification

We believe that ONC–ACB determinations related to the ongoing applicability of the SED certification criterion to certified health IT for the purposes of inherited certified status (§ 170.550(h)), adaptations and other updates would be based on the extent of changes to user-interface aspects of one or more capabilities to which UCD had previously been applied. We believe that ONC–ACBs should be notified when applicable changes to user-interface aspects occur. Therefore, we include these types of changes in our proposal to address adaptations and updates under the ONC–ACB Principles of Proper Conduct (§ 170.523). Please see section IV.D.6 of this preamble for further discussion of this proposal.

- *Quality Management System*

2015 Edition Health IT Certification Criterion

§ 170.315(g)(4) (Quality management system)

We propose to adopt a 2015 Edition ''quality management system'' certification criterion that is revised in comparison to the 2014 Edition ''quality management system'' criterion. We propose to require, for a Health IT Module presented for certification, the identification of the Quality Management System (QMS) used in the development, testing, implementation, and maintenance of capabilities certified under the ONC Health IT Certification Program. The identified QMS must be:

- Compliant with a quality management system established by the federal government or a standards developing organization; or
- mapped to one or more quality management systems established by the federal government or standards developing organization(s).

In the 2014 Edition final rule, we stated that the 2014 Edition QMS criterion was a first step that could be built on in an incremental fashion (77 FR 54191). For the 2015 Edition QMS criterion, we are taking that next step by *not* permitting health IT to be certified that has not been subject to a QMS and also requiring health IT developers to either use a recognized QMS or illustrate how the QMS they used maps to one or more QMS established by the federal government or a standards developing organization(s) (SDOs). As identified in the 2014 Edition final rule (77 FR 54190), QMS established by the federal government and SDOs include FDA's quality system regulation in 21 CFR part 820, ISO 9001, ISO 14971, ISO 13485, and IEC 62304. We encourage health IT developers to choose an established QMS, but developers are not required to do so, and may use either a modified version of an established QMS, or an entirely ''home grown'' QMS. In cases where a health IT developer does not use a QMS established by the federal government or an SDO, the health IT developers must illustrate how their QMS maps to one or more QMS established by the federal government or SDO through documentation and explanation that links the components of their QMS to an established QMS and identifies any gaps in their QMS as compared to an established QMS. We clarify that we have no expectation that there will be detailed documentation of historical QMS or their absence. The documentation of the current status of QMS in a health IT development organization would be sufficient.

We propose that all Health IT Modules certified to the 2015 Edition would need to be certified to the 2015 Edition QMS criterion. As such, we propose to revise § 170.550 to require ONC–ACBs follow this proposed approach (please see section IV.C.2 of this preamble for this proposal).

- *Accessibility Technology Compatibility*

2015 Edition Health IT Certification Criterion

§ 170.315(g)(5) (Accessibility technology compatibility)

We propose to adopt a new 2015 Edition ''accessibility technology compatibility'' certification criterion that would offer health IT developers that present a Health IT Module for certification to one or more certification criteria listed in proposed § 170.315(a), (b), or (e) the opportunity to have their health IT demonstrate compatibility with at least one accessibility technology for the user-facing capabilities included in the referenced criteria.

In response to the Voluntary Edition proposed rule, we received several comments from health IT users with visual impairments or disabilities. These commenters raised concerns about the lack of accessibility in many health IT products certified under the ONC Health IT Certification Program. Commenters suggested a number of ways in which the certification program could be leveraged to ensure that health IT is accessible to visually impaired and disabled individuals. In particular, many commenters strongly recommended that we require as a condition of certification that health IT be compatible with popular text-to-speech (or ''screen reader'') applications and other accessibility technologies.

Joined by our colleagues in the Administration for Community Living and Aging Policy and the Office for Civil Rights, we believe that health IT should be accessible to users regardless of their visual impairments or disabilities. The lack of accessibility features in health IT, including the lack of compatibility with third-party accessibility technologies, can place a significant burden on health IT users who are visually impaired or disabled. Without these features, some health IT users may be unable to access the health IT capabilities they and their patients need. Other health IT users may be forced to rely on human intermediaries, revert to paper-based processes, or employ other workarounds in order to perform basic clinical tasks and essential aspects of their jobs. Such limitations and workarounds not only impact the autonomy, productivity, and employment opportunities of health IT users, but also jeopardize patient safety, healthcare quality, and efficiency. For example, without the use of appropriate accessibility technology, there may be an increased risk of transcription errors, miscommunication between clinicians, improperly documented patient health information, and untimely retrieval of patient health information. For these reasons, we strongly encourage health IT developers to consider the needs of visually impaired and disabled users when designing their products, and, where feasible, to integrate accessibility features directly into health IT. We also encourage them to seek certification to this proposed certification criterion.

We note that a number of text-to-speech applications exist and are widely used by many visually impaired or otherwise disabled individuals in conjunction with a variety of personal computer and mobile applications that lack built-in accessibility features. Text-to-speech applications may also be combined with voice control software and other accessibility technologies and typically provide a scripting language and/or set of APIs that enable third-party developers to leverage the accessibility technology's accessibility features in their own software applications. We have also observed that some health IT is already compatible with accessibility technology, including the U.S. Department of Veterans Affairs' Computerized Patient Record System (CPRS). CPRS is compatible with Job Access With Speech (JAWS), a popular text-to-speech application that enables a computer to verbally describe the controls and content of computer applications.

Certification to this proposed criterion would be available (not required) for Health IT Modules presented for certification to any of the clinical, care coordination, and patient engagement certification criteria specified at § 170.315(a), (b), and (e), respectively, because the use of capabilities associated with these criteria necessarily requires that a user provide input into, receive feedback from, or otherwise interact with the Health IT Module. To meet this proposed certification criterion, for each such ''user-facing'' capability included in certification criteria specified at § 170.315(a), (b), and (e), a Health IT Module would need to demonstrate that the capability is *compatible* with at least one accessibility technology that provides text-to-speech functionality to meet this criterion. Health IT developers would not be required to license or provide such accessibility technology to users in order to meet the criterion. An accessibility technology used to meet this criterion would also *not* be ''relied upon'' for purposes of § 170.523(f). However, it would need to be identified in the issued test report and would ultimately be made publicly available as part of the information ONC–ACBs are required to report to ONC for inclusion on the CHPL (in this case, what was used to demonstrate compliance with this certification criterion) so that users would be able to identify the accessibility technology with which the certified Health IT Module demonstrated its compatibility.

We note that all recipients of federal financial assistance from HHS are covered by the requirements of Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. 794) for programs and services receiving federal financial assistance. We seek comment on the extent to which certification to this criterion would assist in complying with this and other applicable federal (*e.g.,* Section 508 of the Rehabilitation Act of 1973) and state disability laws. We also seek comment on whether certification to this criterion *as proposed* would serve as a valuable market distinction for health IT developers and consumers (*e.g.,* ''Health IT Module with certified accessibility features'').

- *Consolidated CDA Creation Performance*

2015 Edition Health IT Certification Criterion
§ 170.315(g)(6) (Consolidated CDA creation performance)

In the Voluntary Edition proposed rule (79 FR 10899), we proposed to adopt as part of the transitions of care certification criterion a new ''performance standard'' at § 170.212. This performance standard would have required health IT to be able to receive no less than 95% of all of the possible variations that could be implemented under the C–CDA. We summarized in the 2014 Edition Release 2 final rule (79 FR 54459) that commenters voiced concerns about the testability and vagueness of this proposed requirement, questioned its likelihood of success, and noted that the 95% threshold would be impractical, time consuming, and expensive to implement given the wide variation in C–CDA implementation. Ultimately, we did not finalize this proposal in the 2014 Edition Release 2 final rule.

As we considered these comments and reviewed the additional public dialogue surrounding the variability in the C–CDA's implementation by different health IT developers,[177] we concluded that a new certification criterion, focused principally on health IT system behavior and performance related to C–CDA creation was warranted. Thus, we propose to adopt a new certification criterion at § 170.315(g)(6) that would rigorously assess a product's C–CDA creation performance (for both C–CDA Release 1.1 and 2.0) when it is presented for a Health IT Module certification that includes within its scope any of the proposed certification criteria that require C–CDA creation (*e.g.,* § 170.315(b)(2)).

To implement this proposal, we also propose to amend § 170.550 to add a requirement that ONC–ACBs shall *not* issue a Health IT Module certification to a product that includes C–CDA creation capabilities within its scope, unless the product was also tested and satisfied the certification criteria requirements proposed at § 170.315(g)(6) (see also section IV.C.2 of this preamble for further discussion of this proposal). If the scope of certification sought includes multiple certification criteria that require C–CDA creation, § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each. We base this certification efficiency on assumption that passing this proposed certification criterion for one of the certification criteria that includes C–CDA creation will cause a health IT developer to apply these same performance checks to all other capabilities that include C–CDA creation. However, we request public comment on whether this proposed efficiency is desirable or would have any adverse consequences.

We propose that the C–CDA creation performance certification criterion would focus on and require the following technical outcomes to be met:

1. *Reference C–CDA Match:* the Health IT Module must demonstrate that it can create a C–CDA that matches a gold standard, called a Reference C–CDA. Reference C–CDAs would include the 2014 and 2015 edition data elements coded according to the HL7 C–CDA standards and regulatory requirements (the scope of the data would be limited

[177] D'Amore JD, et al. J Am Med Inform Assoc 2014; 21:1060-1068.

to what is proposed for the Common Clinical Data Set definition). As part of the Reference C–CDA Match, health IT developers would be provided test data that includes the 2014 and 2015 data elements and any context specific coding instructions to be used by Health IT Module to create C–CDA documents. The C–CDA documents created by the Health IT Module would be validated by comparing it to a Reference C–CDA.

2. *Document Template Conformance:* the Health IT Module must demonstrate that it can create C–CDA documents for the following C–CDA document templates as applicable to the C–CDA 1.1 and C–CDA 2.0 standards: CCD; Consultation Note; History and Physical; Progress Note; Care Plan; Transfer Summary; Referral Note; and for the inpatient setting only, Discharge Summary. We do not propose require as part of this portion of the certification criterion to require testing to the Diagnostic Imaging Report (DIR); Operative Note; and Procedure Note as they would not be generally applicable to all products.

3. *Vocabulary Conformance:* the Health IT Module must demonstrate that it can create C–CDA documents using the vocabularies and value sets adopted by the 2014 and 2015 edition. For data elements which do not require specific vocabularies and value sets in the regulation, the Health IT Module must use the vocabularies and value sets as specified in the C–CDA standard.

Additionally, in response to wide stakeholder feedback for additional publicly available C–CDA samples, we have coordinated with our colleagues at NIST and understand that NVLAP-Accredited Testing Laboratories would retain the C–CDA files created under test and contribute them to an ONC-maintained repository.

Completeness of Data in the C–CDA

Past feedback from providers has indicated that the variability associated with different functionalities and workflows within health IT can ultimately affect the completeness of the data included in a created C–CDA. Thus, in the same context associated with our proposals in this criterion and the ToC performance certification criterion, we are considering, and request public comment on, adding to either of these certification criteria an additional requirement that would evaluate the completeness of the data included in a C–CDA in order to ensure that the data recorded by health IT is equivalent to the data included in a created C–CDA.

- *Application Access to Common Clinical Data Set*

2015 Edition Health IT Certification Criterion
§ 170.315(g)(7) (Application access to Common Clinical Data Set)

We propose to adopt a new certification criterion as part of the proposed 2015 Edition at § 170.315(g)(7) that would focus on the capability of health IT presented for certification to respond to requests for patient data from other applications.[178] We propose that this certification criterion would require the demonstration of an application programming interface (API) that responds to data requests for any one or more of the data referenced in the Common Clinical Data Set definition (proposed for adoption at § 170.102), including requests for all of the data referenced in the Common Clinical Data Set.

The expanded access to a common data set from other applications through APIs (and other techniques) has been referenced in numerous publications over the past several years.[179] We have also received requests from stakeholders to include a certification requirement for the proposed capability. These stakeholders indicate that such a requirement would help promote innovation and enhance the ease with which health care providers could adopt and use third party software tools along with their core EHR technology to improve patient care.

For the purposes of this certification criterion, we also propose to require that this certification criterion be part of the set of criteria necessary to satisfy the ‘‘2015 Edition Base EHR’’ definition (see also section III.B.1 of this preamble for a discussion of the proposed 2015 Edition Base EHR definition). This additional proposal, due to its linkage to the CEHRT definition, would ensure that all EPs, eligible hospitals, and CAHs would need to adopt a Health IT Module certified to this criterion in order to have the necessary health IT to successfully demonstrate meaningful use under the EHR Incentive Programs.

With limited exceptions, we have broadly specified the technical outcomes required by this certification criterion. We have taken this approach in order to allow for a wide array of implementations to meet the certification criterion. The proposed certification criterion includes three technical outcomes and a documentation requirement.

(1) *Security.* The API needs to include a means for the establishment of a trusted connection with the application that requests patient data. This would need to include a means for the requesting application to register with the data source, be authorized to request data, and log all interactions between the application and the data source.

(2) *Patient Selection.* The API would need to include a means for the application to query for an ID or other token of a patient's record in order to subsequently execute data requests for that record.

(3) *Data requests, response scope, and return format.* The API would need to support two types of data requests and responses: ‘‘by data category’’ and ‘‘all.’’ In both cases, while the scope required for certification is limited to the data specified in the Common Clinical Data Set, additional data is permitted and encouraged.

- For ‘‘data category’’ requests, the API would need to respond to requests for each of the data categories specified in the Common Clinical Data Set (according to the specified standards, where applicable) and return the full set of data for that data category. As the return format, either XML or JSON would need to be produced. For example, an API function to request ‘‘medications’’ from patient 123456 that returns all of a patient's medications in XML or JSON would meet certification requirements.
- For ‘‘all’’ requests, the API would need to respond to requests for all of the data categories specified in the Common Clinical Data Set at one time (according to the specified standards, where applicable). As the return format, the C–CDA version 2.0 would need to be used to produce a patient summary record populated with the data included in the Common Clinical Data Set. For example, an API function to request the full common data set ‘‘all’’ from patient 567890 would return a patient's fully populated summary record formatted in accordance with the C–CDA version 2.0.

We believe the proposed approach provides ample flexibility for health IT developers to implement an API that can best address their customers' needs. It also leverages current standards that most health IT developers would

[178] We intend for the term ‘‘application’’ to generally encompass any other type of system or software that is not the data source responding to the requests for data.

[179] See: (1) President's Council of Advisors on Science and Technology (PCAST) ‘‘Realizing the full potential of health information technology to improve healthcare for Americans: the path forward (December 2010)’’;

(2) JASON: A Robust Health Data Infrastructure (April 2014);

(3) PCAST ‘‘Better health care and lower costs: accelerating improvement through systems engineering (May 2014); and

(4) ONC ‘‘Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable Health IT Infrastructure (June 2014).

already need to develop their products to support in order to seek certification to several other certification criteria. In addition, we believe that this approach supports future, innovative approaches to be used. The intent behind this certification criterion is to allow for, but not require, health IT developers to implement the Fast Health Interoperability Resource (FHIR®) REST API and accompanying FHIR standard specifications.[180] Therefore, if we have not adequately specified this certification criterion in a manner that accomplishes this goal, we solicit public comment on any specific revisions that would.

This certification criterion would require that the API be technically well documented and include its terms of use. It would also require that such technical documentation and the terms of use be submitted as part of testing for this certification criterion and subsequently to ONC–ACBs for review prior to issuing a certification. The technical documentation would need to include, at a minimum: API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns. The terms of use would need to include information of the API's developer policies and required developer agreements so that third party developers could assess these additional requirements before engaging in any development against the API. Similar to how we approached the submission of publicly available test results in our past rulemaking, we propose to require ONC–ACBs to submit a hyperlink (as part of its product certification submission to the CHPL) that would allow any interested party to access the API's documentation and terms of use. This hyperlink would need to be provided by the health IT developer to the ONC–ACB.

With respect to testing for this certification criterion, we expect that functional testing would focus primarily on the third capability we propose. Meaning that for each function call made the health IT developer would need to demonstrate to/show an Accredited Testing Lab the response (*i.e.,* output) for each of the data category requests in JSON or XML and for the ''all'' request, the output according to the Consolidated CDA. For all other aspects of the certification criterion, we expect the testing would include attestation, documentation, and review. Additionally, if these capabilities do not function properly when implemented in the field, the (at that point) certified Health IT Module could be subject to surveillance by its ONC–ACB.

The HITPC called for ''well-defined, fairly applied, business and legal frameworks for using the API.''[181] We request public comment on what additional requirements might be needed to ensure the fostering of an open ecosystem around APIs so that patients can share their information with the tools, applications, and platforms of their own choosing. For instance, should there be any limits expressed on what can be included in the terms of use? Should the terms be required to more granularly address security and authorization requirements, for instance by requiring a certain oAuth profile?

We also request public comment regarding the feasibility of additional API capabilities that could be made available to certification including secure message read/write capability, schedule read/write capability, ordering/e-prescribing capability, and task list read/write capability.

C–CDA Creation Capability Request for Comment

We request public comment on a potential means to provide explicit implementation clarity and consistency as well as to further limit potential burdens on health IT developers. Specifically, should we limit the scope of C–CDA creation capability within this certification criterion to focus solely on the creation of a CCD document template based on the C–CDA Release 2.0? This approach could also have the benefit of creating clear expectations and predictability for other health IT developers who would then know the specific document template implemented for compliance with this criterion.

- *Accessibility-Centered Design*

2015 Edition EHR Certification Criterion
§ 170.315(g)(8) (Accessibility-centered design)

We propose to adopt a new 2015 Edition ''accessibility-centered design'' certification criterion that would apply to all Health IT Modules certified to the 2015 Edition. This criterion would require the identification of user-centered design standard(s) or laws for accessibility that were applied, or complied with, in the development of specific capabilities included in a Health IT Module or, alternatively, the lack of such application or compliance.

This proposed certification criterion would serve to increase transparency around the application of user-centered design standards for accessibility to health IT and the compliance of health IT with accessibility laws. We believe this transparency would be beneficial for those health care providers, consumers, governments, and other stakeholders that have an interest in knowing the degree to which heath IT, particularly certified health IT, meet health IT accessibility standards and laws. This transparency may also encourage health IT developers to pursue the application of more accessibility standards and laws in product development that could lead to improved usability for health care providers with disabilities and health care outcomes for patients with disabilities.

We propose to model our approach and this criterion after the 2014 Edition ''quality management system'' criterion (§ 170.314(g)(4) and see 77 FR 54270–54271). Therefore, as a first step, for each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or compliance with a health IT accessibility law in the development, testing, implementation, and maintenance of that capability must be identified. Working with our colleagues at NIST, we have identified an initial list of health IT accessibility-centered design standards and accessibility laws below. However, health IT developers may choose to use other health IT accessibility standards or laws in the development, testing, implementation, and maintenance of capabilities, but must identify these standards and/or laws for the purposes of certification. As with the 2014 Edition ''quality management system'' criterion, we propose to permit a response that ''no health IT accessibility-centered design standard or law was applied to all applicable capabilities'' as an acceptable means of satisfy this proposed certification criterion. We note, however, that whatever method(s) is used to meet this proposed criterion, it would be reported to the proposed open data CHPL.

We solicit comments on whether the standards and laws identified below are appropriate examples and whether we should limit the certification criteria to which this criterion would apply. For example, limiting it to a Health IT Module certified only to the certification criteria proposed in § 170.315(a), (b), (c), and (e), or

[180] *http://www.hl7.org/implement/standards/fhir/.*

[181] *http://www.healthit.gov/sites/faca/files/JTF_Transmittal%20Letter_2014-1-22-15v3.pdf.*

otherwise. To note, we believe that, at a minimum, this criterion would not apply to the certification criteria in § 170.315(g).

Example health IT accessibility-centered design standards and accessibility laws:

- ETSI ES 202 076—Human Factors (HF); User Interfaces; Generic spoken command vocabulary for ICT devices and services;
- ETSI ETS 300 679—Terminal equipment (TE); Telephony for the hearing impaired; Electrical coupling of telephone sets to hearing aids;
- ETSI TR 102 068 (2002) Human Factors (HF): Requirements for assistive technology devices in ICT;
- ETSI TS 102 511 (2007) Human Factors (HF): AT commands for assistive mobile device interfaces;
- IEEE 802.11 IEEE standard for Information Technology; Telecommunications and information: Exchange between systems; local and metropolitan area network; specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification;
- ISO 13406–1 (1999) Ergonomic requirements for work with visual displays based on flat panels. Part 1—Introduction;
- ISO 13406–2 (2001) Ergonomic requirements for work with visual displays based on flat panels. Part 2—Ergonomic requirements for flat panel displays;
- IEC 80416–1 (2001) Basic principles for graphical symbols for use on equipment—Part 1: Creation of symbol originals;
- ISO 80416–2 (2002) Basic principles for graphical symbols for use on equipment—Part 2: Form and use of arrows;
- IEC 80416–3 (2002) Basic principles for graphical symbols for use on equipment—Part 3: Guidelines for the application of graphical symbols;
- ISO 80416–4 (2005) Basic principles for graphical symbols for use on equipment. Part 4—Guidelines for the adaptation of graphical symbols for use on screens and displays;
- ISO 9241–151 (2008) Ergonomics of human-system interaction—Part 151: Guidance on World Wide Web user interfaces;
- ISO 9355–1 (1999) Ergonomic requirements for the design of displays and control actuators. Part 1: Human interactions with displays and control actuators;
- ISO 9355–2 (1999) Ergonomic requirements for the design of displays and control actuators. Part 2: Displays;
- ISO 9999 (2007) Assistive products for persons with disability—Classification and terminology;
- ISO/CD 24500 Guidelines for all people, including elderly persons and persons with disabilities—Auditory signals on consumer products;
- ISO/IEC 15411 (1999) Information technology—Segmented keyboard layouts;
- ISO/IEC 15412 (1999) Information technology—Portable keyboard layouts;
- ISO/IEC 24755 (2007) Information technology—Screen icons and symbols for personal mobile communication devices;
- ISO/IEC CD 24786–1 Information Technology—User interfaces—Accessible user interface for accessibility setting on information devices—Part 1: General and methods to start;
- ISO/IEC TR 15440 (2005) Information Technology—Future keyboards and other associated input devices and related entry methods;
- ISO/IEC TR 19765 (2007) Information technology—Survey of icons and symbols that provide access to functions and facilities to improve the use of IT products by the elderly and persons with disabilities;
- ISO/IEC TR 19766 (2007) Information technology—Guidelines for the design of icons and symbols accessible to all users, including the elderly and persons with disabilities;
- ITU–T E.902 (1995) Interactive services design guidelines;
- ITU–T P.85 (1994) A method for subjective performance assessment of the quality of speech voice;
- Section 504 of the Rehabilitation Act; and
- Section 508 of the Rehabilitation Act.

Because we propose that Health IT Modules certified to the 2015 Edition would be required to be certified to the 2015 Edition Accessibility-centered design criterion, we also propose to revise § 170.550 to require ONC–ACBs follow this proposed approach (please see section IV.C.2 of this preamble for this proposal).

- *Transport Methods and Other Protocols*

We propose two ways for providers to meet the 2015 Edition Base EHR definition using health IT certified to transport methods. These ways serve to account for transport methods that we understand are being used to readily exchange electronic health information and ensure that providers have interoperable ways to exchange electronic health information. The first way to meet the proposed 2015 Edition Base EHR definition requirement would be for a provider to have health IT certified to § 170.315(b)(1) and (h)(1) (Direct Project specification). This would account for situation where a provider uses a health IT developer's product that acts as the ''edge'' *and* the HISP. The second way would be for a provider to have health IT certified to § 170.315(b)(1) (ToC criterion) and (h)(2) (Direct Project, Edge Protocol, and XDR/XDM). This would account for situations where a provider is using one health IT developer's product that serves as the ''edge'' and another health IT developer's product that serves as a HISP.[182] The capabilities included in proposed § 170.315(h)(2) ensure interoperability by accounting for various electronic health information exchange options using the Direct Project specification. To fully implement this approach, we propose to revise § 170.550 to require an ONC–ACB to ensure that a Health IT Module includes the certification criterion adopted at § 170.315(b)(1) in its certification's scope in order to be certified to the certification criterion proposed for adoption at § 170.315(h)(1). We welcome comment on these proposed approaches and the transport standards listed below in § 170.315(h)(1) through (3).

Consistent with our proposed title of ''transport methods and other protocols'' for § 170.315(h), we proposed to revise the heading of § 170.202 from ''transport standards'' to ''transport standards and other protocols.''

- *Direct Project*

2015 Edition Health IT Certification Criterion
§ 170.315(h)(1) (Direct Project)

We propose to adopt a certification criterion that includes the capability to send and receive according to the Applicability Statement for Secure Health Transport (the primary Direct Project specification) adopted at § 170.202(a). We previously adopted this capability for the 2014 Edition at § 170.314(b)(1), (b)(2) and (h)(1). We remind health IT developers that best practices exist for the sharing of electronic health information and enabling the broadest participation in electronic health information exchange with Direct.[183]

We propose to include as an optional capability for certification, the capability to send and receive according to the Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012, which we propose to

[182] See the 2014 Edition Release 2 final rule for more discussion on such situations (79 FR 54436–38).

[183] *http://wiki.directproject.org/Best+Practices+for+Content+and+Workflow.*

adopt at § 170.202(e). While this is not a capability we have previously adopted, we proposed to adopt it as part of the Voluntary Edition proposed rule (79 FR 10914). The primary Direct Project specification requires that Security/Trust Agents (STAs) must issue a Message Disposition Notification (MDN, RFC3798) with a disposition of processed upon successful receipt, decryption, and trust validation of a Direct message. By sending this MDN, the receiving STA is taking custodianship of the message and is indicating that it will deliver the message to its destination. While the primary Direct Project specification indicates that additional MDNs may be sent to indicate further processing progress of the message, they are not required. The primary Direct Project specification, however, does *not* provide guidance in regards to the actions that should be taken by the sending STA in the event an MDN processed message is not received or if the receiving STA cannot deliver the message to its destination after sending the initial MDN processed message. Due to the lack of specifications and guidance in the primary Direct Project specification regarding deviations from normal message flow, STAs implementing only requirements denoted as ''must'' in Section 3 of the primary Direct Project specification may not be able to provide a high level of assurance that a message has arrived at its destination. The Delivery Notification IG provides implementation guidance enabling STAs to provide a high level of assurance that a message has arrived at its destination and outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system.

Based on CMS guidance, the use of the Delivery Notification IG can be used to provide the necessary level of assurance that sent laboratory results are received by a provider.[184] Additionally, we note that the Delivery Notification IG could be generally useful for any transmission that requires a high level of assurance.

- *Direct Project, Edge Protocol, and XDR/XDM*

2015 Edition Health IT Certification Criterion

§ 170.315(h)(2) (Direct Project, Edge Protocol, and XDR/XDM)

We propose to include three distinct capabilities in this criterion. The first capability is the capability to send and receive according to the Applicability Statement for Secure Health Transport (the primary Direct Project specification) adopted at § 170.202(a). The second capability is to send and receive according to both Edge Protocol methods specified by the standard adopted at § 170.202(d). The third capability is to send and receive according to the XDR and XDM for Direct Messaging Specification adopted at § 170.202(b). These three capabilities were previously adopted as part the 2014 Edition, including through the 2014 Edition and 2014 Edition Release 2 final rules. We remind health IT developers that best practices exist for the sharing of information and enabling the broadest participation in information exchange with Direct.[185]

- *SOAP Transport and Security Specification and XDR/XDM for Direct Messaging*

2015 Edition Health IT Certification Criterion

§ 170.315(h)(3) (SOAP Transport and Security Specification and XDR/XDM for Direct Messaging)

We propose to adopt a 2015 Edition certification criterion for electronic transmission that would include the capability to send and receive according to the Transport and Security Specification (also referred to as the SOAP-Based Secure Transport RTM adopted at § 170.202(c)) and its companion specification XDR and XDM for Direct Messaging Specification adopted at § 170.202(b) We previously adopted this capability for the 2014 Edition at § 170.314(b)(1), (b)(2) and (h)(3).

- *Healthcare Provider Directory—Query Request*

2015 Edition Health IT Certification Criterion

§ 170.315(h)(4) (Healthcare Provider Directory—query request)

In June 2011, the HITPC recommended [186] that we consider the adoption of provider directory capabilities for the ONC Health IT Certification Program as well as work to address many of the issues they raised. To address the HITPC's recommendations, ONC launched a number of initiatives to define a single provider directory standard and to pilot its use.

ONC worked with implementers and subject matter experts in the field to hone in on the specific types of capabilities that should be included in a provider directory criterion. Stakeholders voiced a desire for technology to have the ability to be able to query individual directory sources and directory sources federated by third parties such as HIOs, RHIOs, HISPs etc. This is also known as ''federated querying.'' However, there were only a few implementations of federated querying across the country and many were unique due to the lack of a single standard. Given this challenge, and its potential to inhibit exchange, ONC launched an open source project called ''Modular Specification Provider Directories (MSPD).'' [187]

During the MSPD project, stakeholders collaborated to identify requirements for an updated version of the ''Healthcare Provider Directory (HPD)'' profile in order to provide a unified vendor-neutral platform for implementation of provider directories that supports both federated and non-federated architectures. The project resulted in implementable, testable specifications, and high quality test cases that verify conformance to the ''test implementation'' and it is now part of an approved IHE HPD profile Change Proposal [188]. In addition, ONC awarded a grant to the EHR |√ HIE Interoperability Workgroup [189] to pilot provider directory standards with multiple states.

The original HPD profile created by Integrating the Healthcare Enterprise (IHE) [190] addresses transactions between the client and a single provider directory with a single data source. While the standard can be used for federation, it does not address the complexities introduced by federation; provide a well-defined and straightforward approach to error handling; support targeted queries to federated data sources; or define mechanisms by which to distinguish the source of results in a given response. IHE (in collaboration with ONC, eHealth Exchange and the EHR | HIE Interoperability Work Group) has

[184] See CMS CLIA guidance on the use of Direct with the Delivery Notification IG: *http://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Policy-and-Memos-to-States-and-Regions-Items/Survey-and-Cert-Letter-14-05.html?DLPage=1&DLFilter=2014&DLSort=3&DLSortDir=ascending.*

[185] *http://wiki.directproject.org/Best+Practices+for+Content+and+Workflow.*

[186] *http://www.healthit.gov/sites/default/files/pdf/HITPC_transmit_InfoExchWG_May2011-finalsigned.pdf.*

[187] *http://modularspecs.siframework.org/Provider+Directories+Homepage.*

[188] *ftp://ftp.ihe.net/IT_Infrastructure/TF_Maintenance-2015/CPs/3_FinalText/from_Ballot_24/CP-ITI-792-05.doc.*

[189] *http://www.interopwg.org/.*

[190] *http://wiki.ihe.net/index.php?title=Healthcare_Provider_Directory.*

worked to update the IHE HPD profile to address federation. In September of 2013 ONC submitted a change proposal to IHE to incorporate the MSPD IG into the HPD profile. Through the IHE balloting process modifications were made to the change proposal to be backwards compatible with the existing IHE HPD Profile. These changes were implemented by multiple organizations to prove the feasibility and ease of implementation of the change proposal. This revised change proposal was approved by IHE in September 2014.[191] In August 2013, the HITPC recommended including a provider directory standard in the EHR Incentive Programs Stage 3.[192] The Voluntary Edition proposed rule included a request for public comment on a potential future ''provider directory'' certification criterion that would, ''at a minimum,'' require health IT to be able to query provider directories for the following information and electronically process the response returned in accordance with the IHE HPD profile requirements

- Query for an individual provider;
- Query for an organizational provider; and
- Query for relationships between individual providers and organizational providers.

We received twenty-three comments related to the provide directory question. Twenty of those comments were supportive of the inclusion of a provider directory standard in the 2015 Edition. In July 2014, the HITSC released their analysis on the IHE HPD profile, stating that the IHE HPD+ profile[193] was a good start, but not yet mature enough for nationwide implementation.[194]

Based on the feedback we received from stakeholders on the Voluntary Edition proposed rule recommending the adoption of IHE HPD and the results of pilots undertaken by EHR | HIE Interoperability Workgroup and others, we believe that making the IHE HPD profile available for testing and certification would benefit its further use and implementation in the field. Therefore, we propose a new certification criterion that would require a Health IT Module to be capable of querying a directory using the IHE HPD Profile.[195] In addition, we propose including an optional capability within this certification criterion that addresses federated requirements. In this optional capability, we propose that the Health IT Module would be required to follow the approved federation option of IHE HPD[196] to accomplish querying in federated environments. The federation change proposal was approved in September, 2014 and was incorporated into the IHE HPD Profile.[197] While the IHE HPD profile provides the ability to perform queries about individual providers, organizational providers, provider credentials and other details about providers, this proposed certification criterion seeks to establish a minimum set of queries that a Health IT Module would be required to support. The capabilities that would need to be supported by a Health IT Module include: (1) Querying for an individual provider; (2) Querying for an organizational provider; (3) Querying for both individual and organizational provider in a single query; (4) Querying for relationships between individual and organizational providers; and (5) electronically processing the response according to the IHE HPD Profile.

We believe making this basic infrastructure component available for testing and certification could assist EPs, EHs, and CAHs in achieving the ToC requirements under the EHR Incentive Programs by enabling them to find electronic service information such as Direct addresses for providers who participate in other HISPs/HIEs. It would also drive a common approach to directories across trust communities, which would improve interoperability across these communities.

- *Healthcare Provider Directory—Query Response*

2015 Edition Health IT Certification Criterion
§ 170.315(h)(5) (Healthcare Provider Directory—query response)

To complement the certification criterion we propose for adoption at 170.315(h)(4) related to health IT issuing a ''query request,'' we also propose to adopt a certification criterion at 170.315(h)(5) that would focus on the ''query response'' and include the corresponding set of capabilities to respond to a provider directory query. This proposed separation would provide developers with the flexibility to test and certify for provider directory ''query'' independent of the provider directory ''response.'' A health IT system would be able to be presented for testing and certification to both proposed certification criteria if applicable or just to one or the other as appropriate based on the product's capabilities.

Health IT systems serving as ''directory sources'' that would be seeking testing and certification to (h)(5) would have to support responding to the same queries initiated by systems seeking testing and certification to (h)(4) for interoperability purposes. As part of this proposed certification criterion, we propose that directory sources must demonstrate the capability to respond to provider directory queries according to the IHE HPD profile. Additionally, as part of the certification criteria, we propose that the directory sources must respond to the following provider directory queries

- Query for an individual provider;
- Query for an organizational provider; and
- Query for relationships between individual providers and organizational providers.

In addition we propose including an optional capability within this certification criterion to address federated requirements. In this optional capability, we propose that the Health IT Module would be required to follow the approved federation option of for IHE HPD to accomplish querying in federated environments. The federation change proposal was approved in September, 2014 was incorporated into the IHE HPD Profile.

- *Electronic Submission of Medical Documentation*

2015 Edition Health IT Certification Criterion
§ 170.315(i)(1) (Electronic submission of medical documentation)

We propose to adopt a new certification criterion as part of the proposed 2015 Edition at § 170.315(i)(1) that would focus on the electronic submission of medical documentation.

According to CMS, the Medicare Fee for Service (FFS) program currently spends in excess of $360 billion annually to provide services to over 35 million beneficiaries (excludes Medicare eligible individuals enrolled in non-FFS Medicare Programs).[198] The 2013 CMS Office of Financial Management (OFM) Improper Payment

[191] *ftp://ftp.ihe.net/IT_Infrastructure/TF_Maintenance-2015/CPs/3_FinalText/from_Ballot_24/CP–ITI–792–05.doc.*

[192] *http://www.healthit.gov/FACAS/sites/faca/files/IE%20WG_Recommendation%20Transmittal_MU3v2.docx.*

[193] *http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD_Rev1.4_TI_2013-09-20.pdf.*

[194] *http://www.healthit.gov/FACAS/sites/faca/files/HITSC_NwHIN_Provider_Directory_2014-07-16.pdf.*

[195] *http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf.*

[196] *http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf.*

[197] *http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf.*

[198] *http://www.hhs.gov/budget/fy2015/fy-2015-budget-in-brief.pdf.*

Report[199] noted that 12.7% (or $45.8 B) of the payments from the Medicare trust fund were for claims for services that were either: 1) not medically necessary and appropriate based on documentation that was submitted; or 2) insufficiently documented to determine if the billed service was necessary.

To respond to Congress' mandate[200] to more effectively manage improper payments, while recognizing the importance of reducing administrative burden for providers, CMS OFM's Provider Compliance Group (PCG) established the electronic submission of Medical Documentation (esMD) program to begin to enable the electronic submission of medical documentation.[201] As part of this program, CMS worked with ONC to establish the ''esMD Initiative'' under the S&I Framework.[202] This initiative created use cases and identified appropriate standards to facilitate the electronic exchange of medical documentation among providers and Medicare FFS review contractors. Currently, esMD Phase 1 supports the submission of unstructured data in PDF format. This method of submission is broadly deployed and accounts for over 25% of all Medicare FFS post-payment medical review submissions. In addition to post-payment review, new demonstration programs are focused on prior-authorization for specific services that have high improper payment rates. Prior-authorization ensures appropriate documentation is reviewed prior to these services/items being performed or delivered in order to avoid post-payment denials that may affect the beneficiary, the provider, or both.

In addition to current methods for submitting medical documentation (*e.g.,* mail, fax, PDF), Medicare FFS seeks to also enable a standardized and interoperable electronic approach that would reduce the time, expense, and paper required in current manual processes used for prior authorization, pre-payment review, post-payment audit, and quality management. Acceptable methods must ensure that providers are able to submit any documentation they believe is required in order to show that a proposed or provided service meets applicable requirements.

The esMD Initiative electronic Determination of Coverage (eDoC) workgroup provided an open forum for providers and payers to establish a mutual understanding of the requirements necessary for submission of structured medical documentation to support prior authorization, pre-payment review and post-payment audit. Standards analysis by the workgroup revealed a significant gap in the current standards with respect to uses that went beyond the exchange of a summary care record between providers. To address this gap, participants in the eDoC workgroup created a new Clinical Documents for Payers—Set 1 (CDP1) IG to further extend and constrain the C–CDA Release 2.0 standard.

Non-repudiation of signatures for electronic submission of medical documentation was a complementary challenge faced by the esMD Initiative. While keeping in mind the cost and impact of certain requirements, the esMD Initiative focused on two approaches to digital signatures. The ''Author of Record Level 1'' use case addressed the need for digital signatures on groups of documents and on single transactions. The ''Author of Record Level 2'' use case focused on digital signatures that could be embedded in HL7 CDA documents and included support for multiple signers where each declares their role and signature purpose. In addition to the ability to support digital signatures using industry standards, the use cases also addressed a standards-based method for the delegation, by a holder of a digital certificate, of the right to sign on their behalf by another holder of a digital certificate. While digital signatures have been implemented in the healthcare industry for other purposes, this effort will extend their use to declare and secure the provenance of single documents, bundles of documents, and transactions. The use of digital signatures on C–CDA documents will guarantee the identity of the author and ensure the integrity of the data once the document has been signed.

In summary, the esMD Initiative and its participants successfully produced standards and implementation guides to help minimize improper payments; improve interoperability for electronic submission of medical documentation, including parameters for non-repudiation, and reduce administrative burden associated with prior authorization, pre-payment review, post-payment audit and quality management.

In light of this work, we propose to adopt a certification criterion at § 170.315(i)(1) to support the electronic submission of medical documentation that includes four specific capabilities, which are each discussed in more detail below. As we mentioned in the Executive Summary of this proposed rule and discuss in more detail under section IV.B of this preamble (Modifications to the ONC Health IT Certification Program), we propose to broaden the scope of the ONC Health IT Certification Program beyond just focusing on supporting the EHR Incentive Programs. As such, we seek to make clear that this certification criterion is not within those programs' scope and is meant to be available to support other CMS program policy objectives as well as health care providers' ability to communicate encounter documentation to a payer, in particular to satisfy Medicare FFS coverage determination rules.

Capability 1—We propose that a Health IT Module be able to support the creation of a document in accordance with the HL7 Implementation Guide for CDA Release 2: Additional CDA R2 Templates—Clinical Documents for Payers—Set 1, Release 1—US Realm[203] in combination with the C–CDA Release 2.0 standard (proposed for adoption at § 170.205(a)(4)). We propose to adopt the most recent version of the CDP1 IG at § 170.205(a)(5)(i).[204] The CDP1 IG is designed to be used in conjunction with C–CDA Release 2.0 templates and makes it possible for providers to exchange a more comprehensive set of clinical information. For example, payers such as Medicare FFS allow providers to submit any information they believe substantiates that a service is medically necessary and appropriate under the applicable coverage determination rules.

A Health IT Module's support for the document-level templates formatted in accordance with the CDP1 IG would ensure that the technology is able to communicate all information relative to a patient encounter or assert that information for each ''required'' section is not available/included. If the provider then applies a digital signature to the document (as discussed in more detail below), the result is a non-repudiation

[199] *http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/CERT/index.html?redirect=/cert.*

[200] *http://www.whitehouse.gov/sites/default/files/omb/financial/_improper/PL_107–300.pdf*; *http://www.gpo.gov/fdsys/pkg/PLAW–112publ248/pdf/PLAW–112publ248.pdf;* and *www.whitehouse.gov/sites/default/files/omb/financial/_improper/PL_111-204.pdf.*

[201] *http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/ESMD/index.html?redirect=/ESMD.*

[202] *http://wiki.siframework.org/esMD+-+Charter+and+Members.*

[203] *http://www.hl7.org/special/Committees/claims/index.cfm.* We also note that access to the current draft of the CDP1 IG is freely available for review during the public comment period by establishing an HL7 user account.

[204] This would be the version of the IG (DSTU) that completes the ballot cycle before issuance of a subsequent final rule.

declaration of the encounter information.

The CDP1 IG was balloted in February of 2014 and should complete balloting this spring.[205] The February 2014 balloted version includes the following new templates:

(1) Five (5) new or additionally constrained document level templates:

- Enhanced Encounter Document
- Enhanced Hospitalization Document
- Enhanced Operative Note Document
- Enhanced Procedure Document
- Interval Document

(2) Four (4) new section level templates:

- Additional Documentation Section
- Externally Defined Clinical Data Elements Section
- Placed Orders Section
- Transportation Section

(3) Three (3) additionally constrained C–CDA Release 2.0 section level templates:

- Functional Status Section
- Plan of Treatment Section
- Social History Section

(4) New or additionally constrained entry level templates that provide support for new section level templates.

The most recent changes to the CDP1 IG include:

- Expanded descriptions regarding the use of the IG;
- References to and a list of additional constraints for templates that are based on the C–CDA Release 2.0 templates;
- Updates required for conformance with the published version of the C–CDA Release 2.0 ;
- Removal of attestation language and addition of a document succession description (clarification of standard C–CDA document succession);
- Technical corrections; and
- Name changes for the IG and the individual document level templates.

The CDP1 IG enables documentation to be completely and accurately conveyed in the new document templates. To do this, the document level templates referenced by the CDP1 IG require the inclusion of the referenced section level templates, which also include additional specificity and constraints. While a Health IT Module would need to support the entry of additional information, providers would not necessarily be required to collect any additional information to satisfy the new constraints. In other words, a specific nullFlavor may be used by the Health IT Module when creating the CDP1 IG document to indicate that no information is available for the relevant section or entry level template. Likewise, the Health IT Module may enable the provider to indicate that while information is present in the medical record it is not applicable to the purpose for which the document is intended and would subsequently result in an appropriate nullFlavor in the created CDP1 document.

To meet this capability included in the proposed certification criterion, a Health IT Module must be able to create a document that also conforms to the CDP1 IG's requirements along with appropriate use of nullFlavors to indicate when information is not available in the medical record for section or entry level template required in the CDP1 IG. In addition, a conformant Health IT Module must also demonstrate the ability to generate the document level templates as defined in the C–CDA Release 2.0, including the unstructured document.

We propose to further refine this certification criterion's scope relative to the applicable document templates within the C–CDA Release 2.0 and CDP1 IG that would need to be tested and certified for specific settings for which a Health IT Module is designed. Specifically, we propose that a Health IT Module:

- Would, regardless of the setting for which its designed, need to be tested and certified to the following document templates:
  - ○ Diagnostic Imaging Report;
  - ○ Unstructured Document;
  - ○ Enhanced Operative Note Document;
  - ○ Enhanced Procedure Note Document; and
  - ○ Interval Document.
- Designed for the ambulatory setting would also need to be certified to the Enhanced Encounter Document.
- Designed for the inpatient setting would also need to be certified to Enhanced Hospitalization Document.

Capability 2—We propose that a Health IT Module be able to support the use of digital signatures embedded in C–CDA Release 2.0 and CDP1 IG documents templates by adopting the HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1 (DSDR IG) (proposed for adoption at § 170.205(a)(5)(ii)).[206] This DSDR IG defines a method to embed digital signatures in a CDA document and provides an optional method to specify delegation of right assertions that may be included with the digital signatures. We note, however, that for the purposes of certification, we propose to require that that optional method must be demonstrated to meet this certification criterion. The implementation of this IG will allow payers, such as Medicare, to accurately authenticate the authorized signers of CDA document and trust the validity and authenticity of signed medical documentation. The DSDR IG provides specific guidance on the use of digital signatures embedded in a CDA document to:

- Provide a non-repudiation signature that attests to the role and signature purpose of each authorized signer to the document.
- Provide for a delegation of rights where the signer is a delegated signer and not the authorized signer responsible individual or organization (*e.g.,* the signer is acting as an authorized agent).
- Define the method of incorporating multiple digital signatures and delegation of right assertions into the header of a CDA document.
- Define how to create the digest of the CDA document
- Define how to sign and incorporate the:
  - ○ CDA digest;
  - ○ Timestamp;
  - ○ Role of the signer;
  - ○ Purpose of signature.
- Define how to incorporate the:
  - ○ The public certificate of the signer;
  - ○ Long term validation data, including Online Certificate Status Protocol (OCSP) response and/or Certificate Revocation List (CRL).

Digital signatures ensure that the recipient of the signed document can authenticate the authorized signer's digital certificate, the signature artifact(s), determine the signer's role and signature purpose and validate the data integrity of the document. To create a valid digital signature that meets Federal Information Processing Standards (FIPS) [207], Federal Information Security Management Act of 2002 (FISMA) [208], and Federal Bridge Certification Authority (FBCA) requirements [209], the system used to digitally sign C–CDA Release 2.0 or CDP1 IG documents in accordance with

[205] *http://www.hl7.org/special/Committees/claims/index.cfm.* We also note that access to the current draft of the CDP1 IG is freely available for review during the public comment period by establishing an HL7 user account.

[206] *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=375.*

[207] *http://www.nist.gov/itl/fips.cfm.*

[208] *http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.*

[209] *http://www.idmanagement.gov/sites/default/files/documents/FBCA%20Certificate%20Policy%20v2.27.pdf.*

the DSDR IG must meet the following requirements:

(1) The cryptographic module[210] used must:

a. Be validated to meet or exceed FIPS 140–2, Level 1.

b. Implement a digital signature system and hash function must be compliant with FIPS 186–2 and FIPS 180–2.

c. Store the private key on a FIPS 140–2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm.

(2) The system must support multi-factor authentication that meets or exceeds Level 3 assurance as defined in NIST SP 800–63–2.

(3) The system must set a 10-minute inactivity time period after which the certificate holder must re-authenticate the password to access the private key.

(4) For software implementations, when the signing module is deactivated, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use of, the private key.

(5) The system must have a time system that is synced with the official National Institute of Standards and Technology time source (as described by the standard adopted at 45 CFR 170.210(g)).

For the purposes of testing and certification, we propose that the first requirement (cryptographic module requirements) be met through compliance documentation. For all other specific capabilities in the list above, we expect testing and certification to assess the capabilities expressed.

We also propose that a Health IT Module must demonstrate the ability to validate a digital signature embedded in a C–CDA Release 2.0 document that is conformant with the DSDR IG. The requirements to perform this action are included in the DSDR IG.

Capability 3—We propose that a Health IT Module be able to support the creation and transmission of ''external digital signatures'' for documents. These digital signatures may be used to sign any document for the purpose of both data integrity and non-repudiation. The esMD Initiative defines the requirements in the Author of Record Level 1: Implementation Guide.[211] We propose to adopt this IG at § 170.205(a)(5)(iii). The Author of Record Level I IG uses the IHE DSG standard to provide a signer with the ability to digitally sign multiple documents and embed the W3C compliant XADES signature in a signature document that may accompany the signed documents or as a ''wrapper'' for the documents. This signing capability is intended for use when the sender of one or more documents needs to ensure that the transmitted documents include the non-repudiation identity of the sender and ensure that the recipient can validate that the document s have not been altered from the time of signing. This is not intended to replace the ability to embed multiple digital signatures in a C–CDA Release 2.0 and CDP1 IG document. The Author of Record Level 1 IG provides specific guidance on the use of a single digital signature, external to document, to:

- Provide a non-repudiation signature that attests to the identity of the signer;
- Allows the recipient to validate the data integrity of the signed document;
- Provide for a delegation of rights where the signer is a delegated signer and not the authorized signer responsible individual or organization (*e.g.,* the signer is acting as an authorized agent); and
- Defines how to incorporate the public certificate of the signer.

Digital signatures ensure that the recipient of the signed document can authenticate the authorized signer's digital certificate, the signature artifact(s), and validate the data integrity of the document. The system requirements in place to apply digital signatures on documents are the same as in capability 2 with the addition of a requirement that specifies that a Health IT Module must be able to digitally sign single or bundles of documents in conformance with the Author of Record Level 1 IG.

Capability 4—We propose that a Health IT Module be able to support the creation and transmission of digital signatures for electronic transactions for the purpose of both data integrity and non-repudiation authenticity. The esMD Initiative defines the requirements in the Provider Profiles Authentication: Registration Implementation Guide.[212] We propose to adopt this IG at § 170.205(a)(5)(iv). The Provider Profiles Authentication: Registration IG uses the W3C XADES digital signature standard to ''sign'' the contents of an electronic transaction and include the signature as accompanying metadata in the signed transaction. This signing capability is intended for use when the sender or recipient of a transaction needs to ensure that the transmitted information include the non-repudiation identity of the sender and ensure that the recipient can validate that the authenticity and integrity of the transaction information. This is not intended to replace the digital signature requirements defined in either Capability 2 or 3 above. The Provider Profiles Authentication: Registration IG provides specific guidance on the creation and use of a single digital signature for an electronic transaction, as accompanying metadata, to:

- Provide a non-repudiation signature that attests to the identity of the signer;
- Allow the recipient to validate the data integrity of the signed transaction;
- Provide for a delegation of rights where the signer is a delegated signer and not the authorized signer responsible individual or organization (*e.g.,* the signer is acting as an authorized agent); and
- Define how to incorporate the public certificate of the signer.

Digital signatures ensure that the recipient of the signed transaction can authenticate the authorized signer's digital certificate, the signature artifact(s), and validate the data integrity of the transaction. The system requirements in place to apply digital signatures for transactions are the same as in capability 2 with the addition of a requirement that specifies that a Health IT Module must be able to digitally sign a transaction and create the appropriate metadata in conformance with the Provider Profiles Authentication: Registration IG.

4. Gap Certification Eligibility Table for 2015 Edition Health IT Certification Criteria

We define gap certification at 45 CFR 170.502 as the certification of a previously certified Complete EHR or EHR Module(s) to: (1) all applicable new and/or revised certification criteria adopted by the Secretary at subpart C of part 170 based on the test results of a NVLAP-accredited testing laboratory; and (2) all other applicable certification criteria adopted by the Secretary at subpart C of part 170 based on the test results used to previously certify the Complete EHR or EHR Module(s) (for further explanation, see 76 FR 1307–1308). Our gap certification policy

[210] A cryptographic module is defined in FIPS 140–2 as ''a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.''

[211] *http://wiki.siframework.org/file/view/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx/539084894/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx.*

[212] *http://wiki.siframework.org/file/view/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx/539084920/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx.*

focuses on the differences between certification criteria that are adopted through rulemaking at different points in time. This allows health IT to be certified to only the differences between certification criteria editions rather than requiring health IT to be fully retested and recertified to certification criteria (or capabilities) that remain unchanged from one edition to the next and for which previously acquired test results are sufficient. Under our gap certification policy, ''unchanged'' criteria are eligible for gap certification, and each ONC–ACB has discretion over whether it will provide the option of gap certification.

For the purposes of gap certification, Table 4 below provides a crosswalk of proposed ''unchanged'' 2015 Edition certification criteria to the corresponding 2014 Edition certification criteria. We note that with respect to the 2015 Edition certification criteria proposed for adoption at § 170.315(g)(1) through (g)(3) that gap certification eligibility for these criteria is fact-specific and will depend on any modifications made to the specific certification criteria to which these ''paragraph (g)'' certification criteria apply.

TABLE 4—GAP CERTIFICATION ELIGIBILITY FOR 2015 EDITION EHR CERTIFICATION CRITERIA

2015 edition		2014 edition	
Regulation section § 170.315	Title of regulation paragraph	Regulation section § 170.314	Title of regulation paragraph
(a)(1)	Computerized provider order entry—medications.	(a)(1) (a)(18)	Computerized provider order entry. Computerized provider order entry—medications.
(a)(3)	Computerized provider order entry—diagnostic imaging.	(a)(1) (a)(20)	Computerized provider order entry. Computerized provider order entry—diagnostic imaging.
(a)(8)	Medication list	(a)(6)	Medication list.
(a)(9)	Medication allergy list	(a)(7)	Medication allergy list.
(a)(13)	Image results	(a)(12)	Image results.
(a)(16)	Patient list creation	(a)(14)	Patient list creation.
(a)(18)	Electronic medication administration record	(a)(16)	Electronic medication administration record.
(d)(1)	Authentication, access control, and authorization.	(d)(1)	Authentication, access control, and authorization.
(d)(2)	Auditable events and tamper-resistance	(d)(2)	Auditable events and tamper-resistance.
(d)(3)	Audit report(s)	(d)(3)	Audit report(s).
(d)(4)	Amendments	(d)(4)	Amendments.
(d)(5)	Automatic access time-out	(d)(5)	Automatic log-off.
(d)(6)	Emergency access	(d)(6)	Emergency access.
(d)(7)	End-user device encryption	(d)(7)	End-user device encryption.
(d)(8)	Integrity	(d)(8)	Integrity.
(d)(9)	Accounting of disclosures	(d)(9)	Accounting of disclosures.
(e)(2)	Secure messaging	(e)(3)	Secure messaging.
(h)(1)	Direct Project	(b)(1)(i)(A) and (b)(2)(ii)(A).	Transitions of care—receive, display, and incorporate transition of care/referral summaries. Transitions of care—create and transmit transition of care/referral summaries.
		(h)(1)	Transmit—Applicability Statement for Secure Health Transport.
(h)(2)	Direct Project, Edge Protocol, and XDR/XDM	(b)(1)(i)(B), (b)(2)(ii)(B), and (b)(8)[213].	Transitions of care—receive, display, and incorporate transition of care/referral summaries. Transitions of care—create and transmit transition of care/referral summaries. Transitions of care—send and receive via edge protocol.
		(h)(2) and (b)(8)	Transmit—Applicability Statement for Secure Health Transport and XDR/XDM for Direct Messaging. Transitions of care—send and receive via edge protocol.
(h)(3)	SOAP Transport and Security Specification and XDR/XDM for Direct Messaging.	(b)(1)(i)(C) and (b)(2)(ii)(C).	Transitions of care—receive, display, and incorporate transition of care/referral summaries. Transitions of care—create and transmit transition of care/referral summaries.
		(h)(3)	Transmit—SOAP Transport and Security Specification and XDR/XDM for Direct Messaging.

5. Pharmacogenomics Data—Request for Comment

Pharmacogenomics data identifies genetic variants in individuals that alter their metabolism or other interactions with medications and can lead to serious adverse events. This information is being included in an increasing number of FDA-approved drug labels. Health IT systems that can capture pharmacogenomics information could be used to increase patient safety and enhance patient outcomes.

To our knowledge, in general, health IT has not yet captured genomic and genetic patient information—the presence of clinically significant genomic variants—in a structured manner such as exists for other categorical clinical findings or laboratory-derived data.[214] This information may currently be captured in free text and static PDFs except in a few individual health centers where custom health IT solutions have been developed. However, work on standards and other precursors required for wider adoption is underway, including through the Institute of Medicine, HL7, and LOINC®.[215] Many of these efforts are using pharmacogenomic variations as prototypes because the clinical utility of a subset of such variants has a greater evidence-base, has wide clinical applicability, and is already in clinical use. Pharmacogenomic implementation aims to limit preventable adverse effects and maximize efficacy by using information about genomic variants to enable optimal drug choices and patient-specific dosing.

For the use case of CDS informed by pharmacogenetic information, considerable ambiguity exists with respect to the incorporation of CDS systems that facilitate providers taking advantage of pharmacogenomic information.[216] Thus, there is an opportunity for further specification of standards and implementation of pharmacogenomic data for CDS within health IT systems. We also believe there may be opportunities for capturing genomic patient data in laboratory results, for drug-genome interactions, and for genomic metabolizer status (defined risks to certain medications) in a structured way within health IT.

Note that we have previously adopted a 2014 Edition ‘‘family health history’’ certification criterion that referenced the HL7 standard for representing genomic information and are proposing a 2015 Edition ‘‘family health history—pedigree’’ certification criterion that references that same standard as well as a related IG. In addition to their relevance for the tested patient, genomic test results are unique in that they have the potential to inform the health care of blood relatives of the tested individual, similar to a shared family history. We note that any application of genomic information across family members must be done in accordance with the HIPAA Privacy Rule and other privacy and patient rights laws regarding genetic information at the federal and state levels.

We acknowledge that individually identifiable genetic information may be subject to federal and state privacy laws and regulations that are more privacy restrictive than the HIPAA Privacy Rule. As such, these privacy issues will impact any certification criteria or policy we might propose to adopt in future rulemaking. We therefore welcome input on factors to consider for health IT that allows the user to use or disclose genetic information in a manner compliant with federal and state privacy laws. Note that we are proposing two new 2015 Edition certification criteria for ‘‘data segmentation for privacy—send’’ and ‘‘data segmentation for privacy—receive’’ that would focus on the capability to separately track (‘‘segment’’) individually identifiable health information that is protected by rules that are more restrictive than the HIPAA Privacy Rule (please refer to Section III.A.3 for more information). We believe that the capabilities offered by the proposed ‘‘data segmentation for privacy’’ criteria could be leveraged for the segmentation of individually identifiable genetic information that are protected by federal and state privacy laws and regulations.

We also acknowledge that the inclusion of genomic information in health IT-related mechanisms will need to be carefully implemented to balance the benefit to patients while avoiding discrimination against persons with or at risk for the development of future health issues, and their family members.

In collaboration with the National Institutes of Health, we solicit comment on whether:

- The 2015 Edition ‘‘medication allergy list’’ certification criterion should include the capability to integrate genotype-based drug metabolizer rate information.
- The 2015 Edition ‘‘drug-drug, drug-allergy interactions checks for CPOE’’ certification criterion or as a separate certification criterion should include pharmacogenomic CDS for ‘‘drug-genome interactions.’’
- We should offer 2015 Edition certification for CDS that incorporate a patient's pharmacogenomic genotype data into the CPOE prescribing process with the goal of avoiding adverse prescribing outcomes for known drug-genotype interactions.
- There are certification approaches that could enhance the end-user's (provider's) adoption and continued use of health IT implementations that guide prescribing through CDS using pharmacogenomic data.
- There are existing or developing standards applicable to the capture, storage, display, and exchange of potentially clinically relevant genomic data, including the pharmacogenomic subset.
- We should offer certification for health IT functionality that could facilitate HIPAA-compliant sharing of discrete elements of a patient's genomic information from their record to the family history section of a relative's record.
- The proposed ‘‘data segmentation for privacy’’ criteria would provide needed health IT functions with respect to the storage, use, transmission, and disclosure of genetic, genomic, and pharmacogenomics information that is subject to protections under HIPAA and

[213] Technology must have been certified to both edge protocol methods specified by the standard in § 170.202(d) to be gap certification eligible.

[214] *http://www.genomebc.ca/education/articles/genomics-vs-genetics/;* and *http://www.who.int/genomics/geneticsVSgenomics/en/.*

[215] Clinical Pharmacogenetics Implementation Consortium, *http://www.pharmgkb.org/page/cpic/*; electronic medical records and genomics Network (eMERGE), *http://emerge.mc.vanderbilt.edu/emerge-network* and *http://emerge.mc.vanderbilt.edu/emerge-publications-0*; Clinical Sequencing Exploratory Research (CSER) *https://cser-consortium.org;* Implementing Genomics in Practice (IGNITE), *http://www.ignite-genomics.org/IGNITE_ABOUT.html;* Institute of Medicine (IOM) Action Collaborative, *http://www.iom.edu/Activities/Research/GenomicBasedResearch.aspx;* NHGRI GM7, Genomic Medicine Centers Meeting VII action items relating to pharmacogenomics implementation, *http://www.genome.gov/Multimedia/Slides/GM7/09_Williams-Middleton.pdf;* Clinical Genome Resource, *http://www.clinicalgenome.org/about/;* Clinical Variation Aggregation Database, *https://www.ncbi.nlm.nih.gov/clinvar/; and* HL7 Clinical Genomics Working Group, *http://www.hl7.org/Special/committees/clingenomics/index.cfm.*

[216] Overby CL, Kohane I, Kannry J, et al, *Opportunities for Genomic Clinical Decision Support Interventions,* Genet Med. 2013 October 2015(10):817–23; Rasmussen-Torvik LJ, Stallings SC, Gordon AS, et al, *Design and Anticipated Outcomes of the eMERGE–PGx Project: A Multi-Center Pilot for Pre-Emptive Pharmacogenomics in Electronic Health Record Systems,* Clin Pharmacol Ther. 2014 Jun 24. doi: 10.1038/clpt.2014.137, [Epub ahead of print]; Karnes JH, Van Driest S, Bowton EA, et al, *Using systems approaches to address challenges for clinical implementation of pharmacogenomics,* Wiley Interdiscip Rev Syst Biol Med. 2014 Mar-Apr;6(2):125–35, doi:10.1002/wsbm.1255. Epub 2013 Dec 6; and Peterson JF, Bowton E, Field JR, et al, *Electronic health record design and implementation for pharmacogenomics: a local perspective,* Genet Med. 2013 Oct;15(10):833–41. doi: 10.1038/gim.2013.109. Epub 2013 Sep 5.

additional state and federal privacy and protection laws such as the Genetic Information Nondiscrimination Act (GINA).[217]

- The proposed ''data segmentation for privacy'' criteria adequately balance complex genetic privacy issues, such as those related to behavioral health, with the clinical value of context-appropriate availability of a patient's actionable genetic and genomic information.
- Health IT should be required to apply different rules for the use and exchange of genetic, genome, and pharmacogenomics data based on different groupings of diseases or conditions based on the sensitivity of the information, such as those related to behavioral health.
- There are other factors we should consider for health IT that allows the user to use or disclose genetic information in a manner compliant with federal and state privacy laws.

B. Definitions

1. Base EHR Definitions

We propose to adopt a Base EHR definition specific to the 2015 Edition (*i.e.,* a 2015 Edition Base EHR definition) at § 170.102 and rename the current Base EHR definition at § 170.102 as the 2014 Edition Base EHR definition. To effectively rename the current Base EHR definition as the ''2014 Edition Base EHR'' definition, the Base EHR definition must be removed from the CFR and a ''2014 Edition Base EHR'' definition must be added. This is a procedural requirement and we affirm that the definition itself is not changing. However, for the proposed 2015 Edition Base EHR definition, it would differ from the 2014 Edition Base EHR definition in the following ways:

- It does not include privacy and security capabilities and certification criteria. We believe privacy and security capabilities would be more appropriately addressed through our new proposed approach for the privacy and security certification of Health IT Modules to the 2015 Edition, as discussed under ''Privacy and Security'' in section IV.C.1 of this preamble. Our new privacy and security approach would eliminate EPs', eligible hospitals', and CAHs' responsibilities to ensure that they have technology certified to all the necessary privacy and security criteria. Rather, as part of certification, health IT developers would need to meet applicable privacy and security certification criteria.
- It only includes capabilities to record and export CQM data (§ 170.315(c)(1)). To note, the capabilities to import, calculate and report CQM data are not included in the proposed 2015 Edition Base EHR definition or any other CQM-related requirements. Please refer to the ''Clinical Quality Measures'' section (III.A.3) earlier in this preamble for a more detailed discussion of the CQM certification criteria. Please also see the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register** for proposals related to CQMs, including the CEHRT definition proposal.
- It includes the 2015 Edition ''smoking status'' certification criterion as patient demographic and clinical health information data consistent with statutory requirements.[218] Smoking and the use of tobacco in general is the number one cause of preventable death and disease in the United States. By including this capability and criterion in the definition, it ensures that providers participating in the EHR Incentive Programs have the basic capability to capture the smoking status of patients, which permits more providers to take part in addressing (through intervention and cessation efforts) this cause of preventable disease and death.
- It includes the 2015 Edition ''implantable device list'' certification as patient demographic and clinical health information data consistent with statutory requirements.[219] The ability to record and access a patient's unique device identifiers can improve patient safety. Please see the discussion under the ''implantable device list'' certification criterion for further benefits derived from providers having access unique device identifier(s) for a patient's implantable device(s).
- It includes the 2015 Edition ''application access to Common Clinical Data Set'' certification criterion as a capability to both capture and query information relevant to health care quality and exchange electronic health information with, and integrate such information from other sources.[220] Due to the proposed inclusion of the 2015 Base EHR definition in the proposed CEHRT definition (see ''CEHRT definition'' section below and in the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register**), like all capabilities and criteria included in the 2015 Edition Base EHR definition, this would ensure that all EPs, eligible hospitals, and CAHs would need to adopt a Health IT Module certified to this criterion in order to have the necessary health IT to meet the CEHRT definition. As such, the inclusion of the 2015 Edition ''application access to Common Clinical Data Set'' certification criterion in the 2015 Edition Base EHR definition could further facilitate health information exchange by being specifically used to meet meaningful use objectives and measures as well as through it simply being readily available for use by these providers and their patients.
- It includes the proposed 2015 Edition Health IT certification criteria that correspond to the remaining 2014 Edition certification criteria referenced in the ''2014 Edition'' Base EHR definition (*i.e.,* CPOE, demographics, problem list, medication list, medication allergy list, CDS, transitions of care, data portability, and relevant transport certification criteria). On the inclusion of transport certification criteria, we propose to include the ''Direct Project'' criterion (§ 170.315(h)(1)) as well as the ''Direct Project, Edge Protocol and XDR/XDM'' criterion (§ 170.315(h)(2)) as equivalent alternative means for meeting the 2015 Edition Base EHR definition for the reasons discussed earlier in this preamble under the ''Transport Methods and Other Protocols'' section.

[217] *http://ghr.nlm.nih.gov/spotlight=thegeneticinformationnondiscriminationactgina.*

[218] A Base EHR is the regulatory term we have given to what the HITECH Act defines as a ''qualified EHR.'' Our Base EHR definition(s) include all capabilities found in the ''qualified EHR.'' Please see the 2014 Edition final rule (77 FR 54262) for further explanation.

[219] A capability included in the Base EHR definition, which originates from the ''qualified EHR'' definition found in the HITECH Act.

[220] These are capabilities included in the Base EHR definition, which originate from the ''qualified EHR'' definition found in the HITECH Act.

TABLE 5—CERTIFICATION CRITERIA REQUIRED TO SATISFY THE 2015 EDITION BASE EHR DEFINITION

Base EHR capabilities	Certification criteria
Includes patient demographic and clinical health information, such as medical history and problem lists.	Demographics § 170.315(a)(5) Problem List § 170.315(a)(7) Medication List § 170.315(a)(8) Medication Allergy List § 170.315(a)(9) Smoking Status § 170.315(a)(12) Implantable Device List § 170.315(a)(20)
Capacity to provide clinical decision support	Clinical Decision Support § 170.315(a)(10)
Capacity to support physician order entry	Computerized Provider Order Entry § 170.315(a)(1), (2) or (3)
Capacity to capture and query information relevant to health care quality.	Clinical Quality Measures § 170.315(c)(1)
Capacity to exchange electronic health information with, and integrate such information from other sources.	Transitions of Care § 170.315(b)(1) Data Portability § 170.315(b)(6) Application Access to Common Clinical Data Set § 170.315(g)(7) Direct Project § 170.315(h)(1) or Direct Project, Edge Protocol, and XDR/XDM § 170.315(h)(2)

Marketing

We note that we would continue the same marketing policy that we adopted for the 2014 Edition as it relates to the 2015 Edition Base EHR definition (*i.e.,* health IT developers would have the ability to market their technology as meeting the 2015 Edition Base EHR definition when their Health IT Module(s) is/are certified to all the 2015 Edition health IT certification criteria included in the 2015 Edition Base EHR definition).

2. Certified EHR Technology Definition

We propose to remove the Certified EHR Technology (CEHRT) definition from § 170.102, effective with a subsequent final rule for the following reasons. The CEHRT definition has always been defined in a manner that supports the EHR Incentive Programs. As such, the CEHRT definition would more appropriately reside solely within the EHR Incentive Programs regulations. This would also be consistent with our approach in this proposed rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. Further, this approach should add administrative simplicity in that regulatory provisions, which EHR Incentive Programs participants must meet (*e.g.,* the CEHRT definition), would be defined within the context of rulemakings for those programs.

The EHR Incentive Programs currently include a regulatory definition of CEHRT in 42 CFR 495.4 that simply adopts the CEHRT definition in § 170.102. As proposed in the EHR Incentive Programs Stage 3 proposed rule, published elsewhere in this issue of the **Federal Register**, CMS would adopt a CEHRT definition in 42 CFR 495.4 that would cover all relevant compliance timelines (*i.e.,* specify the CEHRT definition applicable for each year/EHR reporting period) and EHR Incentive Programs requirements. The CEHRT definition proposed by CMS would also continue to point to the relevant Base EHR definitions[221] adopted or proposed by ONC and to other ONC-adopted and proposed certification criteria relevant to the EHR Incentive Programs. We refer readers to EHR Incentive Programs Stage 3 proposed rule for further details regarding the CEHRT definition proposal.

3. Common Clinical Data Set Definition

We propose to revise the ''Common MU Data Set'' definition in § 170.102. We propose to change the name to ''Common Clinical Data Set,'' which aligns with our approach throughout this proposed rule to make the ONC Health IT Certification Program more open and accessible to other types of health IT beyond EHR technology and for health IT that supports care and practice settings beyond those included in the EHR Incentive Programs. To effectively rename the Common MU Data Set as the ''Common Clinical Data Set,'' the Common MU Data Set definition must be removed from the CFR and the ''Common Clinical Data Set'' definition must be added. This is a procedural requirement and all substantive changes to the definition would only affect certification to the 2015 Edition. We also propose to change references to the ''Common MU Data Set'' in the 2014 Edition (§ 170.314) to ''Common Clinical Data Set.''

We propose to revise the definition to account for the new and updated standards and code sets we propose to adopt in this proposed rule that would improve and advance interoperability through the exchange of the Common Clinical Data Set. We also propose to revise the definition to support patient safety through clearly referenced data elements and the inclusion of new patient data. These proposed revisions would *not* change the standards, codes sets, and data requirements specified in the Common Clinical Data Set for 2014 Edition certification. They would only apply to a Health IT Module certified to the 2015 Edition Health IT certification criteria that reference the Common Clinical Data Set.

Vocabulary Standards

We propose to include HL7 Version 3 (''AdministrativeGender'' and a nullFlavor value) for sex, ''Race & Ethnicity—CDC'' code system in PHIN VADS and the OMB standard for race and ethnicity, RFC 5646 for preferred language, the September 2014 Release of the U.S. Edition of SNOMED CT® for problems and procedures, the February 2, 2015 monthly version of RxNorm for medications and medication allergies, LOINC® version 2.50 for laboratory tests, and the LOINC® codes, metadata, and relevant UCUM unit of measures specified for vital signs as discussed under the ''vital signs, BMI and growth charts'' certification criterion in section III.A.3 of this preamble. We note that for race and ethnicity a Health IT Module must be able to express both detailed races and ethnicities according to the ''Race & Ethnicity—CDC'' code system and the aggregate OMB code for each race and ethnicity identified by the patient.

We propose to include immunizations in the ''Common Clinical Data Set'' for 2015 Edition certification. As described

[221] This is required by the HITECH Act under the term ''Qualified EHR'' and references a foundational set of certified capabilities all EPs, eligible hospitals, and CAHs need to adopt.

in more detail in the preamble for the ''transmission to immunization registries'' certification criterion in section III.A.3, the C–CDA Release 2.0 can support NDC codes as a translational data element, but the CVX code is required to accompany it. The NDC code contains more information than the CVX code, such as packaging information, that can assist with tracking for clinical trials and adverse events. We believe that it would not be a heavy burden to map from an NDC code to a CVX code because a mapping from NDC codes to CVX codes is publicly available.[222] Therefore, for the purposes of including immunizations in the ''Common Clinical Data Set'' for 2015 Edition certification, immunizations would be required to be coded according to the CVX code set (HL7 Standard Code Set CVX—Vaccines Administered, updates through February 2, 2015) and the NDC code set (NDC—Vaccine Codes, updates through January 15, 2015) as part of the ''Common Clinical Data Set.''

Unique Device Identifier(s)

We also propose to include the Unique Device Identifier(s) of a patient's Implantable Device(s) for certification to the 2015 Edition. As discussed under the ''implantable device list'' certification criterion, this information leads to improved patient safety when available to providers. By including this information in the Common Clinical Data Set, a Health IT Module certified to criteria referencing the Common Clinical Data Set would be capable of exchanging this information and further facilitating improvements in patient safety.

Assessment and Plan of Treatment, Goals, and Health Concerns

We propose to include the ''assessment and plan of treatment,'' ''goals,'' and ''health concerns'' in the ''Common Clinical Data Set'' for certification to the 2015 Edition. The ''assessment and plan of treatment,'' ''goals,'' and ''health concerns'' are intended to replace the concept of the ''care plan field(s), including goals and instructions'' which is part of the ''Common MU Data Set'' in the 2014 Edition. Based on conversations with stakeholders, we are aware that the ''care plan field(s), including goals and instructions'' may be interpreted in two different ways. It might be interpreted to mean the assessment, plan of care (for treatment), goals, and health concerns documented for a single patient encounter (in ambulatory settings) or for the duration of an inpatient stay (in inpatient settings). However, ''care plan field(s), including goals and instructions'' could also be interpreted to mean a comprehensive shared care plan that represents the synthesis and reconciliation of multiple plans of care (for treatment) produced by each provider to address specific health concerns. Stakeholders have indicated that in implementation, they have interpreted ''care plan field(s), including goals and instructions'' in the ''Common MU Data Set'' as the assessment, plan of care (for treatment), goals, and health concerns *for a single patient encounter or inpatient stay.* These stakeholders have expressed safety concerns that the volume of data in a comprehensive care plan can be so extensive that it may be difficult for a provider to quickly determine the information of value for the patient for the given situation.

In consideration of this feedback, we clarify that we intend ''care plan field(s), including goals and instructions'' to be a single provider's documentation of their assessment, plan of treatment, goals, and health concerns for the patient (this clarification applies for 2014 Edition certification). We also make this clarification to better align with the terms used in the C–CDA Release 2.0, which includes the ''Assessment and Plan Section (V2),'' ''Assessment Section (V2),'' ''Plan of Treatment Section (V2),'' ''Goals Section,'' and ''Health Concerns Section.'' In previous iterations of the C–CDA, the ''Plan of Treatment Section'' was called the ''Plan of Care Section,'' which resulted in the same level of confusion on whether the information was intended to represent a single encounter or the synthesis of multiple encounters. For that reason, the ''Plan of Care Section'' is now called the ''Plan of Treatment Section'' to indicate that it is intended to represent a single encounter and not to be confused with the ''Care Plan document template.''

For certification to the 2015 Edition, we propose to include in the Common Clinical Data Set ''assessment and plan of treatment,'' ''goals,'' and ''health concerns'' data in accordance with the C–CDA Release 2.0 ''Assessment and Plan Section (V2)'' or both the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2);'' the ''Goals Section;'' and the ''Health Concerns Section.'' In practice, health care providers may document the assessment and plan of treatment together or separately, and the C–CDA Release 2.0 provides for both modes of practice. We understand that the C–CDA Release 2.0 permits both free-text and structured documentation of the assessment, plan of treatment, goals, and health concerns information in the sections named above. While we do not propose to require that this information is documented in a structured way, we encourage health IT developers to allow for structured documentation or tagging that would allow a provider to choose relevant pieces of assessment, plan of treatment, goals, and health concerns data that could be synthesized into a comprehensive care plan. We note that all proposed 2015 Edition certification criteria that reference the ''Common Clinical Data Set'' (*e.g.,* the ToC criterion) would therefore also require a Health IT Module to be able to capture ''assessment and plan of treatment,'' ''goals,'' and ''health concerns'' data.

We continue to believe in the value of a comprehensive care plan and discuss our proposal for a 2015 Edition certification criterion for this functionality in Section III.A.3 of the preamble (see the ''care plan'' certification criterion). As stated above, a comprehensive care plan may contain a large volume of data that is burdensome to transmit for the purposes of sharing information relevant for a single encounter or inpatient stay, and thus we do not propose to include it in the ''Common Clinical Data Set'' definition.

Alignment With Clinical Practice

We recognize that the data included in the Common Clinical Data Set may change over time. Therefore, we request comment on ways in which we can engage the public to keep the Common Clinical Data Set relevant to clinical practice.

4. Cross Referenced FDA Definitions

As discussed in our proposal for the 2015 Edition ''implantable device list'' certification criterion, we propose to adopt in § 170.102 new definitions for ''Implantable Device,'' ''Unique Device Identifier,'' ''Device Identifier,'' and ''Production Identifier.'' We propose to adopt the same definitions already provided to these phrases at 21 CFR 801.3. Again, we believe adopting these definitions in our rule will prevent any interpretation ambiguity and ensure that each phrase's specific meaning reflects the same meaning given to them in the Unique Device Identification System final rule at 21 CFR 801.3. Capitalization was purposefully applied to each word in these defined phrases in order to signal to readers that they have specific meanings.

[222] *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=ndc.* See also: *http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.*

IV. Provisions of the Proposed Rule Affecting the ONC Health IT Certification Program

A. Subpart E—ONC Health IT Certification Program

We propose to replace the term ''HIT'' with the term ''health IT'' wherever it may occur in subpart E. While ''HIT'' is a term used in the HITECH Act, we believe the term ''health IT'' offers more clarity than ''HIT'' for stakeholders. Similarly, we propose to replace the ''ONC HIT Certification Program'' with ''ONC Health IT Certification Program'' wherever it may occur in subpart E. In referring to the certification program, the term ''health'' is capitalized. We also propose to remove § 170.553 ''Certification of health information technology other than Complete EHRs and EHR Modules'' as we believe this section is no longer relevant based on our proposals for the ONC Health IT Certification Program discussed in more detail below.

B. Modifications to the ONC Health IT Certification Program

In the Voluntary Edition proposed rule (79 FR 10929–30) we recited our authority and the history of the ONC Health IT Certification Program, including multiple requests for comment and significant feedback on making the program more accessible to health IT beyond EHR technology and health care settings and practices not directly tied to the EHR Incentive Programs. With consideration of stakeholder feedback and our policy goals, we attempted to make the ONC Health IT Certification Program more open and accessible through a proposal in the Voluntary Edition proposed rule (79 FR 10918–20) to create MU and non-MU EHR Modules. We subsequently determined that our proposal was not the best approach (79 FR 54472–73). Since that rulemaking, the HITPC has issued recommendations supporting certification for care/practice settings beyond the ambulatory and inpatient settings.[223] We have also reconsidered how best to structure the program and make it open and accessible to more types of health IT, health IT that supports a variety of care and practice settings, and programs that may reference the ONC Health IT Certification Program, including Medicaid and Medicare payment programs and various grant programs.

1. Health IT Modules

We propose to rename EHR Modules as Health IT Modules. To effectively rename EHR Modules as Health IT Modules, the EHR Module definition must be removed from the CFR at § 170.102 and a ''Health IT Module'' definition must be added. This proposed change would be effective on the effective date of a subsequent final rule, which would make this change applicable for certification to the 2014 Edition and 2015 Edition (if adopted). An EHR Module is defined in § 170.102 as any service, component, or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary. The definition essentially covers any type of technology that could be certified to one or more certification criterion under the ONC Health IT Certification Program. As such, our proposed change will have no substantive impact on the technologies that might be, or have been, certified under the ONC Health IT Certification Program. We believe this proposal best addresses the full range of health IT that has and might be certified to adopted certification criteria now and in the future. This approach also gives more appropriate attribution to certifications issued to technologies that would not generally be considered ''EHR'' functionality, such as functionality provided by a HISP, HIE, or LIS. The switch to ''Health IT Module'' could also have long-term practicality as the ONC Health IT Certification Program evolves.

For technologies already certified to the 2014 Edition as EHR Modules, this proposal would not affect the certification of those technologies or the ability to use those technologies to meet the CEHRT definition. Further, we see no reason why these technologies could not be called Health IT Modules if the developer wished to do so. We suggest, however, that health IT developers check with the ONC–ACB that issued the certification to ensure this would be permissible based on the issued certification.

We also emphasize that a Health IT Module is simply the name for a technology that gets issued a certification under the ONC Health IT Certification Program. One Health IT Module certification or multiple Health IT Modules certifications can be of sufficient scope to meet the Base EHR definition and even the CEHRT definition.

2. ''Removal'' of Meaningful Use Measurement Certification Requirements

We propose to *not* require ONC–ACBs to certify Health IT Modules to the 2015 Edition ''meaningful use measurement'' certification criteria (§ 170.315(g)(1) ''automated numerator recording'' and § 170.315(g)(2) ''automated measure calculation''). This is a change from prior certification policy, such as with the certification of technology to the 2014 Edition and the requirements of § 170.550(f)(1). We believe this will make the ONC Health IT Certification more accessible to the certification of health IT for other purposes beyond the EHR Incentive Programs. Further, we have received feedback from stakeholders that these requirements can pose a significant burden on health IT development and come at the cost of improving clinical functionality and usability (79 FR 54469). We have also heard from stakeholders that these criteria can impact innovation. Whether this feedback is entirely accurate is not the primary reason for our changed approach. Rather, we believe that not all health IT certified under the ONC Health IT Certification Program needs to have these capabilities and that it is more appropriate to align our approach to these criteria with our primary policy of administering a certification program that includes certification criteria that broadly support the health care system, while making available for health IT developers the flexibility to present their health IT for certification to the criteria that support their specific customers' and providers' needs.

We emphasize that this proposed approach *does not preclude* health IT developers from seeking certification to § 170.315(g)(1) or (2) in support of their customers' and provider's needs related to the EHR Incentive Programs. Moreover, the EHR Incentive Programs Stage 3 proposed rule, published elsewhere in this issue of the **Federal Register**, includes a proposed CEHRT definition that would require EPs, eligible hospitals, and CAHs to have health IT certified to these criteria in order to meet the CEHRT. Accordingly, health IT developers supporting providers participating the EHR Incentive Programs should strongly consider seeking certification to these certification criteria, as applicable.

3. Types of Care and Practice Settings

As noted above, the HITPC issued recommendations generally supporting certification for a variety of care and practice settings under the ONC Health IT Certification Program, particularly

[223] *http://www.healthit.gov/facas/sites/faca/files/TransmittalLetter_LTPAC_BH_Certification.pdf* and *http://www.healthit.gov/facas/sites/faca/files/HITPC_LTPAC_BH_Certification_Recommendations_FINAL.pdf.*

focusing on long-term post-acute care (LTPAC) and behavioral health settings. Consistent with those recommendations, we have made proposals to make the ONC Health IT Certification Program more agnostic to care and practice settings (*e.g.,* the proposals to revise § 170.300 and ''remove'' ''meaningful use measurement'' certification requirements) and we have proposed new ''data segmentation'' certification criteria (§§ 170.315(b)(7) and (8)) that include capabilities that can support care and practice settings that service patients with sensitive health information, including behavioral health.

In the Voluntary Edition final rule (79 FR 54473), we pointed stakeholders to the guidance we issued in 2013 for health IT developers serving providers ineligible for the EHR Incentives Programs. The guidance, ''Certification Guidance for EHR Technology Developers Serving Health Care Providers Ineligible for Medicare and Medicaid EHR Incentive Payments,'' [224] was developed in close coordination with HHS agencies, including the Substance Abuse and Mental Health Services Administration (SAMHSA). The guidance is designed for certification to the 2014 Edition and focuses on two key area, interoperability-focused certification criteria (highlighting the ''transitions of care'' and ''clinical information reconciliation'' criteria as criteria that support interoperable summary care record exchange—a fundamental capability necessary to enable care coordination across different settings) and privacy and security certification criteria. The HITPC similarly concluded that LTPAC and behavioral health providers should focus on adopting health IT certified to these capabilities (certification criteria).[225]

The 2015 Edition includes many certification criteria with the same capabilities as those certification criteria identified in the 2014 guidance, but with new and/or enhanced functionality. As one pertinent example, the 2015 Edition ''transitions of care'' certification criterion (§ 170.315(b)(1)) includes capabilities for formatting a care/referral summary according to the Common Clinical Data Set and the C–CDA Release 2.0. The C–CDA Release 2.0 includes new document templates for: Care Plan; Referral Note; Transfer Summary, and new sections for: Goals; Health Concerns; Health Status Evaluation/Outcomes; Mental Status; Nutrition; Physical Findings of Skin and new entries (*e.g.* Wound Observation) that may be particularly beneficial to providers that serves medically-complex patients with chronic care conditions. As to privacy and security, we highlight that our new proposed approach in this rule focuses on ensuring that all health IT presented for certification is certified to the appropriate privacy and security certification criteria. Overall, we have proposed a diverse edition of health IT certification criteria with capabilities included that could support a wide range of providers practicing in various settings.

We anticipate that, similar to the 2014 Edition guidance, we would issue general interoperability guidance for the 2015 Edition when it becomes final. However, we have no plans to *independently* develop and issue certification ''paths'' or ''tracks'' by care or practice setting (*e.g.,* a ''LTPAC certification'') as it would be difficult to independently devise such ''paths'' or ''tracks'' in a manner that was sure to align with other relevant programs and specific stakeholder needs. Rather, we believe we are best suited for supporting the development of standards for specific settings/use cases and providing technical assistance to both health IT developers and providers about the certification criteria, the standards and capabilities they include, and the processes of the ONC Health IT Certification Program. In this regard, we would welcome working with HHS or other agencies, or provider associations, in identifying the appropriate functionality and certification criteria to support their stakeholders, including jointly developing specialized certification ''paths'' or ''tracks.'' To note, we believe this approach is also consistent with stakeholder feedback we received through rulemaking (79 FR 54473–74) and the HITPC recommendations for us to work with HHS and other agencies.

We seek comment on potential future certification criteria that could include capabilities that would uniquely support LTPAC, behavioral health, or pediatrics care\practice settings, as well as other settings. We are specifically interested in public comment on whether certification criteria focused on patient assessments (*e.g.,* Minimum Data Set (Nursing Homes), OASIS (Home Health), IRF–PAI (Inpatient Rehabilitation Facility), or Long Term Care Hospital (CARE data set) would support key functionality needed in these settings and if there standards mature enough for structured patient assessments. Similarly, we seek comment on whether certification criteria focused on patient assessments for behavioral health settings would be of value to health IT developers and health care providers.

4. Referencing the ONC Health IT Certification Program

Our proposals throughout this proposed rule, including the proposed adoption of various criteria that support functionality for different care and practice settings and the proposals to make the ONC Health IT Certification Program open and accessible to more types of health IT and health IT that supports a variety of care and practice settings, would permit further referencing and use of certified health IT.

Currently, in addition to the EHR Incentive Programs, the adopted certification criteria editions already support and are referenced by other HHS programs (*e.g.,* the CMS and HHS Office of Inspector General (OIG) final rules to modify the Physician Self-Referral Law exception and Anti-kickback Statute safe harbor for certain EHR donations (78 FR 78751) and (78 FR 79202), respectively).[226] Certified health IT has also been referenced in CMS payment rules such as the CY 2015 Physician Fee Schedule final rule (79 FR 67721–28) for chronic care management services and in a proposed rule (79 FR 61186) encouraging the use of certified health IT by home health agencies. The Department of Defense has also referenced certified health IT in a request for proposal for its Healthcare Management System Modernization Program.[227] In the private sector, The Joint Commission requires the use of certified health IT to participate as an Outcomes Research Yields Excellence (ORYX) vendor and submit electronic clinical quality measures on behalf of hospitals.[228]

The proposed 2015 Edition and proposed open and flexible certification processes in this proposed rule would continue to facilitate the efforts

[224] *http://www.healthit.gov/sites/default/files/generalcertexchangeguidance_final_9-9-13.pdf.*

[225] *http://www.healthit.gov/facas/sites/faca/files/TransmittalLetter_LTPAC_BH_Certification.pdf* and *http://www.healthit.gov/facas/sites/faca/files/HITPC_LTPAC_BH_Certification_Recommendations_FINAL.pdf.*

[226] CMS final rule, ''Medicare Program; Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships: Exception for Certain Electronic Health Records Arrangements'' (78 FR 78751) (December 27, 2013). OIG final rule, ''Medicare and State Health Care Programs: Fraud and Abuse; Electronic Health Records Safe Harbor Under the Anti-Kickback Statute'' (78 FR 79202) (December 27, 2013).

[227] *https://www.fbo.gov/index?s=opportunity&mode=form&id=573cfbaa71e7843341a7c145888c48e0&tab=core&_cview=1.*

[228] *http://www.jointcommission.org/assets/1/18/2015_eCQM_Vendor_List.pdf.* (page 3).

described above as well as other ongoing and future efforts to reference and use certified health IT.

C. Health IT Module Certification Requirements

1. Privacy and Security

We propose a new approach for privacy and security (P&S) certification to the 2015 Edition. In our past rulemakings, we have discussed and instituted two different policy approaches and sought comment on others for ensuring that health IT and providers have privacy and security capabilities while also trying to minimize the level of regulatory burden imposed on health IT developers. In the 2011 Edition, we included an upfront requirement that required Health IT Modules to meet all P&S certification criteria as a condition of certification unless the health IT developer could demonstrate that certain P&S capabilities were either technically infeasible or inapplicable. In the 2014 Edition, we eliminated the upfront requirement for each Health IT Module to be certified against the P&S criteria in favor of what we thought would better balance the burden potentially posed by our rulemaking. Thus, the P&S criteria were made part of the ''2014 Edition Base EHR definition'' that all EPs, EHs, and CAHs must meet in order to satisfy the CEHRT definition (meaning each provider needed, post-certification to ultimately have technology certified to the P&S criteria).

On March 23, 2013, the HITSC recommended that we should change our certification policy for P&S. They recommended that each Health IT Module presented for certification should be certified through one or more of the following three paths:

- Demonstrate, through system documentation and certification testing, that the Health IT Module includes functionality that meets at least the ''minimal set'' [229] of privacy and security certification criterion.
- Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces that enable it to access external services necessary to conform to the ''minimal set'' of privacy and security certification criterion.
- Demonstrate through documentation that the privacy and security certification criterion (and the minimal set that the HITSC defined) is inapplicable or would be technically infeasible for the Health IT Module to meet. In support of this path, the HITSC recommended that ONC develop guidance on the documentation required to justify inapplicability or infeasibility.

In response to the HITSC recommendations and stakeholder feedback we sought comment in the Voluntary Edition proposed rule (79 FR 10925–26) on the following four options we believed could be applied to Health IT Module certification for privacy and security: (1) Re-adopt the 2011 Edition approach; (2) maintain the 2014 Edition approach; (3) adopt the 2013 HITSC recommendation; or (4) adopt a limited applicability approach—under which ONC would establish a limited set of P&S functionality that every Health IT Module would be required to address in order to be certified.

In response to our request for comments, we received comments generally in support of the 2014 approach (including P&S in the Base EHR definition). While some commenters supported requiring a subset of P&S criteria (option 4), many disagreed on the scope and did not see the value vis-a-vis HIPAA compliance. The HITSC preferred a different option. They recommended that ONC revise each privacy and security criterion to specify the conditions under which it is applicable (similar to how the end-user device encryption criterion currently is written), and allow each criterion to be met using one of the three paths the HITSC recommended in 2013.[230]

During their discussions regarding the Voluntary Edition proposed rule, the HITSC's Privacy and Security Workgroup (PSWG) completed an assessment of which P&S functionality should be required for each proposed certification criterion. The PSWG recognized that the privacy and security criteria are not equally applicable or useful to every criterion in each of the other regulatory functional areas (*i.e.,* clinical, care coordination, clinical quality, patient engagement, public health, utilization, and transmission) because each P&S criterion is designed to address specific risk conditions that may or may not be present within a specific regulatory functional area.

The PSWG model allows for the appropriate safeguards to be in place for each criterion, without overburdening health IT developers by requiring them to include all P&S functionality for each criterion. We believe this serves as a good model, in combination with the 2013 HITSC recommendations, to propose a new, simpler, straight-forward approach to the P&S certification requirements for Health IT Modules that merges many of the recommendations and feedback we have received to date. Under the proposed approach, a health IT developer would know exactly what it needed to do in order to get its Health IT Module certified and a purchaser of a Health IT Module would know exactly what privacy and security functionality against which the Health IT Module had to be tested in order to be certified.

We propose to require that an ONC–ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text ''first level paragraph'' category (*e.g.,* § 170.315(a)) of § 170.315 identified below is certified to either approach 1 (technically demonstrate) or approach 2 (system documentation) as follows:

[229] The minimal set includes the following certification criteria: ''authentication, access control, and authorization,'' ''auditable events and tamper resistance,'' ''audit report(s),'' ''amendments,'' ''automatic log-off,'' ''emergency access,'' ''end-user device encryption,'' and ''integrity.'' The full recommendation can be found at: *http://www.healthit.gov/sites/default/files/pswgtransmittalmemo_032613.pdf.*

[230] *http://www.healthit.gov/sites/default/files/pswgtransmittalmemo_032613.pdf.*

If the Health IT Module includes capabilities for certification listed under:	It will need to be certified to approach 1 or approach 2 for each of the P&S certification criteria listed in the "approach 1" column	
	Approach 1	Approach 2
§ 170.315(a)	§ 170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6)(emergency access), and (d)(7) (end-user device encryption).	For each applicable P&S certification criterion not certified for approach 1, there must be system documentation sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.
§ 170.315(b)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) (integrity).	
§ 170.315(c)	§ 170.315(d)(1) through (d)(3).	
§ 170.315(e)	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(7).	
§ 170.315(f)	§ 170.315(d)(1) through (d)(3) and (d)(7).	
§ 170.315(h)	§ 170.315(d)(1) through (d)(3).	
§ 170.315(i)	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	

To illustrate approach 1 of privacy and security certification, if a Health IT Module is presented for certification to § 170.315(a)(5) (''demographics''), then the Health IT Module must also be certified to § 170.315(d)(1) through (7). We refer readers to Appendix A of this proposed rule for a listing of the P&S certification requirements for each 2015 Edition criterion under approach 1.

Because we have explicitly proposed which P&S certification criteria would be applicable to the associated criteria adopted in each regulatory text ''first level paragraph'' category and have also proposed approach 2, we have not proposed to permit the 2011 Edition policy of allowing for a criterion to be met through documentation that the criterion is inapplicable or would be technically infeasible for the Health IT Module to meet.

We seek comment on the overall clarity and feasibility of this approach.

2. Design and Performance (§ 170.315(g))

We propose to revise § 170.550 to add paragraph (g), which would require ONC–ACBs to certify Health IT Modules to certain proposed certification criteria under § 170.315(g). We propose to require ONC–ACBs to certify Health IT Modules to § 170.315(g)(3) (safety-enhanced design) and § 170.315(g)(6) (Consolidated CDA creation performance) consistent with the requirements included in these criteria. Paragraph (g) also includes a requirement for ONC–ACBs to certify all Health IT Modules presented for certification to the 2015 Edition to § 170.315(g)(4) (quality system management) and (g)(8) (accessibility-centered design). The proposed certification requirements for § 170.315(g)(3) and (4) maintain the policy approach established with certification to the 2014 Edition (see § 170.550(f)(2) and (3)), which ensures Health IT Modules, as applicable, are certified to these specific safety and quality certification criteria. The proposed certification requirements for § 170.315(g)(6) is associated with the new ''Consolidated CDA creation performance'' criterion we have proposed for the 2015 Edition and discuss in more detail in section III.A.3 of this preamble. Again, the requirement is similarly designed to ensure that Health IT Modules (with Consolidated CDA creation capabilities within their scope) are also certified to the ''Consolidated CDA creation performance'' criterion. The proposed certification requirements for § 170.315(g)(8) is associated with the new ''accessibility-centered design'' criterion we have proposed for the 2015 Edition and discuss in more detail in section III.A.3 of this preamble. This criterion and approach to certification is patterned after the 2014 Edition ''quality system management'' criterion.

D. Principles of Proper Conduct for ONC–ACBs

1. ''In-the-Field'' Surveillance and Maintenance of Certification

We propose to adopt new requirements for ''in-the-field'' surveillance under the ONC Health IT Certification Program. Our proposal would build on ONC–ACBs' existing surveillance responsibilities by requiring ONC–ACBs to initiate in-the-field surveillance of certified Complete EHRs and certified Health IT Modules in certain circumstances and in accordance with certain standards and procedures described below. Our proposal would also clarify ONC–ACBs' responsibilities for requiring certified Health IT Module and certified Complete EHR developers to take corrective action in instances where the technology fails to conform to the requirements of its certification. We believe these proposed requirements would promote greater consistency, transparency, and rigor in the surveillance of certified capabilities in the field. They would also provide ONC–ACBs, health IT developers, and users of certified health IT subject to surveillance with greater clarity and predictability regarding this important aspect of the ONC Health IT Certification Program.

Our proposal focuses on ONC–ACBs' responsibilities for conducting surveillance ''in the field.'' In-the-field surveillance is already a requirement of the ONC Health IT Certification Program [231] and is among the most

[231] We explicitly recognized an ''in-the-field surveillance'' requirement in the Proposed Establishment of Certification Programs for Health Information Technology; Proposed Rule, 75 FR 11328 (Mar 10, 2010), wherein we proposed that an ONC–ACB would be required to ''evaluate and reevaluate previously certified Complete EHRs and/or EHR Modules to determine whether [they] continued to perform in an acceptable, if not the same, manner *in the field* as they had performed when they were certified.'' 75 FR 11349 (emphasis added). We finalized this requirement in the Establishment of the Permanent Certification for Health Information Technology; Final Rule, 76 FR 1262 (Jan. 7, 2011) (hereinafter ''PCP Final Rule''). Subsequently, we issued initial and annual guidance to ONC–ACBs clarifying our interpretation of the requirements for in-the-field surveillance under the ONC HIT Certification Program, the preparation and submission of ONC–ACBs' annual surveillance plans, and the reporting of surveillance results to the National Coordinator on an annual basis. *See* ONC HIT Certification Program Guidance #13–01 (July 2013), available at *http://www.healthit.gov/sites/default/files/onc-acb_2013annualsurveillanceguidance_final_0.pdf; see also* ONC HIT Certification Program Guidance #14–

important responsibilities with which an ONC–ACB is charged. It is rooted in the need to provide assurance to purchasers, implementers, and users that certified Complete EHRs and certified Health IT Modules not only meet the requirements of certification in a controlled testing environment but will continue to do so when implemented and used in a production environment. This basic assurance protects the integrity of the ONC Health IT Certification Program and federal health IT investments by enabling individuals to rely upon certifications issued on behalf of ONC to select appropriate technologies and capabilities; identify potential implementation or performance issues; and implement certified health IT in a predictable, reliable, and successful manner.[232] The need to evaluate certified health IT in the field is particularly important for capabilities related to interoperability, patient safety, and privacy and security, which present special implementation challenges, complexities, or risks.[233]

Recognizing that in-the-field surveillance presents technical, operational, and other challenges, we have previously avoided prescribing specific requirements in this area; instead we have provided guidance to ONC–ACBs and encouraged them to develop and refine their own approaches to surveillance. We continue to regard such flexibility as important for minimizing the burden of surveillance on all stakeholders and ensuring that ONC–ACBs' approaches to surveillance reflect their unique expertise and judgment. However, we also believe that establishing certain minimum expectations and procedures for in-the-field surveillance could provide ONC–ACBs as well as health IT developers and users with greater clarity and predictability regarding this important aspect of the ONC Health IT Certification Program. Accordingly, we propose the following additional requirements for in-the-field surveillance under the ONC Health IT Certification Program.

"In-The-Field Surveillance" Defined

Our proposal explicitly defines in-the-field surveillance to mean an ONC–ACB's assessment of whether a certified Complete EHR or certified Health IT Module to which it has issued a certification continues to conform to the certification's requirements once implemented and in use in the field. This assessment would, by definition, require the ONC–ACB to assess the certified Complete EHR or certified Health IT Module's capabilities in a production environment. The assessment of a capability would be based on the use of the capability with protected health information (PHI) unless the use of test data would provide an equivalent assessment of the capability and were specifically approved by the National Coordinator.[234]

The following hypothetical scenarios illustrate our proposed approach.

- *Scenario 1:* An ONC–ACB initiates in-the-field surveillance for a certified Health IT Module for the medication list certification criterion (proposed at 45 CFR 170.315(a)(8)). An ONC–ACB would then assess this capability at several locations at which the certified Health IT Module has been implemented. The ONC–ACB would assess whether the implemented capability can electronically record, change, and access one or more patients' active medication lists and medication histories as required by the certification criterion.
- *Scenario 2:* An ONC–ACB initiates in-the-field surveillance for a certified Health IT Module's transitions of care capability and one or more applicable transport certification criteria (proposed at 45 CFR 170.315(b)(1) and (h), respectively). During this surveillance, the ONC–ACB would assess these capabilities at several locations at which the certified Health IT Module is implemented to determine whether these certified capabilities perform in compliance with the applicable certification criteria.
- *Scenario 3:* An ONC–ACB initiates in-the-field surveillance for a certified Health IT Module related to the data portability criterion adopted at 45 CFR 170.314(b)(7). Again, the ONC–ACB would need to assess at several locations at which the Health IT Module is implemented whether the certified Health IT Module's data portability capability performed in compliance with the certification criterion.

As these scenarios illustrate, an ONC–ACB's evaluation of health IT in the field must focus on compliance with one or more certification criteria to which a Complete EHR or Health IT Module is certified. Such compliance must be assessed in the production environment in which the Complete EHR or Health IT Module is actually *implemented and used.*

Because certified Complete EHRs and certified Health IT Modules will be integrated with other systems, processes, and people, we acknowledge that the unique circumstances and contexts in which a certified Complete EHR or certified Health IT Module operates could impact an ONC–ACB's ability to assess whether it continues to perform in compliance with adopted certification criteria once it has been implemented and in use. For example, if during in-the-field surveillance an ONC–ACB observed that the certified capability did not perform in a compliant manner, the ONC–ACB would need to determine whether the failure was the result of a problem with the certified capability or, alternatively, whether the failure was caused entirely by other factors beyond the scope of certification, such as a configuration or implementation issue (for which the user was primarily responsible) or the failure of a third-party technology or service over which the health IT developer had limited or no control.

Further, we recognize that the assessment of a certified Complete EHR or certified Health IT Module in a production environment would require ONC–ACBs to employ different methodologies than testing and certification in a controlled environment. Given the additional factors and complexities described above, there could be situations in which an in-person site visit is the best or perhaps the only reliable means of evaluating whether health IT, as implemented in the field, conforms to the requirements of its certification. However, in general, we expect that ONC–ACBs should be able to effectively assess certified capabilities "in the

01 (July 2014), available at *http://www.healthit.gov/sites/default/files/onc-acb_cy15annualsurveillanceguidance.pdf.*

[232] *See, e.g., FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework* (April 2014) (draft for public comment) (hereinafter "FDASIA Report"), available at *http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf,* at § 5.3.2 ("For the consumer, ONC certification provides purchasing clarity and assurance that the certified EHR product meets certain criteria and/or functions in a certain way.")

[233] *See, e.g., FDASIA Report, supra,* at section 5.2.1 ("Errors in communication due to inadequate interoperability, such as the transmission of test results inaccurately or for the wrong patient, do occur and can lead to patient harm."); ONC HIT Certification Program Guidance #13–01, supra, at 3–4 (prioritizing surveillance for safety-related capabilities); *Health IT Safety Plan, supra,* at 14 (discussing incorporation of health IT safety in post-market surveillance of certified EHR technology).

[234] In consultation with the Office for Civil Rights, we have clarified that under the "health oversight agency" exception of the HIPAA Privacy Rule, a healthcare provider would be permitted to disclose protected health information (PHI) to an ONC–ACB during the course of authorized in-the-field surveillance activities, without patient authorization and without a business associate agreement. *See* ONC Regulation FAQ #45 [12–13–045–1], available at *http://www.healthit.gov/policy-researchers-implementers/45-question-12-13-045.*

field'' using other remote methods that would not involve in-person site visits. We believe that such methods may be less intrusive for health care providers, less costly or burdensome for ONC–ACBs, or offer other benefits. Therefore, we request comment on these and other approaches to in-the-field surveillance, on ways to minimize the burden and costs of in-the-field surveillance for ONC–ACBs and health care providers, and on appropriate industry standards or best practices that we should consider adopting to provide ONC–ACBs with consistent, objective, and reliable methods for conducting these evaluations.

Duty To Initiate In-The-Field Surveillance

In addition to defining in-the-field surveillance, this proposal would require ONC–ACBs to initiate in-the-field surveillance in at least two sets of circumstances. These two separate requirements—which we refer to as ''reactive'' and ''randomized'' in-the-field surveillance—are discussed in detail below. Together they would implement sections 7.9.2 and 7.9.3 of ISO/IEC 17065 (the standard to which ONC–ACBs are accredited under the ONC HIT Certification Program), which provide that surveillance ''shall include periodic surveillance . . . to ensure ongoing validity of the demonstration of fulfilment of [] requirements.''[235] As such, the requirements would become part of the ''certification scheme'' for purposes of ISO/IEC 17065 and would therefore be directly enforceable by the ONC–AA, which is responsible for accrediting ONC–ACBs and verifying their conformance to ISO/IEC 17065 and other program requirements.

Reactive Surveillance

To satisfy the proposed ''reactive'' surveillance requirement, an ONC–ACB would be required to initiate in-the-field surveillance whenever it becomes aware of facts or circumstances that call into question a certified Complete EHR or certified Health IT Module's continued conformance to the requirements of its certification. This reactive surveillance requirement aligns with ONC–ACBs' existing annual surveillance plans, which should specify how an ONC–ACB will ''[s]ystematically obtain and synthesize feedback from users of [health IT] that the ONC–ACB has certified to determine if certain capabilities should be evaluated with the [health IT] developer or with the user in the field, or both.''[236] We anticipate that such feedback would include (although not be limited to) complaints received from existing and prospective users and implementers of the Complete EHRs and Health IT Modules the ONC–ACB has certified.

We clarify that the receipt of a single complaint would not automatically trigger an ONC–ACB's duty to initiate in-the-field surveillance. In general, an ONC–ACB would be required to consider and weigh the volume, substance, and credibility of complaints received against the type and extent of the alleged non-conformance, in light of the ONC–ACB's expertise and experience with the particular capabilities, health IT, and certification criteria at issue.

We also propose as part of ''reactive'' surveillance that an ONC–ACB must consider the impact and effect of the disclosures made by a Complete EHR or Health IT Module developer on the product's continued conformance to adopted certification criteria. We have proposed this additional review because we believe there are additional factors and circumstances that an ONC–ACB will be unable to assess at the time the health IT was initially certified based on tests completed by the developer in a controlled environment. For example, the ONC–ACB may determine that while a health IT developer's Complete EHR or Health IT Module demonstrated it could perform a required capability in a controlled environment, users in the field cannot reasonably access or use the capability because the health IT developer does not make the capability available; substantially restricts or limits its use; or has not disclosed known material information about the implementation or use of the capability. These and other practices, such as those discussed in our proposal ''Transparency and Disclosure Requirements'' below, could substantially interfere with the performance of certified capabilities in the field and creates a substantial risk that existing or prospective users will encounter problems implementing the capability in a manner consistent with a Complete EHR or Health IT Module's certification. As a result, we have proposed that as part of ''reactive'' surveillance ONC–ACBs evaluate the disclosures in connection with, and in the context of, the certified capability/capabilities under surveillance to gain a full understanding of the way in which the product performs in the field.

We clarify our expectation that ONC–ACBs could render a certified Complete EHR or certified Health IT Module non-conformant to the certification criteria in instances where the developer does not make the capability available; substantially restricts or limits its use; or has not disclosed known material information about the implementation or use of the capability. We also note that we expect ONC–ACBs to give considerable weight to complaints or other indications that a developer has failed meet the disclosure requirements of § 170.523(k)(1).

Consistent with current practice, we expect that the National Coordinator will continue to prioritize certain certification criteria for purposes of surveillance. For example, certification criteria may be prioritized based on the special implementation challenges or risks associated with certain capabilities, especially those related to interoperability, patient safety, and privacy and security. ONC–ACBs would be required to give special scrutiny to complaints about capabilities or disclosures related to these prioritized certification criteria. If an ONC–ACB detected a pattern or trend of such complaints, it would be required to initiate in-the-field surveillance to investigate the complaints and the extent of any non-conformance with the requirements of a certified Complete EHR or certified Health IT Module's certification.

Finally, for the reasons discussed earlier in this proposal and immediately below in our proposal ''Transparency and Disclosure Requirements,'' during reactive surveillance of a certified Complete EHR or Health IT Module in the field, an ONC–ACB would need to verify that the health IT developer has satisfied the mandatory disclosure requirements currently and proposed a § 170.523(k)(1), as applicable, for the certification criteria that are the subject of the ONC–ACB's surveillance.

Randomized Surveillance

Separate from the reactive surveillance described above, we also propose to require ONC–ACBs to conduct ''randomized'' surveillance of the Complete EHRs and Health IT Modules they have certified. We believe randomized surveillance will serve two important purposes: First, it will enable ONC–ACBs to identify nonconformities that are difficult to detect through complaint-based or other reactive forms of surveillance. Second, it will enable ONC–ACBs to detect patterns of non-conformance that indicate a more widespread or recurring problem requiring a more comprehensive

[235] ISO/IEC 17065:2012, available at *http://www.iso.org/iso/catalogue_detail.htm?csnumber=46568.*

[236] ONC HIT Certification Program Guidance #13–01, supra, at 3.

corrective action plan, as discussed below. For these reasons, we believe that randomized surveillance will complement reactive surveillance and strengthen the overall surveillance of certified health IT under the ONC Health IT Certification Program.

Under our proposal, an ONC–ACB would be required to conduct randomized surveillance of prioritized certification criteria (as described in the context of reactive surveillance earlier in this proposal). Focusing on these prioritized certification criteria would maximize the impact and minimize any associated costs or burdens of randomized surveillance. For the same reason, ONC–ACBs would be required to not select certified Complete EHRs and certified Health IT Modules that were selected for randomized surveillance at any time within the preceding twelve months. [237]

To satisfy the proposed randomized surveillance requirement, an ONC–ACB would be required during each calendar year to randomly select at least 10% of the Complete EHRs and Health IT Modules to which it has issued a certification. For each certified Complete EHR or certified Health IT Module selected, the ONC–ACB would initiate in-the-field surveillance at the lesser of 10 or 5% of locations at which the Complete EHR or Health IT Module is implemented and in use in the field.

- *Example:* A Health IT Module is in use at 1,000 locations. Five percent of 1,000 locations equals 50 locations, which is greater than 10 locations. Therefore, the ONC–ACB must evaluate the Health IT Module at a minimum of 10 locations.
- *Example:* A Health IT Module is in use at 100 locations. Five percent of 100 locations equals 5 locations, which is less than 10 locations. Therefore the ONC–ACB must evaluate the Health IT Module at a minimum of 5 locations.

The locations would need to be selected at random by the ONC–ACB from a list of all locations at which the certified Complete EHR or certified Health IT Module is implemented. Where practicable, the sample would need to reflect a diversity of practice types, sizes, settings, and locales.

Similar to reactive surveillance, if in the course of randomized surveillance an ONC–ACB finds that a certified Complete EHR or certified Health IT Module is non-conformant at one or more locations at which surveillance takes place, the ONC–ACB must take appropriate action with the health IT developer, consistent with the ONC–ACB's accreditation, to remedy the nonconformity.

In addition to addressing individual, potentially one-off, nonconformities, an ONC–ACB would also be required to evaluate the overall results of any certified Complete EHR or certified Health IT Module that is subjected to randomized surveillance. If the ONC–ACB finds a pattern of nonconformity—defined as a failure to demonstrate conformance to any prioritized certification criterion at 20% or more of the locations surveilled—the ONC–ACB would regard these results as deficient and would need to require the health IT developer to submit a corrective action plan to address the apparent widespread or recurring issue. Upon making such determination, an ONC–ACB would be required to contact the health IT developer and require that it submit a proposed corrective action plan to the ONC–ACB. The corrective action plan would be required to include, at a minimum, for each certification criterion or required disclosure for which the health IT was deemed deficient:

- A description of the identified deficiencies;
- an assessment of how widespread or isolated the identified deficiencies may be;
- how the developer will address the identified conformance deficiencies in general and at the locations under which surveillance occurred; and
- the timeframe under which corrective action will be completed.

The ONC–ACB would require the health IT developer to submit a proposed corrective action plan to the ONC–ACB within 30 days of the date that the developer was notified by the ONC–ACB of the deficiency or deficiencies above. In general, ONC–ACBs would be responsible for prescribing the required form and content of corrective action plans, consistent with the general elements required above, and for developing specific procedures for the submission and approval of corrective action plans. ONC may also issue guidance to ensure consistency across ONC–ACBs corrective action procedures.

Consistent with an ONC–ACB's accreditation and procedures for suspending a certification, an ONC–ACB would be permitted to initiate certification suspension procedures for a Complete EHR or Health IT Module if the heath IT developer thereof:

- Does not submit a proposed corrective action plan to the ONC–ACB within 30 days of being notified of its deficient surveillance results;
- does not comply with the ONC–ACB's directions for addressing any aspects of the proposed corrective action plan that do not meet the requirements of the ONC–ACB or the ONC Health IT Certification Program; or
- does not complete an approved corrective action plan within 6 months of approval of the plan by the ONC–ACB.

Following the suspension of a certified Complete EHR or certified Health IT Module's certification for the reasons above, an ONC–ACB would be permitted to initiate certification termination procedures for the Complete EHR or Health IT Module (consistent with its accreditation to ISO/IEC 17065 and procedures for terminating a certification) should the developer not complete the actions necessary to reinstate the suspended certification.

Reporting of Surveillance Results

Under our proposal, ONC–ACBs would be required to report the results of in-the-field surveillance to the National Coordinator on at least a quarterly basis. This requirement would reduce the time between when surveillance is initiated and when results are submitted to ONC. Currently under the ONC Health IT Certification Program, ONC–ACBs are not required to submit surveillance results for as long as 14 months after initiating in-the-field surveillance—a significant limitation in our ability to be responsive, including providing relevant information to stakeholders.

Upon requiring a corrective action plan for a certified Complete EHR or certified Health IT Module, an ONC–ACB would be required to report the corrective action plan and related data to the publicly accessible open data CHPL, as detailed below in our proposal ''Open Data Certified Health IT Product List (CHPL).'' The purpose of this reporting requirement, as described in that proposal, would be to ensure that health IT users, implementers, and purchasers are alerted to potential conformance issues in a timely and effective manner, consistent with the patient safety, program integrity, and transparency objectives described subsequently in this proposed rule.

To implement the new requirements for in-the-field surveillance outlined in this proposal, we propose to add § 170.556 (In-the-field surveillance and

[237] This screening requirement would apply only for the purpose of randomized surveillance. The ONC–ACB would still be expected to initiate reactive and other surveillance, including in-the-field surveillance, as necessary to ensure that the Complete EHRs and Health IT Modules it has certified continue to perform in an acceptable manner and meet all certification program requirements.

maintenance of certification for health IT). We would also amend § 170.503 (ONC–AA Ongoing Responsibilities) and § 170.523 (ONC–ACB Principles of Proper Conduct) consistent with the requirements described in this proposal and the related proposals ''Transparency and Disclosure Requirements'' and ''Open Data Certified Health IT Product List (CHPL)'' below. The requirements would provide a floor only, and would in no way limit an ONC–ACB's ability or responsibility to conduct additional surveillance, including in-the-field surveillance, according to the requirements of its accreditation and the ONC Health IT Certification Program. As we have done in the past, we would continue to give ONC–ACBs substantial flexibility and discretion to decide how to implement these requirements as part of their overall approach to surveillance. ONC–ACBs would continue to describe their surveillance programs in their annual surveillance plans, which must be submitted to the National Coordinator prior to the covered calendar year surveillance period. We would also continue to provide annual surveillance guidance to ONC–ACBs, and other guidance or programmatic direction as needed.

At the time of this proposed rule, ONC–ACBs have submitted their annual surveillance plans for calendar year 2015, which include their existing approaches and methodologies for randomized surveillance. To minimize disruption to ONC–ACBs' current surveillance activities, we propose to phase in the requirements proposed at § 170.556(c) for randomized surveillance. As such, the randomized surveillance requirements would become effective beginning January 1, 2016, enabling ONC–ACBs to implement these new requirements in their next annual surveillance plans and incorporate additional guidance and clarification from ONC and the ONC–AA. All other new requirements for in-the-field surveillance—*i.e.,* the requirements proposed at § 170.556(a), (b), and (d)—would be effective immediately; we would expect ONC–ACBs to implement these requirements within 3 months of the effective date of a subsequent final rule. We request comment on whether this timeline and plan for implementation is appropriate and on ways to minimize disruption and ensure that the requirements and purpose of this proposal are timely and effectively achieved.

2. Transparency and Disclosure Requirements

We propose to revise the principles of proper conduct for ONC–ACBs in order to provide for greater and more effective disclosure by health IT developers of certain types of limitations and additional types of costs that could interfere with the ability to implement or use health IT in a manner consistent with its certification. We believe that these additional disclosure requirements are necessary to ensure that existing and potential users and implementers of certified health IT are fully informed about these implementation considerations that accompany capabilities certified under the ONC Health IT Certification Program.

In the 2014 Edition final rule, we adopted new ''price transparency'' requirements that require ONC–ACBs to ensure that health IT developers include—on their Web sites and in all marketing materials, communications, and other assertions related to certified health IT—any ''additional types of costs'' that an EP, eligible hospital, or CAH would pay to implement certified health IT capabilities in order to meet meaningful use objectives and measures (§ 170.523(k)(1)(iii)). [238] We stated that there is value in requiring ONC–ACBs to ensure that developers are transparent about the types of costs associated with certified health IT and that such transparency could provide greater purchasing clarity to EPs, eligible hospitals, and CAHs (77 FR 54274). In regard to purchasing clarity, we further stated that this disclosure requirement could help prevent purchasers from being surprised by additional costs beyond those associated with the adoption and implementation of capabilities certified as part of their certified health IT (77 FR 54275). With this requirement and other transparency requirements under § 170.523(k)(1), we have sought to mitigate potential confusion in the marketplace and reduce the risk that consumers will encounter unexpected difficulties in the implementation and use of certified health IT.

Notwithstanding these modest disclosure requirements, many health IT consumers still have limited access to certain types of information necessary to accurately assess the potential costs, benefits, limitations, and trade-offs of alternative technologies and solutions.[239] This is especially true for small health care providers and other individuals and organizations who may not have the time, resources, or expertise to conduct extensive market research.[240] Health care and health IT industry participants and observers describe a marketplace in certified health IT products and services that is largely opaque and in which consumers often lack up-front information about the products and services they purchase or license. For example, the American Medical Association (AMA) has expressed concern on behalf of its provider members about ''the lack of transparency in EHR contracts,'' which ''may be unclear or fail to itemize specific expenses'' associated with certified health IT capabilities.[241] The

[238] 77 FR 54273–75. For example, under our current disclosure requirements, if health IT is certified to the ''view, download, and transmit to 3rd party'' certification criterion, and an EP would be expected to pay an ''ongoing'' monthly service fee to the technology developer for it to host/administer this capability in order for the EP to meet the correlated meaningful use objective and measure, the existence of this potential ''ongoing'' cost (though not the actual amount or ''dollar value'' of the cost itself) would need to be disclosed by the health IT developer. As another example, a Health IT Module certified to the public health electronic lab reporting certification criterion (§ 170.314(f)(4)) would be able to create a valid HL7 message for electronic submission. However, for the purposes of achieving meaningful use a hospital may be expected to pay their technology developer a separate ''one-time'' and/or ''ongoing'' interface development and configuration fee to establish connectivity between their certified Health IT Module and a public health authority. In such a situation, the potential costs of the interface development and configuration fee would need to be disclosed (though, again, the developer would not be required to disclose the actual ''dollar amount'' of the fee). A final example would be where a health IT developer charges a ''one-time'' fee to integrate its certified health IT with a hospital's other certified technology or a health information exchange organization. Again, just like the other examples, the potential for this fee (but not the ''dollar amount'' itself) would need to be disclosed by the technology developer. Building off these examples, we said that a health IT developer could meet the disclosure requirements by disclosing: 1) the type(s) of additional cost; and 2) to what the cost is attributed. In reference to the first example above, we stated that a developer could meet our price transparency requirement by disclosing that ''an additional ongoing fee may apply to implement XYZ online patient service.'' In situations where the same types of cost apply to different services, we stated that listing each as part of one sentence would be acceptable, such as ''a one-time fee is required to establish interfaces for reporting to immunization registries, cancer registries, and public health agencies.''

[239] *See, e.g.,* Jodi G. Daniel & Karson Mahler, *Promoting Competition to Achieve Our Health IT and Health Care Goals* (Oct. 7, 2014), *http://www.healthit.gov/buzz-blog/health-information-exchange-2/promoting-competition-achieve-healthit-health-care-goals/.*

[240] *See, e.g.,* Kelly Devers, Arnav Shah, and Fredric Blavin, *How Local Context Affects Providers' Adoption and Use of Interoperable Health Information Technology: Case Study Evidence from Four Communities in 2012 (Round One)* (2014), at 7 (describing significant challenges faced by smaller providers dealing with certified EHR vendors, including ''understanding vendor contracts that were very complex.'')

[241] FTC Workshop, Submission #00151 on behalf of the American Medical Association (April 30,

AMA further noted that while ONC has taken steps to promote greater contract transparency, these efforts have fallen short, ''leaving broad discretion and uncertainty'' in the marketplace for certified health IT products.[242]

Other observers have described practices that may interfere with the performance of certified health IT capabilities in ways that are not obvious to consumers at the time they purchase or license technology or services. For example, some health IT contracts may restrict a health care provider's ability to use data contained within an EHR[243] require health care provider staff to complete costly developer-imposed training and accreditation programs before they are allowed to extract patient data; or impose ''access and use agreements'' that restrict a provider's ability to ''engage a third party to assist with extracting and using data to benefit patients . . . .''[244] Some developers also purportedly charge ''additional fees to allow providers to extract patient data from their systems, even though the marginal cost of providing that data is small.[245] In addition, as discussed elsewhere in this proposed rule, Congress has expressed concern that some health IT developers of certified health IT may be engaging in business practices that block health information exchange and thereby frustrate congressional intent, devalue taxpayer investments in health IT, and make health IT less valuable and more burdensome for eligible hospitals and eligible providers to use.[246]

We do not assume that examples cited above are typical or widespread. Yet it must be acknowledged that even ONC has but limited visibility into developers' business practices and cannot reliably assess the extent to which such practices are occurring or the degree to which they may be interfering with the successful implementation and use of certified health IT. That acknowledgement alone should be a sufficient indication of the need to require greater transparency in the marketplace.[247]

The prevailing lack of transparency raises several specific and serious concerns. Most importantly, health IT developers not disclosing known material limitations or additional types of costs associated with the implementation or use of certified health IT creates a substantial risk that existing or prospective users will encounter problems implementing the capabilities of the health IT in a manner consistent with its certification. This in turn diminishes the reliability of certifications issued under the ONC Health IT Certification Program. Moreover, inadequate or incomplete information about health IT products and services distorts the marketplace for certified health IT, for without reliable information consumers cannot accurately estimate costs and assess capabilities in order to effectively compare technologies and choose appropriate solutions for their individual circumstances or needs.[248] Poor health IT purchasing decisions increase the likelihood of downstream implementation challenges and, ultimately, reduced opportunities to use health IT to improve health and health care. Finally, consumers who purchase or license inappropriate or suboptimal technologies may find it difficult to switch to superior alternatives due to the often significant financial and other resources they have already invested in implementation, training, integration with other IT systems, new clinical and administrative processes, and the many other costs and organizational changes associated with implementing health IT. When providers become ''locked in'' to technologies or solutions that do not meet their needs or the needs of their patients, health IT developers may have fewer incentives to innovate and compete on those aspects of health IT that these consumers most value.

For all of these reasons, we propose to revise the principles of proper conduct for ONC–ACBs in order to supplement and strengthen our existing transparency and disclosure requirements under the ONC Health IT Certification Program. As currently set forth in § 170.523(k), ONC–ACBs must require health IT developers to disclose conspicuously on their Web sites and in all marketing materials, communications statements, and other assertions related to certified health IT any additional types of costs[249] that an EP, eligible hospital, or CAH would pay to implement certified health IT to meet meaningful use objectives and measures. We propose to carry forward and expand these requirements as follows.

First, we would no longer limit health IT developers' disclosure obligations to the scope of the EHR Incentive Programs. In the context of our proposals in this proposed rule to make the ONC Health IT Certification Program open and accessible to more types of health IT and to health IT that support various care and practice settings beyond the EHR Incentive Programs, we believe that disclosure requirements should go beyond a link to the EHR Incentive Programs. Consumers are increasingly seeking to leverage certified health IT for a wide range of uses beyond the EHR Incentive Programs, such as to support care coordination with other types of health care providers as part of new quality improvement initiatives and public and private sector value-based payment programs. These consumers of certified health IT need reliable information associated with implementing and using health IT for all of these uses, not just those that are tied to a meaningful use objective or measure. Likewise, as the ONC Health IT Certification Program begins to focus on supporting these new users and uses, it will be important to ensure that certification is meaningful and that surveillance is effective for all certified health IT and capabilities, not just those

2014), available at *http://www.ftc.gov/system/files/documents/public_comments/2014/04/00151–89996.pdf* (accessed Dec. 19, 2014).

[242] *Id.*

[243] FTC Workshop, Submission #00187 on behalf of the Advisory Board Company (April 30, 2014), available at *http://www.ftc.gov/system/files/documents/public_comments/2014/04/00187-89979.pdf* (accessed Dec. 19, 2014).

[244] *Id.*

[245] FTC Workshop, Submission #00045 on behalf of the Health IT Now Coalition (March 10, 2014), available at *http://www.ftc.gov/system/files/documents/public_comments/2014/03/00045-88879.pdf* (accessed Dec. 19, 2014).

[246] 160 Cong. Rec. H9047, H9839 (daily ed. Dec. 11, 2014) (see explanatory statement submitted by Rep. Rogers, chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015).

[247] We recognize that there is value in encouraging developers to experiment, innovate, and compete to deliver products and services that consumers demand and also to price and distribute such products and services in ways that consumers find attractive and that meet the needs of individual customers. Our proposal to require greater transparency in developers' business practices is intended not to limit but to promote such price and non-price innovation and competition by providing individuals who purchase or license certified health IT with access to basic information necessary to make informed decisions in the marketplace.

[248] *Compare* American Academy of Family Physicians, *Understanding EHR Contracting and Pricing, http://www.aafp.org/practice-management/health-it/product/contracting-pricing.html* (accessed Dec 7, 2014) (noting that there are ''many different ways of pricing EHR software'' and that to ''compare 'apples to apples''' potential purchasers need to consider many variables when selecting an EHR) *with* FTC Workshop, Submission #00151 on behalf of the American Medical Association (April 30, 2014) (expressing concern about ''lack of transparency in EHR vendor contracts'' and ''broad discretion and uncertainty'' despite ONC efforts to promote greater transparency).

[249] Costs vary widely across different developers, products, and services. They may include but are not limited to the cost of purchasing or licensing necessary equipment and software; installing, configuring, maintaining, and updating technology; training staff and integrating technology into clinical workflows; securing and backing up data; licensing information or services used in conjunction with technology; and establishing interfaces or connectivity to other IT systems. Costs may also be incurred on a ''one time'' or on a ''recurring'' or ''ongoing'' basis.

that that are directly tied to the EHR Incentive Programs. For these reasons, we would require ONC–ACBs to ensure that developers disclose any ''additional types of costs'' that a user may incur in order to implement or use capabilities of certified health IT, whether to demonstrate meaningful use objectives or measures or for any other purpose within the scope of the health IT's certification.

Second, the important reasons we have described above for requiring greater transparency and disclosure convince us that we must move beyond our current focus on identifying additional types of costs and consider other factors that may similarly interfere with a user's ability to successfully implement certified health IT. In particular, the failure to disclose material information about limitations associated with certified health IT creates a substantial risk that current or prospective users will encounter problems implementing certified health IT in a manner consistent with its certification. From the perspective of both ONC and the consumer, therefore, the disclosure of this information is no less important than the disclosure of information about additional types of costs. Accordingly, we propose to add this additional category of information to those which a health IT developer must disclose.

Third, to ensure that these disclosure requirements serve their intended purpose, we propose that developers' disclosures be broader and provide greater detail than is currently required. In contrast with our current price transparency requirement, which requires disclosure only of additional types of costs that a user ''would pay'' to implement certain capabilities, our proposal would require health IT developers to be more proactive in identifying the kinds of limitations and additional types of costs that a user *may* pay or encounter in order to achieve any use within the scope of a Complete EHR or Health IT Module's certification. For example, we expect that health IT developers would disclose any additional types of costs or limitations that may be based on potential conditions applicable to the user or options available to the user. This would be different than the current ''would pay'' requirement that focuses on more definitive circumstances. We believe that it is reasonable to require health IT developers to identify this information because they are uniquely familiar with the costs and limitations of their own products and services and possess sophisticated technical knowledge related to the implementation and use of health IT in a variety of settings in which their products are services are deployed.

Health IT developers would therefore be required to provide, in plain language, a detailed description of any material information about limitations that a purchaser may encounter and additional types of costs that a user may be required to pay in the course of implementing or using capabilities to achieve any use within the scope of the its certification. Such information would be ''material'' (and its disclosure therefore required) if the failure to disclose it could substantially interfere with the ability of a user or prospective user to implement certified health IT in a manner consistent with its certification.

To illustrate our expectations as to the types of information that health IT developers would be required to disclose, we provide the following list of types of limitations and additional types of costs that would always be ''material'' and required to be disclosed. We seek comment on whether we should revise or add to the types of information delineated below, including whether we should require the disclosure of more specific cost structures (*e.g.,* the cost structure of a health IT developer's for sending transitions of care summaries, including all relevant factors—*e.g.,* volume transmissions, geography, interfaces, and exchange partner technology).

- Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.
- Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified.
- Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

Because this proposal would significantly expand a health IT developer's existing disclosure obligations, we further clarify our expectations regarding what a health IT developer would and would not be required to disclose. A health IT developer would not be required to disclose specific prices or price information. The health IT developer would be required, however, to describe with particularity the nature and magnitude of any additional types of costs, providing sufficient detail from which a person could arrive at a reasonably accurate estimation of what the likely costs might be, given the person's circumstances and intended use of the capabilities within the certified health IT. For example, if a health IT developer charged a fee every time a user wished to send a transition of care summary record to another user of certified health IT, the health IT developer would be required to fully disclose not only the existence of the fee but the circumstances in which it would apply. The health IT developer would also be required to provide additional information to assist the user in realistically estimating what the cost would be to use the transitions of care capability. The health IT developer could satisfy this requirement by providing data illustrating that there are levels of costs for different types of users (*e.g.,* users who send a ''low,'' ''medium,'' or ''high'' number of summary of care records per month). Alternatively, the health IT developer could indicate that for most (*e.g.,* nine out of every ten) of its users, transaction fees represent less than 1% of a user's total monthly service costs. Other methods of disclosure would also suffice, provided they were similarly calculated and likely to inform.

Health IT developers would not be required to disclose trade secrets or intellectual property. Similar to the disclosure of information about additional types of costs, health IT developers could describe other types of limitations in terms that protect their intellectual property interests and trade secrets. Generalized assertions of ''proprietary information'' would not immunize a developer, however, from a finding by an ONC–ACB that the developer failed to disclose known material information.

Health IT developers would not be required to disclose information of which they are not and could not reasonably be aware. In particular, we recognize that health IT functions in combination with many third party technologies and services whose specific costs/limitations may be difficult for a health IT developer to precisely predict or ascertain. Local implementation factors and other individual circumstances also vary substantially among customers and impact the cost and complexity of implementing certified health IT. In addition, the costs of upgrading health IT to meet new regulatory requirements or compliance timelines, which are subject to change, may make some particular types of additional costs especially difficult to forecast. While we do not expect health IT developers to account for every conceivable cost or implementation hurdle that a customer may encounter in order to successfully implement and use the capabilities of a developer's certified health IT, we believe it reasonable to assume that health IT developers are experts in their own products and services and possess sophisticated technical knowledge related to the implementation and use of health IT in a variety of settings in which their products are used. Through their accumulated experience developing and providing health IT solutions to their customers, health IT developers should over time become familiar with the types of costs and limitations that most users encounter, and should be able to describe these in sufficient detail so as to provide potential customers with the information they need to make informed purchasing and implementation decisions. We also believe that it is reasonable to expect that a health IT developer would provide a detailed description of any additional considerations that a customer should be aware of in order to reliably estimate the resources needed to purchase the certified health IT and arrive at a realistic expectation of the product's capabilities and performance in the field, to the extent that the health IT developer has knowledge of the customer's circumstances and based on its range of experience (including with other customers).

We propose one additional aspect that we believe will complement the mandatory disclosure requirements set forth in this proposal. In addition to requiring health IT developers to disclose known material information about their certified health IT, an ONC–ACB would be required to obtain a voluntary public attestation from every health IT developer to which it issues or has at any previous time issued a certification for any edition of certified health IT. The attestation would take the form of a written ''pledge'' by the health IT developer to be transparent with regard to the information it is required to disclose under the ONC Health IT Certification Program. Specifically, the health IT developer would be required to attest that, in addition to disclosing such information via its public Web site, marketing materials, communications statements, and other assertions related to certified health IT, it will voluntarily provide this information to: (1) Customers, prior to providing any certified health IT or related product or service (including subsequent updates, add-ons, or additional products or services to be provided during the course of an on-going contract); (2) prospective customers (*i.e.,* persons who request or receive a quotation, estimate, or other similar marketing or promotional material); and (3) other persons who request such information.

To be clear, this attestation would not broaden or change the types of information that a health IT developer would be required to disclose as a condition of certification, nor the persons to whom such information would have to be disclosed. While all health IT developers would be required to make the attestation, their adherence to it would be strictly voluntary, and an ONC–ACB would continue to hold health IT developers only to the mandatory disclosure requirements already described above in this proposal and proposed at § 170.523(k)(1).

Although the attestation would not establish any new regulatory disclosure obligations for health IT developers, it would create a powerful incentive for health IT developers to go beyond what is strictly required of them by regulation and to be more transparent about their health IT products, services, and business practices. The attestation would accomplish this goal by publicly committing health IT developers to make a good faith effort to ensure that consumers actually receive the information that developers are required to disclose at such times and in such a manner as is likely to be useful in informing their health IT purchasing or licensing, implementation, and other decisions.

In particular, health IT developers would be required to attest publicly that they will provide information about their certified health IT to any person who requests it. This would empower not only existing or prospective customers but all consumers and their representatives (*e.g.,* providers' professional associations) to approach developers directly and request information that is most relevant to consumers' health IT purchasing or licensing, and implementation decisions. We believe that as a result consumers will come to expect greater transparency from health IT developers in general, and that developers, having publicly attested that they will provide this information, will have a stronger interest in doing so in order to protect their reputations. Moreover, health IT developers who are the most transparent and provide the most meaningful information about their products and services will be able to differentiate themselves from their competitors, creating additional incentives for other developers to be more transparent.

Attestation will, by encouraging greater interaction between health IT developers and all consumers, provide important feedback to developers about the types of information that consumers find important, and which are therefore likely to be material for purposes of health IT developers' mandatory disclosure obligations under the ONC Health IT Certification Program. For example, requests for information and other feedback from consumers may alert a health IT developer to the fact that it has failed to disclose (or to disclose with sufficient specificity) material information about a particular limitation or additional type of cost associated with its certified health IT. By encouraging consumers to make such inquiries, the proposed attestation requirement will assist health IT developers in meeting their disclosure obligations.

Overall, we believe these proposed requirements will enable more transparency in the marketplace for certified health IT, provide consumers with greater and more ready access to information relevant to their health IT planning, purchasing, and implementation decisions, and reduce the risk of implementation problems and surprise described in this proposal.

3. Open Data Certified Health IT Product List (CHPL)

In the initial rulemaking that we used to establish the Temporary Certification Program, we indicated that the National Coordinator intended to make a master CHPL of all Complete EHRs and EHR Modules tested and certified by ONC–ATCBs available on the ONC Web site and that the CHPL would be a public service and would be a single, aggregate source of all the certified product information ONC–ATCBs provide to the National Coordinator (75 FR 36170). Since 2010, we have maintained the CHPL and as the ONC Health IT Certification Program has matured, ONC–ACBs have continued to report the products and information about the products they have certified to ONC for listing on the CHPL.

As part of the 2014 Edition final rule (77 FR 54271), we required additional transparency in the ONC Health IT Certification Program in the form of a hyperlink that ONC–ACBs needed to maintain that would enable the public to access the test results that the ONC–ACB used as the basis for issuing a certification. In the time post-final rule, the NVLAP Accredited Testing Laboratories (ATLs) and ONC–ACBs worked together to develop a standard test results summary template for consistent data presentation and use throughout the ONC Health IT Certification Program. For all 2014 Edition products certified under the ONC Health IT Certification Program, the test result summary is accessible and can be found as part of the product's detailed information page on the CHPL Web page.

The test result summary includes granular detail from ATLs about the testing performed, including, among other information: The certification criteria tested; the test procedure, test data, and test tool versions used during testing for each certification criterion; instances where optional portions of certification criteria were tested; and which standard was used for testing when a certification criterion allowed for more than one standard to be used to meet the certification criterion. The test result summary also includes the user-centered design information and summative tests results applicable to a product in cases where it was required to meet the ''safety-enhanced design'' certification criterion (§ 170.314(g)(3)) in order to ultimately be certified.

Multiple stakeholders have commented to us that while the availability of the test report summary and the addition detail it contains is beneficial, its location on the CHPL and its overall accessibility as a PDF makes it difficult to use for any kind of product analysis. In response to this feedback and our overall vision to efficiently administer the CHPL in the future, we intend to convert the CHPL in its current form to an open data file represented in both XML and JSON and with accompanying API functionality. We estimate that this conversion along with the future additional data collection we have proposed for 2015 Edition certifications will occur over the next 12 to 18 months.

To complement this conversion, we propose to require ONC–ACBs to report an expanded set of information to ONC for inclusion in the open data file that would make up the CHPL. Specifically, we propose to revise § 170.523(f) to move the current (f) to (f)(2) and to create a new paragraph (f)(1) that would require ONC–ACBs upon issuing a 2015 Edition (or any subsequent edition certification) to report on the same data elements they report to ONC under § 170.523(f), the information contained in the publicly available test report, and additional data. The data that would be required is as follows:

- The Health IT Module developer name; product name; product version; developer Web site, physical address, email, phone number, and contact name;
- The ONC–ACB Web site, physical address, email, phone number, and contact name, contact function/title;
- The ATL Web site, physical address, email, phone number, and contact name, contact function/title;
- Location and means by which the testing was conducted (*e.g.,* remotely with developer at its headquarters location);
- The date(s) the Health IT Module was tested;
- The date the Health IT Module was certified;
- The unique certification number or other specific product identification;
- The certification criterion or criteria to which the Health IT Module has been certified, including the test procedure and test data versions used, test tool version used, and whether any test data was altered (*i.e.,* a yes/no) and for what purpose;
- The way in which each required privacy and security criterion was addressed for the purposes of certification (note: this is proposed to track the privacy and security certification proposal for Health IT Modules);
- The standard or mapping used to meet the quality management system certification criterion;
- The standard(s) or lack thereof used to meet the accessibility-centered design certification criterion;
- *Where applicable,* the hyperlink to access an API's documentation and terms of use;
- *Where applicable,* which certification criteria were gap certified;
- *Where applicable,* if a certification issued was a result of an inherited certified status request;
- *Where applicable,* the clinical quality measures to which the Health IT Module has been certified;
- *Where applicable,* any additional software a Health IT Module relied upon to demonstrate its compliance with a certification criterion or criteria adopted by the Secretary;
- *Where applicable,* the standard(s) used to meet a certification criterion where more than one is permitted;
- *Where applicable,* any optional capabilities within a certification criterion to which the Health IT Module was tested and certified;
- *Where applicable,* and for each applicable certification criterion, all of the information required to be submitted by Health IT Module developers to meet the safety-enhanced design certification criterion (note: This would include each user-centered design element required to be reported at a granular level (*e.g.,* task success/failure)); and
- *Where applicable,* for each instance in which a Health IT Module failed to conform to its certification and for which a corrective action plan was instituted under § 170.556:
  - ○ The specific certification criterion or certification program requirement (*e.g.,* required disclosure) to which the health IT failed to conform as determined by the ONC–ACB;
  - ○ the dates surveillance was initiated and when available, completed;
  - ○ the results of the surveillance (pass rate for each criterion);
  - ○ the number of sites that were used in surveillance;
  - ○ the date corrective action began;
  - ○ when available, the date corrective action ended;
  - ○ a summary of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformance; and
  - ○ when available, the developer's explanation of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformance.

Consistent with ONC–ACBs' current reporting practice required by § 170.523(f), ONC–ACBs would be required to submit the additional data listed above no less frequently than weekly. Because this expanded list of data would largely subsume the data included in the test results summary, we would no longer require for 2015 Edition and subsequent edition certifications that ONC–ACBs provide a publicly accessible hyperlink to the test results used to certify a Health IT Module.

The last category of data above would be reportable for Complete EHRs and Health IT Modules that have been designated for corrective action as described in our proposal '''In-the-field' Surveillance and Maintenance of Certification'' above. Under that proposal, an ONC–ACB would be required to initiate a corrective action plan for a Complete EHR or Health IT

Module when randomized in-the-field surveillance reveals a pattern of non-conformance to any prioritized certification criterion. Under this Open Data CHPL proposal, the initiation of corrective action would trigger the duty to report the surveillance-related information specified in the last category above for inclusion in the open data file. This reporting requirement would be separate from and in addition to the ''rolling'' (*i.e.,* at least quarterly) reporting of all surveillance results described in our in-the-field surveillance proposal referenced above. The purpose of this separate reporting requirement would be to ensure that health IT users, implementers, and purchasers are alerted to potential conformance issues in a timely and effective manner, consistent with the patient safety, program integrity, and transparency objectives described in this proposed rule. By incorporating data on health IT that has failed surveillance in the open data file, such information would be updated and available to the public at least weekly. Combined with the API functionality described above, such data could also be used more effectively by patient safety, consumer, and other organizations to analyze and disseminate information about product safety and performance.

Our rationale with respect to the reporting of data for health IT that has failed surveillance applies to all, and not only 2015 Edition, certified health IT. Accordingly, we propose to revise new § 170.523(f)(2) (formerly § 170.523(f)) so as to also require the reporting of this surveillance-related data for health IT certified to the 2014 Edition.

In submitting this data related to surveillance of certified health IT, ONC–ACBs would be required to exclude any information that would identify any user or location that participated in or was subject to surveillance (as currently required for ONC–ACBs' annual surveillance results reported to the ONC).

None of the reporting requirements above would require (or authorize) an ONC–ACB to submit or disclose health IT developer's proprietary business information or trade secrets. ONC–ACBs would be required to implement appropriate safeguards to ensure that any proprietary business information or trade secrets of the health IT developer the ONC–ACB might encounter during the course of its surveillance activities would be kept confidential by the ONC–ACB and protected from disclosure. With respect to the safety-enhanced-design data, as stated in our proposal for the 2015 Edition ''safety-enhanced design'' certification criterion (section III.A.3 of this preamble), we do not expect health IT developers to include proprietary information in the submission of summative usability test results to ONC–ACBs. Accordingly, ONC–ACBs would not be required and should take care not to submit proprietary information to ONC for inclusion in the open data file. Similarly, with respect to the reporting of surveillance information for health IT for which corrective action has been initiated, an ONC–ACB would be able to meet the requirement to report a summary of the deficiencies leading to its determination that health IT no longer conforms to the requirements of its certification without disclosing information that the ONC–ACB believes could be proprietary or expose it to liability. Should we adopt this proposal, we would provide additional guidance to ONC–ACBs regarding the particular format of the data required to be submitted to the open data file.

While we recognize that this additional data places a new reporting burden on ONC–ACBs, we believe that the benefit to the public of having all of this data about product certification in granular detail far outweighs the administrative burden it will take to report this information. Further, depending on the certification scope sought some of this data will not need to be collected by ONC–ACBs or will be in hand for subsequent issued certifications. We seek public comment on whether we have omitted any additional data generated during the testing and certification process or the surveillance process that would be useful to the public.

Consistent with these proposals, we also propose to make a conforming modification to 45 CFR 170.523(k)(1)(ii) which currently cross references § 170.523(f) to cross reference proposed paragraph (f)(2) for 2014 Edition certifications and an equivalent set of data (minus the test results summary) in paragraph (f)(1) for 2015 Edition and subsequent certifications.

4. Records Retention

We propose to change the records retention requirement in § 170.523(g) in two ways. We propose to require that ONC–ACBs retain all records related to the certification of Complete EHRs and/or Health IT Module(s) (including EHR Modules) for a minimum of six years instead of five years as currently required. This proposed revision would make certification records available longer, which may be necessary for HHS programs' purposes, such as evaluations our audits. To illustrate, certification to the 2014 Edition began in early 2013 and CMS proposes in the EHR Incentive Programs Stage 3 proposed rule, published elsewhere in this issue of the **Federal Register**, to permit the use of health IT certified to the 2014 Edition through 2017. With attestation taking place in 2018, records may need to be available for a minimum of six years. In addition, a six-year records retention requirement aligns with current accreditation standards within the industry. We also propose that records of certifications performed under the ONC Health IT Certification Program must be available to HHS upon request during the six-year period that a record is retained. We believe this would help clarify the availability of certification records for agencies (*e.g.,* CMS) and authorities (*e.g.,* the Office of Inspector General) within HHS.

5. Complaints Reporting

We propose that ONC–ACBs provide ONC (the National Coordinator) with a list of complaints received on a quarterly basis. We propose that ONC–ACBs indicate in their submission how many complaints were received, the nature or substance of the complaint, and the type of complainant (*e.g.,* type of provider, health IT developer, etc.). We believe this information will provide further insight into potential concerns with certified health IT or the ONC Health IT Certification Program and give ONC a better ability to identify trends or issues that may require action including notification of the public. We propose to include this new requirement in § 170.523(n).

6. Adaptations and Updates of Certified Health IT

We propose a new principle of proper conduct (PoPC) that would serve to benefit ONC–ACBs as well as all stakeholders interested in the ONC Health IT Certification Program and the health IT certified under the program. We propose to require that ONC–ACBs obtain monthly reports from health IT developers regarding their certified health IT. Specifically, we propose to require that ONC–ACBs obtain a record of all adaptations and updates, including changes to user-facing aspects, made to certified health IT (*i.e.,* Complete EHRs and certified Health IT Modules), on a monthly basis each calendar year. We request comment on whether we should require even more frequent reporting.

This new PoPC would apply for all certified Complete EHRs and certified Health IT Modules (which includes ''EHR Modules'') to the 2014 Edition and all certified Health IT Modules to the 2015 Edition. The PoPC would become effective with a subsequent final rule and we would expect ONC–ACBs to begin complying with the PoPC at the beginning of the first full calendar month that is at least 30 days after the effective date of the final rule. For example, if a final rule became effective on September 6, 2015, then the first full calendar month would be November 2015. In this instance and others, there may be no record to obtain from some health IT developers because their Complete EHRs and Health IT Modules may have been recently certified and they may not have yet created any adaptations or made any updates. We would, however, expect that a health IT developer would still provide a ''record'' indicating that no adaptations had been created and that no updates had occurred to its ONC–ACB for its certified health IT.

We would not expect the information in these records to be reported to ONC and listed on the CHPL. Rather, in weighing the need for ONC–ACBs to properly manage the certifications they issue versus the additional burden a regulatory scheme of ''check-ins'' and potential re-testing/certification for every adaptation and update, we determined that the best course of action would be to provide awareness to ONC–ACBs on adaptations and updates made to technologies they certified. By doing so, we believe ONC–ACBs would be able to make informed decisions when conducting surveillance of certified Complete EHRs and certified Health IT Modules. For example, if an ONC–ACB became aware that a certified Health IT Module had been updated 10 or more times in a month (which could be common with cloud-based products), resulted in 6 adaptations over three months, or had its user-facing aspects altered in an apparent significant way, then an ONC–ACB may want to conduct surveillance on that certified Health IT Module. Overall, we believe our proposed approach protects the integrity of certified health IT and promotes safety and security of certified health IT in a way that seeks to minimizes burden for health IT developers.

E. ''Decertification'' of Health IT—Request for Comment

In the explanatory statement [250] accompanying Public Law 113–235 (Consolidated and Further Continuing Appropriations Act, 2015) the Congress urged ONC to use its certification program to ensure certified electronic health record technology (CEHRT) provides value to eligible hospitals, eligible providers and taxpayers. It also stated that ONC should use its authority to certify only those products that clearly meet current meaningful use program standards and that do not block health information exchange. Further, it stated that ONC should take steps to ''decertify'' products that proactively block the sharing of information.

This proposed rule takes certain steps to support the certification of health IT that meets relevant program standards and permits the unrestricted use of certified capabilities that facilitate health information exchange (*see* the ''In-The-Field Surveillance and Maintenance of Certification'' and ''Transparency and Disclosure Requirements'' proposals in section IV.D of this preamble). We believe, however, that additional rulemaking would be necessary to implement any approach that would include ONC appropriating an ONC–ACB's delegated authority to issue and terminate a certification, including establishing new program requirements and processes by which ONC or an ONC–ACB would have the grounds to terminate an issued certification. Any such rulemaking would need to, at a minimum, address the circumstances, due process, and remedies for the termination of an issued certification. Given that Congress also requested the HITPC to consider and submit a report to them on the challenges and barriers to interoperability within the year,[251] we believe it is premature to include such proposals in this rulemaking. We do, however, solicit public comment on the circumstances, due process, remedies, and other factors that we should consider regarding the termination of a certification. In preparing comments in response to this solicitation, we ask commenters to keep in mind all parties involved, including ONC–ACBs, health IT developers, and consumers (including those providers that participate in the EHR Incentives Programs). Additionally, to help inform commenters, the following provides a brief background of the ONC Health IT Certification Program and examples of the complexities and potential impacts associated with terminating a certification.

Section 3001(c)(5) of the Public Health Service Act (PHSA) provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health information technology.[252] Specifically, this section requires the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), to keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with applicable certification criteria [253] (*i.e.,* certification criteria adopted by the Secretary under section 3004 of the PHSA). Section 3001(c)(5) also requires that any such certification program(s) must include, as appropriate, testing in accordance with section 13201(b) of the HITECH Act, which requires that with respect to the development of standards and implementation specifications, the Director of NIST support the establishment of a conformance testing infrastructure, including the development of technical test beds.

In developing the ONC Health IT Certification Program, ONC consulted with NIST and created the program structure based on industry best practice. This structure includes the use of two separate accreditation bodies: (1) An accreditor that evaluates the competency of a health IT testing laboratory to operate a testing program in accordance with international standards; and (2) an accreditor that evaluates the competency of a health IT certification body to operate a certification program in accordance with international standards. After a certification body is accredited, it may apply to the National Coordinator to receive authorization to certify health IT on ONC's behalf. Once authorized, we refer to these certification bodies as ONC-Authorized Certification Bodies or ONC–ACBs. The ONC Health IT Certification Program includes a full process by which ONC oversees the operations of ONC–ACBs. It also includes a process for the issuance of certain types of violations as well as a process to revoke an ONC–ACBs authorization to certify health IT on ONC's behalf.[254]

[250] 160 Cong. Rec. H9047, H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015); and *https://www.congress.gov/congressional-record/2014/12/11/house-section/article/H9307-1.*

[251] *https://www.congress.gov/congressional-record/2014/12/11/house-section/article/H9307-1.*

[252] ''health information technology'' is defined in Section 3000(5) to mean ''hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information''.

[253] ''certification criteria'' is defined in Section 3001(c)(5)(B) to mean ''with respect to standards and implementation specifications for health information technology, criteria to establish that the technology meets such standards and implementation specifications.''

[254] See the Permanent Certification Program final rule (76 FR 1262); subpart E, part 170 of title 45;

With respect to ONC–ACBs and the international standard (ISO Guide 65/ ISO 17065) to which they are accredited, they are uniquely positioned and accountable for determining whether a certified product continues to conform to the certification requirements to which the product was certified. If an ONC–ACB can substantiate a non-conformity, either as a result of surveillance or otherwise, the international standard requires that the ONC–ACB consider and decide upon the appropriate action, which could include: (1) The continuation of the certification under specified conditions (*e.g.* increased surveillance); (2) a reduction in the scope of certification to remove nonconforming product variants; (3) suspension of the certification pending remedial action by the developer; or (4) withdrawal/ termination of the certification.[255]

With respect to ONC's role and ability to revoke or terminate an issued certification, ONC's regulations do not address this point directly and have largely deferred, with one exception, to the ONC–ACBs autonomy and delegated authority to effectively administer its certification business. The one exception involves the scenario where ONC revokes an ONC–ACB's authorization due to a ''type-1'' program violation that calls into question the legitimacy of the issued certification (see 45 CFR 170.570). In such an instance, we established a process by which the National Coordinator would review and determine whether an ONC–ACB's misconduct justifies revoking the certification issued to one or more products (76 FR 1297–99).

In general, we believe that it's important for commenters to account for the potentially profound asymmetric impacts revoking a certification could create, especially if based on the business practices (by a health IT developers or their customers) associated with the health IT's use and not necessarily the health IT's performance according to certification requirements. These asymmetric impacts are present in any paradigm in which a certified product is required for compliance with a program (*e.g.,* the use of certified health IT under the Medicare and Medicaid EHR Incentive Programs and Electronic Prescribing of Controlled Substances). To illustrate, the impact of revoking a certification based on a health IT developer's business practice(s) may create a lopsided (and arguably unfair/ inequitable) impact to all those who rely on the certification in order to comply with the legal requirement(s) of a program they are participating in. Additionally, if such a health IT developer's business practice(s) were not universally applied to all customers, the outright removal of a certification could unfairly penalize the health IT developer's other customers who were unaffected by the business practice. Similarly, if the practices of a group of a health IT developer's customers were found to be impeding information exchange, outright revoking the product's certification (for how it was requested to be implemented or configured) could in this case unfairly penalize the health IT developer as well as other ''good actor'' customers and information exchange partners of the developer. We also note that there could be contractual and other legal agreements affected by any action that terminates a certification.

All of the above potential circumstances are meant to highlight for commenters the significant analysis, complexity, and need for root cause determinations that would be necessary to develop and implement a regulatory scheme supporting an equitable certification termination process led or directed by ONC under the ONC Health IT Certification Program. To support justification of such a process based on the blocking of health information exchange, we further solicit comment on examples of health IT certified under the ONC Health IT Certification Program that may have been used in the past, or currently, to proactively block the sharing of health information.

V. Response to Comments

Because of the large number of public comments normally received in response to Federal Register documents, we are not able to acknowledge or respond to them individually. We will consider all comments we receive by the date and time specified in the **DATES** section of this preamble, and, when we proceed with a subsequent document, we will respond to the comments in the preamble of that document.

VI. Incorporation by Reference

The Office of the Federal Register has established new requirements for materials (*e.g.,* standards and implementation specifications) that agencies propose to incorporate by reference in the **Federal Register** (79 FR 66267; 1 CFR 51.5(a)). Specifically, § 51.5(a) requires agencies to discuss, in the preamble of a proposed rule, the ways that the materials it proposes to incorporate by reference are reasonably available to interested parties or how it worked to make those materials reasonably available to interested parties; and summarize, in the preamble of the proposed rule, the material it proposes to incorporate by reference.

To make the materials we intend to incorporate by reference reasonably available, we provide a uniform resource locator (URL) for the standards and implementation specifications. In many cases, these standards and implementation specifications are directly accessible through the URL provided. In instances where they are not directly available, we note the steps and requirements necessary to gain access to the standard or implementation specification. In most of these instances, access to the standard or implementation specification can be gained through no-cost (monetary) participation, subscription, or membership with the applicable standards developing organization (SDO) or custodial organization. In a few instances, where noted, access requires a fee or paid membership.

The National Technology Transfer and Advancement Act (NTTAA) of 1995 (15 U.S.C. 3701 *et seq.*) and the Office of Management and Budget (OMB) Circular A–119 [256] require the use of, wherever practical, technical standards that are developed or adopted by voluntary consensus standards bodies to carry out policy objectives or activities, with certain exceptions. The NTTAA and OMB Circular A–119 provide exceptions to selecting only standards developed or adopted by voluntary consensus standards bodies, namely when doing so would be inconsistent with applicable law or otherwise impractical. As discussed in section III of this preamble, we have followed the NTTAA and OMB Circular A–119 in proposing standards and implementation specifications for adoption, including describing any exceptions in the proposed adoption of standards and implementation specifications. Over the years of adopting standards and implementation specifications for certification, we have worked with SDOs, such as HL7, to make the standards we propose to adopt, and subsequently adopt and incorporate by reference in the **Federal Register**, available to interested stakeholders. As described above, this includes making the standards and implementation specifications available

and *http://www.healthit.gov/policy-researchers-implementers/about-onc-hit-certification-program.*

[255] ISO 17065 (§ 170.599(b)(3)). See also § 170.599(a) for general availability of this standard.

[256] *http://www.whitehouse.gov/omb/circulars_a119.*

through no-cost memberships and no-cost subscriptions.

As required by § 51.5(a), we provide summaries of the standards and implementation specifications we propose to adopt and subsequently incorporate by reference in the **Federal Register**. We also provide relevant information about these standards and implementation specifications throughout section III of the preamble. In particular, in relevant instances, we identify differences between currently adopted versions of standards and implementation specifications and proposed versions of standards and implementation specifications.

We have organized the following standards and implementation specifications that we propose to adopt through this rulemaking according to the sections of the Code of Federal Regulation (CFR) in which they would be codified and cross-referenced for associated certification criteria that we propose to adopt in 45 CFR 170.315. We note, in certain instances, we request comment in this proposed rule on multiple standards or implementation specifications that we are considering for adoption *and incorporation by reference* for a particular use case. We include all of these standards and implementation specifications in this section of the preamble.

Transport and Other Protocol Standards—45 CFR 170.202

- *ONC Implementation Guide for Delivery Notification in Direct.*

URL: *http://wiki.directproject.org/file/view/Implementation+Guide+for+Delivery+Notification+in+Direct+v1.0.pdf.* This is a direct link.

Summary: This document provides implementation guidance enabling Security/Trust Agents (STAs) to provide a high level of assurance that a message has arrived at its destination. It also outlines the various exception flows that result in a compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system.

- *Healthcare Provider Directory, Trial Implementation, October 13, 2014.*

URL: *http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf.* This is a direct link.

Summary: This document introduces the Healthcare Provider Directory (HPD) that supports queries against and management of, health care provider information that may be publicly shared in a directory structure. HPD directory structure is a listing of two categories of health care providers, individual and organizational providers.

Functional Standards—45 CFR 170.204

- *HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application. (''Infobutton''), Knowledge Request, Release 2.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=208.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Context-aware knowledge retrieval specifications (Infobutton) provide a standard mechanism for clinical information systems to request context-specific clinical knowledge from online resources. Based on the clinical context, which includes characteristics of the patient, provider, care setting, and clinical task, Infobutton(s) anticipates clinicians' and patients' questions and provides automated links to resources that may answer those questions.

- *HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=283.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: Context-aware knowledge retrieval (Infobutton) into clinical information systems help deliver clinical knowledge to the point of care as well as patient-tailored education material. This specification enables the implementation of context-aware knowledge retrieval applications through a Service Oriented Architecture based on the RESTful software architectural style.

- *HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=22.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: Context-aware knowledge retrieval (Infobutton) in clinical information systems help deliver clinical knowledge to the point of care as well as patient-tailored education material. This implementation guide provides a standard mechanism for EHR systems to submit knowledge requests over the HTTP protocol through a standard using a URL format.

- *HL7 Version 3 Standard: Clinical Decision Support Knowledge Artifact Specification, Release 1.2 Draft Standard for Trial Use.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=337.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Clinical Decision Support Knowledge Artifact Specification provides guidance on how to specify and implement shareable CDS knowledge artifacts using XML. The scope of the Specification includes event-condition-action rules, order sets, and documentation templates.

- *HL7 Implementation Guide: Decision Support Service, Release 1.1, US Realm, Draft Standard for Trial Use.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=334.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: A Decision Support Service takes in patient data as the input and provides back patient-specific assessments and recommendations. A Decision Support Service facilitates the implementation of CDS capabilities in a scalable manner. This implementation guide defines a Decision Support Service implementation approach that combines the HL7 Decision Support Service Release 2 standard with the HL7 Virtual Medical Record for CDS information model standard to enable the provision of standards-based, interoperable decision support services.

Content Exchange Standards and Implementation Specifications for Exchanging Electronic Health Information—45 CFR 170.205

- *HL7 Implementation Guide for CDA® R2: Quality Reporting Document Architecture—Category I, DSTU Release 2 (US Realm) and Errata (September 2014).*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=35.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement. The DSTU package must be downloaded in order to access the errata.

Summary: The Quality Reporting Document Architecture (QRDA) is an electronic document format that provides a standard structure with which to report quality measure data to organizations that will analyze and interpret the data. The Implementation Guide is consistent with CDA, and Category I is an individual-patient-level quality report. The September 2014 Errata reflects updates for the implementation of QRDA Category I consistent with the Quality Data Model-based Health Quality Measures Format Release 2.1, an incremental version of harmonized clinical quality measure and CDS standards.

- *HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.0.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=379.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Consolidated CDA (C–CDA) implementation guide contains a library of CDA templates, incorporating and harmonizing previous efforts from HL7, IHE, and Health Information Technology Standards Panel (HITSP). It represents harmonization of the HL7 Health Story guides, HITSP C32, related components of IHE Patient Care Coordination (IHE PCC), and Continuity of Care (CCD). The C–CDA Release 2 implementation guide, in conjunction with the HL7 CDA Release 2 (CDA R2) standard, is to be used for implementing the following CDA documents and header constraints for clinical notes: Care Plan including Home Health Plan of Care, Consultation Note, CCD, Diagnostic Imaging Reports, Discharge Summary, History and Physical, Operative Note, Procedure Note, Progress Note, Referral Note, Transfer Summary, Unstructured Document, and Patient Generated Document (US Realm Header).

- *HL7 Implementation Guide for CDA® Release 2: Additional CDA R2 Templates—Clinical Documents for Payers—Set 1, Release 1—US Realm, Draft Standard for Trial Use.*

URLs: *http://www.hl7.org/special/Committees/claims/index.cfm* and *http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember.* This is a direct access link to the most recent publicly available version of the implementation guide. HL7 policy normally requires a paid membership or a ''non-member participation'' fee to access the balloting process of a standard or implementation guide. HL7 has, however, agreed to make current balloted versions of the implementation guide freely available for review during the public comment period of this proposed rule. Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The purpose of the Clinical Documents for Payers—Set 1(CDP1) implementation guide is to provide guidance on a standardized, implementable, interoperable electronic solution to reduce the time and expense related to the exchange of clinical and administrative information between and among providers and payers. This guide describes structured documentation templates that meet requirements for documentation of medical necessity and appropriateness of services to be delivered or that have been delivered in the course of patient care. These document templates are designed for use when the provider needs to exchange more clinical information than is required by the C–CDA R2 document-level templates and/or must indicate why information for specific section-level or entry-level templates is not included.

- *HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=375.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Digital Signature and Delegation of Rights Implementation Guides provide a standardized method of applying Digital Signatures to CDA documents. The standard provides for multiple signers, signer's declaration of their role, declaration of purpose of the signature, long-term validation of the Digital Signatures and data validation of the signed content.

- *Author of Record Level 1: Implementation Guide.*

URL: *http://wiki.siframework.org/file/view/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx/539084894/esMD%20AoR%20Level%201%20Implementation%20Guide%20v5%20FINAL.docx.* This is a direct link. This implementation guide was developed under the Standards and Interoperability (S&I) Framework.[257]

Summary: The Author of Record Level 1 Implementation Guide utilizes the IHE Document Digital Signature standard and Security Assertion Markup Language (SAML) assertions to support applying digital signatures and delegation of rights information to bundles of documents exchanged over content neutral transports.

- *Provider Profiles Authentication: Registration Implementation Guide.*

URL: *http://wiki.siframework.org/file/view/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx/539084920/esMD%20Use%20Case%201%20Implementation%20Guide%20V24%20FINAL.docx.* This is a direct link. This implementation guide was developed under the Standards and Interoperability (S&I) Framework.[258]

Summary: The Provider Profiles Authentication Implementation Guide provides methods for applying digital signatures and delegation of rights information to the most common administrative and clinical transactions, including: ASC X12, CONNECT, Direct, and HL7 V2.

- *HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders from EHR, Draft Standard for Trial Use, Release 2—US Realm.*

URL: *http://www.hl7.org/participate/onlineballoting.cfm?ref=nav#nonmember.* HL7 policy normally requires a paid membership or a ''non-member participation'' fee to access the balloting process of a standard or implementation guide. HL7 has, however, agreed to make current balloted versions of the implementation guide freely available for review during the public comment period of this proposed rule. Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Laboratory Orders Implementation Guide identifies the requirements, specifications, and standards, and provides the implementation guidance for the electronic ordering of laboratory tests in the US Realm. The scope of the Laboratory Orders Interface Use Case includes requirements to enable a particular implementation of an Electronic Health Record System (EHR–S) to use standardized structured data in a defined inter-organizational laboratory transaction. The Use Case requirements are directed at laboratory test orders between an Ambulatory Provider's EHR–S and a Laboratory's Laboratory Information System (LIS). Future versions of this guide may harmonize with existing guides to extend interoperability of laboratory results across care settings, *e.g.,* acute care.

- *HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Test Compendium Framework, Release 2, Version 1.2 (eDOS).*

URL: *http://www.hl7.org/participate/online balloting.cfm?ref=nav#nonmember.* HL7 policy normally requires a paid membership or a ''non-member participation'' fee to access the balloting process of a standard or implementation guide. HL7 has, however, agreed to

[257] *http://www.healthit.gov/policy-researchers-implementers/standards-interoperability-si-framework.*

[258] *http://www.healthit.gov/policy-researchers-implementers/standards-interoperability-si-framework.*

make current balloted versions of the implementation guide freely available for review during the public comment period of this proposed rule. Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The focus of the Laboratory Test Compendium Framework is to provide a standardized means of electronically communicating a Laboratory's Directory of Services (eDOS). The content is owned by the sending laboratory for the purpose of being used by the compendium consumer to order laboratory services and to understand the requirements and components of those services. The consumer (and consuming systems) should not modify or delete the content unless instructed to do so by the producer via eDOS updates or some other form of written communication. Adding to the content to provide additional information specific to the consumer's needs such as cross reference to local codes and/or other performing labs, or other information that does not change or conflict with the content of the original information provided by the performing laboratory, is permitted.

- *HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Draft Standard for Trial Use, Release 2—US Realm.*

URL: *http://www.hl7.org/participate/online balloting.cfm?ref=nav#nonmember.* HL7 policy normally requires a paid membership or a ''non-member participation'' fee to access the balloting process of a standard or implementation guide. HL7 has, however, agreed to make current balloted versions of the implementation guide freely available for review during the public comment period of this proposed rule. Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The Laboratory Results Interface (LRI) Implementation Guide identifies the requirements, defines specifications and standards, and provides implementation guidance for electronic reporting of laboratory test results to ambulatory care providers in the US Realm. The scope of the Laboratory Results Interface Use Case includes requirements to enable the incorporation of clinical laboratory test results into an EHR–S as standardized structured data using the defined inter-organizational laboratory transaction. The Use Case requirements are directed at laboratory test results reporting between a LIS and an ambulatory EHR–S in different organizational entities (*e.g.,* different corporate structure, ownership or governance). Future versions of this guide may harmonize with existing guides to extend interoperability of laboratory results across care settings (*e.g.,* acute care).

- *HL7 Version 3 Implementation Guide: Family History/Pedigree Interoperability.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=301.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: The HL7 Clinical Genomics Family Health History (Pedigree) Model is a data standard for capturing, within a system, and transmitting family histories between systems. This includes describing a patient's full pedigree (family and familial relationships) with diseases and conditions, and the option to link genetic information and risk analysis. This standard allows EHR/personal health record interoperability.

- *NCPDP Formulary and Benefit Standard Implementation Guide v3.0.*

URL: *http://ncpdp.org/Standards/Standards-Info* and *http://ncpdp.org/?ReturnUrl=%2fmembers%2fStandards-Lookup.aspx.* Access requires completion of a membership application and a paid membership. NCPDP has stated that membership allows NCPDP to provide a forum wherein a diverse membership can develop business solutions, standards, and guidance for promoting information exchanges related to medications, supplies, and services within the health care system through consensus building processes. We note that CMS has already adopted the NCPDP Formulary and Benefit Standard Implementation Guide v3.0 and incorporated it by reference in the **Federal Register** as a standard for electronic prescribing under the voluntary Medicare prescription drug benefit program.[259]

Summary: The NCPDP Formulary and Benefit Standard Implementation Guide provides a standard means for pharmacy benefit payers to communicate formulary and benefit information to prescribers via technology vendor systems. It enables the physician to consider information during the prescribing process to help make an appropriate drug choice for the patient. Compared to v2.1, v3.0 removes some unused information, provides some value clarifications, adds additional RxNorm references to fields, and adds support for text messaging.

- *NCPDP Formulary and Benefit Standard Implementation Guide v4.0.*

URL: *http://ncpdp.org/Standards/Standards-Info* and *http://ncpdp.org/?ReturnUrl=%2fmembers%2fStandards-Lookup.aspx.* Access requires completion of a membership application and a paid membership. NCPDP has stated that membership allows NCPDP to provide a forum wherein a diverse membership can develop business solutions, standards, and guidance for promoting information exchanges related to medications, supplies, and services within the health care system through consensus building processes.

Summary: The NCPDP Formulary and Benefit Standard Implementation Guide provides a standard means for pharmacy benefit payers to communicate formulary and benefit information to prescribers via technology vendor systems. It enables the physician to consider information during the prescribing process to help make an appropriate drug choice for the patient. Compared to v3.0, v4.0 modifies a field size, removes some values, and makes editorial edits to a figure.

- *NCPDP Formulary and Benefit Standard Implementation Guide v4.1.*

URL: *http://ncpdp.org/Standards/Standards-Info* and *http://ncpdp.org/?ReturnUrl=%2fmembers%2fStandards-Lookup.aspx.* Access requires completion of a membership application and a paid membership. NCPDP has stated that membership allows NCPDP to provide a forum wherein a diverse membership can develop business solutions, standards, and guidance for promoting information exchanges related to medications, supplies, and services within the health care system through consensus building processes.

Summary: The NCPDP Formulary and Benefit Standard Implementation Guide provides a standard means for pharmacy benefit payers to communicate formulary and benefit information to prescribers via technology vendor systems. It enables the physician to consider information during the prescribing process to help make an appropriate drug choice for the patient. Compared to v4.0, v4.1 removes files to support electronic Prior Authorization (ePA) transactions since these were added to the NCPDP SCRIPT Standard Implementation Guide v2013011 (January 2013) and later versions, makes typographical corrections, adds a new coverage type for ePA routing, and adds an RxNorm qualifier to some data elements.

[259] 42 CFR 423.160(b)(5)(iii). *http://www.ecfr.gov/cgi-bin/text-idx?SID=776f4d6a1759e7616051 6348d3ca4454&node=se42.3.423_1160&rgn=div8.*

- *NCPDP Formulary and Benefit Standard Implementation Guide v42.*

URL: *http://ncpdp.org/Standards/Standards-Info* and *http://ncpdp.org/?ReturnUrl=%2fmembers%2fStandards-Lookup.aspx.* Access requires completion of a membership application and a paid membership. NCPDP has stated that membership allows NCPDP to provide a forum wherein a diverse membership can develop business solutions, standards, and guidance for promoting information exchanges related to medications, supplies, and services within the health care system through consensus building processes.

Summary: The NCPDP Formulary and Benefit Standard Implementation Guide provides a standard means for pharmacy benefit payers to communicate formulary and benefit information to prescribers via technology vendor systems. It enables the physician to consider information during the prescribing process to help make an appropriate drug choice for the patient. Compared to v4.1, v42 [260] includes changes to reduce the formulary file size, modifies some code lists and values, and revises some fields.

- *NCPDP Telecommunication Standard Implementation Guide vE6.*

URL: *http://ncpdp.org/Standards/Standards-Info* and *http://ncpdp.org/?ReturnUrl=%2fmembers%2fStandards-Lookup.aspx.* Access requires completion of a membership application and a paid membership. NCPDP has stated that membership allows NCPDP to provide a forum wherein a diverse membership can develop business solutions, standards, and guidance for promoting information exchanges related to medications, supplies, and services within the health care system through consensus building processes.

Summary: The Telecommunication Standard was developed to provide a standard format for the electronic submission of third party drug claims. The development of the standard was to accommodate the eligibility verification process at the point-of-sale and to provide a consistent format for electronic claims processing. The Telecommunication Standard includes transactions for eligibility verification, claim and service billing, predetermination of benefits, prior authorization, information reporting, and controlled substance (general and regulated) transaction exchanges.

- *ASC X12 270/271 Health Care Eligibility Benefit Inquiry and Response Implementation Guide.*

URL: *http://store.x12.org/store/healthcare-5010-consolidated-guides.* Access requires either a membership with ASC X12 or the user to purchase a single user or unlimited user license. ASC X12 develops and maintains EDI and CICA standards along with XML standards for a number of sectors, including health care, insurance, transportation, finance, government, and supply chain. ASC X12 has stated that membership allows it to support standards development and participation; meetings, conferences, and educational venues; standards and publications; tools for members; and networking and visibility.

Summary: The Health Care Eligibility/Benefit Inquiry and Information Response Implementation Guide describes the use of the Eligibility, Coverage or Benefit Inquiry (270) Version/Release 005010 transaction set and the Eligibility, Coverage, or Benefit Information (271) Version/Release 005010 transaction set for the following usages: Determine if an Information Source organization, such as an insurance company, has a particular subscriber or dependent on file; and determine the details of health care eligibility and/or benefit information.

- *HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=354.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: This guide supports segmenting clinical records so that protected health information (PHI) can be appropriately shared as may be permitted by privacy policies or regulations.

- *HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5.*

URL: *http://www.cdc.gov/vaccines/programs/iis/technical-guidance/downloads/hl7guide-1-5-2014-11.pdf.* This is a direct link.

Summary: This document represents the collaborative effort of the American Immunization Registry Association and CDC to improve inter-system communication of immunization records. The guide is intended to facilitate exchange of immunization records between different systems.

- *PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Ambulatory Care, and Inpatient Settings, Release 2.0.*

URL: *http://www.cdc.gov/phin/library/guides/SyndrSurvMessagGuide2_MessagingGuide_PHN.pdf.* This is a direct link.

Summary: This document represents the collaborative effort of the International Society for Disease Surveillance, CDC, and NIST to specify a national electronic messaging standard that enables disparate health care applications to submit or transmit administrative and clinical data for public health surveillance and response. The scope of the guide is to provide guidelines for sending HL7 v.2.5.1 compliant messages from emergency department, urgent and ambulatory care, and inpatient settings to public health authorities.

- *HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 2 (US Realm), Draft Standard for Trial Use R1.1.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=329.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: This guide is the result of collaborative efforts between HL7 and the S&I Laboratory Results Interface Initiative. The guide describes constraints, comments, and elements necessary for laboratory reporting to public health.

- *HL7 Implementation Guide for CDA⊃© Release 2: Reporting to Public Health Cancer Registries From Ambulatory Healthcare Providers, Release 1.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=383.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: As ambulatory health care providers adopt modern EHR systems, the opportunity to automate cancer registry reporting from ambulatory health care provider settings is also increasing and becoming more feasible. This document provides clear and concise specifications for electronic reporting form ambulatory health care provider EHR systems to public health central cancer registries using the HL7 CDA based standards. This document is designed to guide EHR vendors and public health central cancer registries in the implementation of standardized electronic reporting.

- *IHE IT Infrastructure Technical Framework Volume 2b (ITI TF–2b).*

URL: *http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7–0_Vol2b_FT_2010-08-10.pdf.* This is a direct link.

Summary: This document defines specific implementations of established

[260] Please note a change to the naming convention starting with Version 42.

standards to achieve integration goals that promote appropriate sharing of medical information to support ongoing patient care. The IHE IT Infrastructure Technical Framework identifies a subset of functional components of the health care enterprise, called ''IHE actors,'' and specified their interactions in terms of a set of coordinated, standards-based transactions. Volume 2b corresponds to transactions [ITI–29] through [ITI–57].

- *IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation.*

URL: *http://www.ihe.net/uploadedFiles/Documents/QRPH/IHE_QRPH_Suppl_SDC.pdf.* This is a direct link.

Summary: The Structured Data Capture Content Profile provides specifications to enable an EHR system or other application to retrieve a data capture form and submit data from the completed form. This supplement is based on the work of ONC's S&I Framework Structured Data Capture (SDC) Initiative. The SDC Initiative has developed use cases, identified national standards for the structure of common data elements and form model definition, developed guidance to assist in implementation, and conducted pilots for evaluation of SDC.

- *HL7 FHIR Implementation Guide: Structured Data Capture (SDC).*

URL: *http://hl7.org/implement/standards/FHIR-Develop/sdc.html#SDC.* This is a direct link.

Summary: This implementation guide is intended to support clinical systems in the creation and population of forms with patient-specific data. It defines a mechanism for linking questions in forms to pre-defined data elements to enable systems to automatically populate portions of the form based on existing data, either locally or by invoking an operation on a third-party system. Note that the SDC FHIR Implementation Guide is balloted as comment-only.

- *HL7 Implementation Guide for CDA® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm.*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=20.* Access requires a ''user account'' and a license agreement. There is no monetary cost for a user account and license agreement.

Summary: This document specifies a standard for electronic submission of health care associated infection reports (HAI) to the National Healthcare Safety Network of the CDC. This document defines the overall approach and method of electronic submission and develops constraints defining specific HAI report types.

- *HL7 Implementation Guide for CDA® Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, Draft Standard for Trial Use (December 2014).*

URL: *http://www.hl7.org/implement/standards/product_brief.cfm?product_id=385.* Consistent with HL7 policy, non-member access would not be available until April 14, 2015. HL7 has, however, agreed to waive the normal 90-day waiting period and make the implementation guide freely available during the public comment period of this proposed rule. Access requires a ''user account'' and license agreement. There is no monetary cost for a user account and license agreement.

Summary: The HL7 Implementation Guide for CDA Release 2: National Health Care Surveys (NHCS), Release 1—US Realm will provide a standardized format for implementers to submit data to fulfill requirements of the Centers for Disease Control and Prevention/National Center for Health Statistics/National Health Care Surveys. This guide will support automatic extraction of the data from a provider's EHR system or data repository. The data are collected through three surveys of ambulatory care services in the United States: The National Ambulatory Medical Care Survey with information from physicians and two national hospital care surveys: The National Hospital Ambulatory Medical Care Surveys and the National Hospital Care Survey with data from hospital emergency and outpatient departments.

- *NCPDP SCRIPT Implementation Recommendations Version 1.29.*

URL: *http://www.ncpdp.org/NCPDP/media/pdf/SCRIPTImplementationRecommendationsV1-29.pdf.* This is a direct link. The Implementation Recommendations Version 1.29 is available at no monetary cost, but references the NCPDP Structured and Codified Sig Implementation Guide Version 1.2. Access to NCPDP standards requires completion of a membership application and a paid membership. NCPDP has stated that membership allows NCPDP to provide a forum wherein a diverse membership can develop business solutions, standards, and guidance for promoting information exchanges related to medications, supplies, and services within the health care system through consensus building processes.

Summary: This Implementation Recommendations document includes recommendations for implementation of the structured and codified sig format for a subset of component composites that represent the most common Sig segments using NCPDP Structured and Codified Sig Implementation Guide Version 1.2. The recommendations promote consistent and complete prescription transactions of the NCPDP SCRIPT Standard.

Vocabulary Standards for Representing Electronic Health Information—45 CFR 170.207

- *IHTSDO SNOMED CT®, U.S. Edition, September 2014 Release.*

URL: *http://www.nlm.nih.gov/research/umls/Snomed/us_edition.html.* Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: Systemized Nomenclature of Medicine—Clinical Terms (SNOMED CT®) is a comprehensive clinical terminology, originally created by the College of American Pathologists and, as of April 2007, owned, maintained, and distributed by the International Health Terminology Standards Development Organisation. SNOMED CT® improves the recording of information in an EHR system and facilitates better communication, leading to improvements in the quality of care.

- *Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.50, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc.*

URL: *http://loinc.org/downloads.* Access requires registration, a user account, and license agreement. There is no monetary cost for registration, a user account, and license agreement.

Summary: LOINC® was initiated in 1994 by the Regenstrief Institute and developed by Regenstrief and the LOINC® committee as a response to the demand for electronic movement of clinical data from laboratories that produce the data to hospitals, provider's offices, and payers who use the data for clinical care and management purposes. The scope of the LOINC® effort includes laboratory and other clinical observations. The LOINC® database facilitates the exchange and pooling of results for clinical care, outcomes management, and research.

- *RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, February 2, 2015 Release.*

URL: *http://www.nlm.nih.gov/research/umls/rxnorm/docs/rxnormfiles.html.* Access requires a user account and license agreement. There is no monetary cost for a user account and license agreement.

Summary: RxNorm provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software. By providing links between vocabularies commonly used in pharmacy management and drug interaction software, RxNorm can mediate messages between systems not using the same software and vocabulary. RxNorm now includes the National Drug File—Reference Terminology (NDF–RT) from the Veterans Health Administration, which is used to code clinical drug properties, including mechanism of action, physiologic effect, and therapeutic category.

- *HL7 Standard Code Set CVX—Vaccines Administered, updates through February 2, 2015.*

URL: *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=cvx.* This is a direct link.

Summary: CDC's National Center of Immunization and Respiratory Diseases developed and maintains HL7 Table 0292, Vaccine Administered (CVX). CVX includes both active and inactive vaccines available in the U.S. CVX codes for inactive vaccines allow transmission of historical immunization records; when paired with a manufacturer (MVX) code, the specific trade named vaccine may be indicated.

- *National Drug Code Directory—Vaccine Codes, updates through January 15, 2015.*

URL: *http://www2a.cdc.gov/vaccines/iis/iisstandards/ndc_tableaccess.asp.* This is a direct access link.

Summary: The Drug Listing Act of 1972 requires registered drug establishments to provide the FDA with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it by commercial distribution. Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which services as the universal product identifier for drugs. This standard is limited to the NDC vaccine codes identified by CDC at the URL provided.

- *HL7 Standard Code Set MVX—Manufacturers of Vaccines Code Set, updates through October 30, 2014.*

URL: *http://www2a.cdc.gov/vaccines/iis/iisstandards/vaccines.asp?rpt=mvx.* This is a direct link.

Summary: CDC's National Center of Immunization and Respiratory Diseases developed and maintains HL7 Table 0227, Manufacturers of Vaccines (MVX). The MVX table includes both active and inactive vaccines available in the U.S. MVX codes allow transmission of historical immunization records. When MVX code is paired with a CVX code, the specific trade named vaccine may be indicated.

- *''Race & Ethnicity—CDC'' code system in the PHIN Vocabulary Access and Distribution System (VADS), Release 3.3.9.*

URL: *https://phinvads.cdc.gov/vads/ViewCodeSystem.action?id=2.16.840.1.113883.6.238.* This is a direct link.

Summary: The Public Health Information Network (PHIN) VADS is a web-based enterprise vocabulary systems for accessing, searching, and distributing vocabularies used within the PHIN. PHIN VADS provides standard vocabularies to CDC and its public health partners in one place. It promotes the use of standards-based vocabulary to support the exchange of consistent information among public health partners.

- *Request for Comments (RFC) 5646.*

URL: *http://www.rfc-editor.org/info/rfc5646.* This is a direct access link.

Summary: RFC 5646 describes the structure, content, construction, and semantics of language tags for use in cases where it is desirable to indicate the language used in an information object. It also describes how to register values for use in language tags and the creation of user-defined extensions for private interchange.

- The Unified Code of Units of Measure, Revision 1.9.

URL: *http://unitsofmeasure.org/trac/.* This is a direct access link. The codes can be viewed in html or xml.

Summary: The Unified Code of Units of Measure is a code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with units.

Standards for Health Information Technology To Protect Electronic Health Information Created, Maintained, and Exchanged—45 CFR 170.210

- *Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2, October 8, 2014.*

URL: *http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.* This is a direct link.

Summary: Federal Information Processing Standards Publication (FIPS PUB) 140–2, *Security Requirements for Cryptographic Modules,* specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems. The standard provides four increasing qualitative levels of security that are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

VII. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995 (PRA), agencies are required to provide 60-day notice in the **Federal Register** and solicit public comment on a proposed collection of information before it is submitted to the Office of Management and Budget for review and approval. In order to fairly evaluate whether an information collection should be approved by the Office of Management and Budget, section 3506(c)(2)(A) of the PRA requires that we solicit comment on the following issues:

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency;
2. The accuracy of the agency's estimate of the information collection burden;
3. The quality, utility, and clarity of the information to be collected; and
4. Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

Under the PRA, the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section are to be considered. We explicitly seek, and will consider, public comment on our assumptions as they relate to the PRA requirements summarized in this section. To comment on the collection of information or to obtain copies of the supporting statements and any related forms for the proposed paperwork collections referenced in this section, email your comment or request, including your address and phone number to *Sherette.funncoleman@hhs.gov,* or call the Reports Clearance Office at (202) 690–6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above email address within 60 days.

Abstract

Under the ONC Health IT Certification Program, accreditation organizations that wish to become the ONC-Approved Accreditor (ONC–AA) must submit certain information, organizations that wish to become an

ONC–ACB must submit the information specified by the application requirements, and ONC–ACBs must comply with collection and reporting requirements, records retention requirements, and submit annual surveillance plans and annually report surveillance results.

In the Permanent Certification Program final rule (76 FR 1312–14), we solicited public comment on each of the information collections associated with the requirements described above (and included in regulation at 45 CFR 170.503(b), 170.520, and 170.523(f), (g), and (i), respectively). In the 2014 Edition final rule (77 FR 54275–76), we sought comment on these collection requirements again and finalized an additional requirement at § 170.523(f)(8) for ONC–ACBs to report to ONC a hyperlink with each EHR technology they certify that provides the public with the ability to access the test results used to certify the EHR technology. These collections of information were approved under OMB control number 0955–0013 (previous OMB control number 0990–0378).

As discussed in more detail below, we estimate less than 10 annual respondents for all of the regulatory ''collection of information'' requirements under Part 170 of Title 45, including those previously approved by OMB and proposed in this proposed rule. Accordingly, the regulatory ''collection of information'' requirements under the ONC Health IT Certification Program described in this section are not subject to the PRA under 5 CFR 1320.3(c). We welcome comments on this conclusion and our supporting rationale for this conclusion as recited below. We also set out below proposed revisions to previously approved ''collections of information'' and potential new ''collections of information'' as well as our burden estimates for these ''collections of information.''

We propose to change the records retention requirement in § 170.523(g) from five years to six years. It is our understanding that a six-year records retention requirement aligns with current accreditation standards that ONC–ACBs follow. Therefore, we do not believe there will be any additional burden based on this proposed change.

We propose in § 170.523(o) that ONC–ACBs provide ONC with a list of complaints received on a quarterly basis. We only request that ONC–ACBs indicate in their submission how many complaints were received, the nature or substance of the complaint, and the type of complainant (*e.g.,* type of provider, health IT developer, etc.). Therefore, we believe ONC–ACBs will face little burden in complying with this new proposed requirement.

For regulatory clarity in relation to new proposed ONC–ACB collection and reporting requirements, we have proposed to move all of the current ONC–ACB collection and reporting requirements in § 170.523(f) to § 170.523(f)(2). These collection and reporting requirements are specific to the certification of health IT to the 2014 Edition. We note that we have also proposed to add a data element to the list of collection and reporting requirements for 2014 Edition certifications. The data element is the reporting of any corrective action instituted under the proposed provisions of § 170.556 (see section IV.D.3 of this preamble; see also § 170.523(f)(2)(ix)).

We propose to add a new ONC–ACB collection and reporting requirements for the certification of health IT to the 2015 Edition (and any subsequent edition certification) in § 170.523(f)(1). As proposed for § 170.523(f)(1), ONC–ACBs would be required to report on the same data elements they report to ONC under current § 170.523(f), the information contained in the publicly available test report, and additional data in an open data file format. These collection and reporting requirements are described in more detail in section IV.D.3, titled ''Open Data Certified Health IT Product List (CHPL).'' We do not anticipate any additional burden on ONC–ACBs for reporting similar information for 2015 Edition certifications as they do for 2014 Edition certifications. For the additional data that we propose they report, we believe that burden would be minimal as discussed below.

For the purposes of estimating the additional potential burden for reporting under § 170.523(f)(1) and (2):

- We assume there will be three ONC–ACBs as this is the current number of ONC–ACBs.
- We assume ONC–ACBs will continue to report weekly (*i.e.,* respondents will respond 52 times per year) as is the current practice.
- We assume an equal distribution among ONC–ACBs in certifying Health IT Modules on a weekly basis. As such, based on the number of Complete EHRs and EHR Modules listed on the CHPL at the end of July of 2014 (approximately one and a half years since ONC began certifying 2014 Edition products), we estimate that, on average, each ONC–ACB will report information to ONC on 2015 Edition certifications for 2.5 Health IT Modules per week.
- We expect 2014 Edition certifications to slow upon issuance of a subsequent final rule and estimate that each ONC–ACB will only issue, on average, one 2014 Edition certification per week after a subsequent final rule is effective. Therefore, we have reduced the average burden hours per response to .75 from 1.33 for § 170.523(f)(2). This new average burden hour estimate takes into account any potential ONC–ACB reporting of data associated with the new proposed provisions for corrective action instituted under § 170.556 (see § 170.523(f)(2)(ix)).
- We believe it will take approximately 1.5 hours per week on average to collect and report to ONC the information required for 2015 Edition certifications in § 170.523(f)(1), including the information that goes beyond what is currently collected and reported for 2014 Edition certifications. Our estimate includes a potential wide range of certifications issued for Health IT Modules, including, but not limited to, certifying Health IT Modules to multiple certification criteria and CQMs. Our estimates also take into account that it may take ONC–ACBs more time in the beginning of the collection and reporting processes as they may need to recode their systems to collect and report the new information in an automated manner. Therefore, we believe 1.5 hours represents a reasonable average of the amount of time for an ONC–ACB to collect and report the information proposed under § 170.523(f)(1). Our burden estimate is incorporated into the table below.

As stated above, we anticipate that there will be three ONC–ACBs participating in the ONC Health IT Certification Program as this is the current number of ONC–ACBs. Further, since the establishment of the ONC Health IT Certification Program in 2010, ONC has never had more than six applicants for ONC–ACB or ONC–ATCB status or selected more than six ONC–ACBs or ONC–ATCBs.[261] Therefore, we have aligned the estimated number of respondents for the applicable regulation provisions (*i.e.,* § 170.523(f)(1) and (2), (g), (i), and (o); and § 170.540(c)) with the current number of ONC–ACBs. We have also revised the estimated number of respondents for § 170.503(b) (applicants for ONC-Approved Accreditor (ONC–AA) status) based on past selection processes for the ONC–AA, which have

[261] See also: *http://www.healthit.gov/policy-researchers-implementers/authorized-testing-and-certifications-bodies* and *http://www.healthit.gov/policy-researchers-implementers/certification-bodies-testing-laboratories.*

included no more than two applicants. We have retained the same number of responses per respondent and average burden hours per response for the regulation provisions currently included in OMB control number 0995–0013, except for § 170.523(f) as specified above (now § 170.523(f)(2)). Our estimates for the total burden hours are expressed in the table below.

ESTIMATED ANNUALIZED TOTAL BURDEN HOURS

Type of respondent	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
45 CFR 170.503(b)	2	1	1	2
45 CFR 170.520	1	1	1	1
45 CFR 170.523(f)(1)	3	52	1.5	234
45 CFR 170.523(f)(2)	3	52	.75	117
45 CFR 170.523(g)	3	n/a	n/a	n/a
45 CFR 170.523(i)	3	2	1	6
45 CFR 170.523(o)	3	4	1	12
45 CFR 170.540(c)	3	1	1	3
Total burden hours				375

VIII. Regulatory Impact Statement

A. Statement of Need

This proposed rule is being published to adopt the 2015 Edition. Certification criteria and associated standards and implementation specifications would be used to test and certify health IT in order to make it possible for EPs, eligible hospitals, and CAHs to adopt and implement health IT that can be used to meet the CEHRT definition. EPs, eligible hospitals, and CAHs who participate in the EHR Incentive Programs are required by statute to use CEHRT.[262]

The certification criteria and associated standards and implementation specifications would also support the certification of more types of health IT and health IT that supports care and practice settings beyond the scope of the EHR Incentive Programs.

The adoption and implementation of health IT certified to the 2015 Edition promotes interoperability in support of a nationwide health information infrastructure and improves health care quality, safety and efficiency consistent with the goals of the HITECH Act.

B. Overall Impact

We have examined the impact of this proposed rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993), Executive Order 13563 on Improving Regulation and Regulatory Review (February 2, 2011), the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), and Executive Order 13132 on Federalism (August 4, 1999).

1. Executive Orders 12866 and 13563—Regulatory Planning and Review Analysis

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any 1 year). OMB has determined that this proposed rule is an economically significant rule as ONC has estimated the costs to develop and prepare health IT to be tested and certified may be greater than $100 million per year. Because of the public interest in this proposed rule, we have prepared an RIA that to the best of our ability presents the costs and benefits of the proposed rule.

a. Costs

This proposed rule proposes the adoption of standards, implementation specifications, and certification criteria that would establish the capabilities that health IT would need to demonstrate to be certified to the 2015 Edition. Our analysis focuses on the direct effects of the provisions of this proposed rule—the costs incurred by health IT developers to develop and prepare health IT to be tested and certified in accordance with the certification criteria (and the standards and implementation specifications they include) adopted by the Secretary. That is, we focus on the technological development and preparation costs necessary for health IT *already certified to the 2014 Edition* to upgrade to the proposed 2015 Edition and for, in limited cases, developing and preparing a new Health IT Module to meet the 2015 Edition. The costs for the testing and certification of health IT to the 2015 Edition were captured in the regulatory impact analysis of the Permanent Certification Program final rule as we discuss in more detail below (VIII.B.1.a.iii ‘‘Testing and Certification Costs for the 2015 Edition’’). Because the costs that EPs, eligible hospitals, and CAHs would incur in adopting and implementing (including training, maintenance, and any other ongoing costs) health IT certified to the 2015 Edition is overwhelmingly attributable to CMS's EHR Incentive Programs Stage 3 proposed rule (proposed elsewhere in this issue of the **Federal Register**), and would not be incurred in the absence of such rulemaking, such costs are not within the scope of the analysis of this proposed rule; similarly, any benefits that are contingent upon adoption and implementation would be attributable to CMS's rulemaking.[263] We also note that this proposed rule does not impose the costs cited as compliance costs, but rather as investments which health IT

[262] Section 1848(o) of the Social Security Act.

[263] ONC administers a voluntary certification program that provides no incentives for certification. Therefore, to the extent that providers' implementation and adoption costs are attributable to CMS's rulemaking, health IT developers' preparation and development costs would also be attributable to that rulemaking (because all of the costly activities are, directly or indirectly, incentivized by CMS's proposed payment structure). However, even if CMS's proposed rule were not finalized, a professional organization or other such entity could require or promote certification, thus generating costs and benefits that are attributable to this proposed rule. To avoid giving the misleading impression that such effects equal zero, we present in this RIA a subset of the relevant impacts—a quantification of costs that are incurred by health IT developers and a qualitative discussion of benefits. (The missing portion of the subset is providers' implementation and adoption costs.)

developers voluntarily take on and expect to recover with an appropriate rate of return.

i. Development and Preparation Costs for the 2015 Edition

The development and preparation costs we estimate are derived through a health IT developer per criterion cost. In simple terms, we estimate: (1) How many health developers will prepare and develop products against the proposed certification criteria; (2) how many products they will develop; and (3) what it will likely cost them to develop and prepare those products to meet the proposed certification criteria.

We are not aware of an available *independent* study (*e.g.,* a study capturing the preparation efforts and costs to develop and Health IT Modules to meet the requirements of the 2014 Edition) that we could rely upon as a basis for estimating the efforts and costs required to develop and prepare health IT to meet the 2015 Edition. We welcome comments identifying such a study or on any valid and reliable data upon which we could base our estimates in a subsequent final rule.

Proposed Certification Criteria

We have divided the proposed certification criteria into two tables. One table is for the certification criteria associated with EHR Incentive Programs Stage 3 proposed objectives and measures (''Stage 3 Criteria''). This table also includes certification criteria that are included in conditional certification requirements, such as privacy and security, safety-enhanced design, and quality management system certification criteria as certified Health IT Modules certified to these criteria would likely be used to meet the CEHRT definition under the EHR Incentive Programs. The second table is for all other proposed certification criteria (''Independent Criteria''). We have done this because, based on available data, we can more accurately estimate the number of health IT developers that may develop and prepare Health IT Modules for certification to proposed certification criteria associated with the EHR Incentive Programs.

Health IT Developers

We derive our estimates for the number of health IT developers by beginning with the number of Health IT developers certified to each of the 2014 Edition certification criteria as identified in CHPL data from November 10, 2014. For the Stage 3 Criteria that correspond to 2014 Edition certification criteria, we have reduced the number of Health IT developers by 30% from the number that certified against the 2014 Edition. We have done this because we have found a 22% drop in the number of health IT developers that certified technology against the 2014 Edition versus the 2011 Edition. We believe that as both interoperability requirements increase by edition and certain health IT developers gain more market share through competition and acquisition of other health IT developers, there will be an even greater drop in the number of health IT developers that seek certification to the 2015 Edition. We welcome comments on this assumption.

For the Independent Criteria, we have established a number of health IT developers for all the criteria at 16. We derived this number by taking the lowest number of health IT developers certified to a 2014 Edition certification criteria and reducing that number by 50%. Only 32 health IT developers have certified to the 2014 Edition ''transmission to cancer registries'' certification criterion (§ 170.314(f)(6)) even though it is associated with an EHR Incentive Programs Stage 2 menu objective. The Independent Criteria are not currently associated with the EHR Incentive Programs or other HHS payment programs. Therefore, we estimate that a small number of health IT developers would certify to these criteria (*i.e.,* 50% less than the least amount of health IT developers certified to a certification criterion that supports the EHR Incentive Programs). We welcome comments on our approach to estimating the number of health IT developers for Independent Criteria. We also seek comment on reasons (*e.g.,* use cases) why health IT developers would currently seek certification to these criteria in general or for each proposed criteria.

To note, the estimated number of Health IT developers for each criterion includes any potential new entrants to the market.

Number of Health IT Modules

We estimate 2.5 products per health IT developer for each Stage 3 criterion. We reached this estimate based both on the number of unique[264] certified products listed on the CHPL as of November 10, 2014 divided by the number of health IT developers certified and stakeholder feedback on our Voluntary Edition proposed rule (79 FR 54474). We estimate 1 product for each of the Independent Criteria (60% less). As noted above, the Independent Criteria are not currently associated with the EHR Incentive Programs or other HHS payment programs. Therefore, it is not only unclear how many health IT developers will seek certification to these criteria, but also how many products they would certify to these criteria. We can only assume that the number of products certified by each health IT developer will likely be less than for Stage 3 Criteria. Again, we welcome comments on estimates.

Average Development and Preparation Hours

Our estimated average development hours are based on feedback we received in response to the RIA we completed for on our Voluntary Edition proposed rule and internal estimates for criteria where there is no external data to validly rely upon. As noted in the Voluntary Edition final rule, we have generally used estimates from the Electronic Health Record Association as a basis for our high estimates, where applicable. For the Stage 3 Criteria, we include the development and preparation for 2.5 certified products per health IT developer in the estimated average development and preparation hours. For the Independent Criteria, we have built in an estimate of 60% less overall development and preparation hours due to our assumption that a health IT developer would develop only one product.

As mentioned above, for proposed 2015 Edition certification criteria that have a corresponding 2014 Edition criterion, we estimate only the development and preparation hours to meet the new and revised capabilities included in a proposed criterion.

Health IT Developer Hourly Cost and Cost Range

We have based the effort levels on the hours necessary for a software developer to develop and prepare the health IT for testing and certification. The U.S. Department of Labor, Bureau of Labor Statistics estimates that the median hourly wage for a software developer is $44.55.[265] We have also calculated the costs of an employee's benefits by assuming that an employer expends thirty-six percent (36%) of an employee's hourly wage on benefits for the employee. We have concluded that a 36% expenditure on benefits is an appropriate estimate because it is the routine percentage used by HHS for contract cost estimates. We have rounded up the average software

[264] We attempted to discern how many Complete EHRs and Health IT Modules were used that would not constitute a newer version of the same technology.

[265] *http://www.bls.gov/oes/current/oes151132.htm.*

developer's wage with benefits to $61 per hour.

To calculate our cost estimates for each certification criterion in the tables below, we have multiplied both the average low and average high number of development and preparation hours by $61. For tables 8 and 9, dollar amounts are expressed in 2013 dollars.

For unchanged certification criteria,[266] we have estimated a range of 0–50 hours to account for new entrants in the Stage 3 Criteria table (Table 6) and used 60% less of that estimate in the ''Independent Criteria'' table (Table 7). To illustrate, that would produce a high development hours of 12,700 for the ''medication list'' criterion (item # 7). This likely still overestimates the burden hours of all potential new entrants.

Estimated Health IT Developers and Development Hours Per Criterion

TABLE 6—ESTIMATED HEALTH IT DEVELOPERS AND DEVELOPMENT AND PREPARATION HOURS FOR PROPOSED CERTIFICATION CRITERIA—CRITERIA ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3

[Stage 3 Criteria]

Item No.	CFR text	Certification criterion name	Number of health IT developers who develop product(s) for certification to criterion	Hourly development effort by health IT developer	
				Low Avg	High Avg
1	§ 170.315(a)(1)	CPOE—medications	83.3	0	50
2	§ 170.315(a)(2)	CPOE—laboratory	83.3	1,000	2,000
3	§ 170.315(a)(3)	CPOE—diagnostic imaging	83.3	0	50
4	§ 170.315(a)(4)	DD/DAI Checks for CPOE	242.2	400	800
5	§ 170.315(a)(5)	Demographics	268.8	500	1,000
6	§ 170.315(a)(7)	Problem List	256.9	100	200
7	§ 170.315(a)(8)	Medication List	254.8	0	50
8	§ 170.315(a)(9)	Medication Allergy List	252.7	0	50
9	§ 170.315(a)(10)	Clinical Decision Support	235.2	600	1,200
10	§ 170.315(a)(11)	Drug-formulary and Preferred Drug List Checks.	233.1	310	620
11	§ 170.315(a)(12)	Smoking Status	266.7	100	200
12	§ 170.315(a)(14)	Family Health History	216	100	200
13	§ 170.315(a)(15)	Family Health History—pedigree	24	500	1,200
14	§ 170.315(a)(17)	Patient-specific Education Resources	249.2	600	1,200
15	§ 170.315(a)(19)	Patient Health Information Capture	88.9	500	1,000
16	§ 170.315(a)(20)	Implantable Device List	90	1,100	1,700
17	§ 170.315(b)(1)	Transitions of Care	242.9	1,550	3,100
18	§ 170.315(b)(2)	Clinical Information Reconciliation and Incorporation.	224	600	1,200
19	§ 170.315(b)(3)	Electronic Prescribing	224.7	1,050	2,100
20	§ 170.315(b)(6)	Data Portability	228.9	800	1,600
21	§ 170.315(c)(1)	CQMs—record and export	246.4	200	500
22	§ 170.315(d)(1)	Authentication, Access Control, Authorization.	333.9	0	50
23	§ 170.315(d)(2)	Auditable Events and Tamper-resistance	272.3	0	50
24	§ 170.315(d)(3)	Audit Report(s)	280	0	50
25	§ 170.315(d)(4)	Amendments	243.6	0	50
26	§ 170.315(d)(5)	Automatic Access Time-out	333.9	0	50
27	§ 170.315(d)(6)	Emergency Access	308.7	0	50
28	§ 170.315(d)(7)	End-User Device Encryption	267.4	0	50
29	§ 170.315(d)(8)	Integrity	312.2	0	50
30	§ 170.315(e)(1)	View, Download, and Transmit to 3rd party	256.2	1,000	2,000
31	§ 170.315(e)(2)	Secure Messaging	246.4	0	50
32	§ 170.315(f)(1)	Transmission to Immunization Registries	220.5	680	1,360
33	§ 170.315(f)(2)	Transmission to Public Health Agencies—syndromic surveillance.	213.5	480	960
34	§ 170.315(f)(3)	Transmission to Public Health Agencies—reportable laboratory tests and values/results.	49	520	1,040
35	§ 170.315(f)(4)	Transmission to Cancer Registries	22.4	500	1,000
36	§ 170.315(f)(5)	Transmission to Public Health Agencies—case reporting.	21	500	1,000
37	§ 170.315(f)(6)	Transmission to Public Health Agencies—antimicrobial use and resistance reporting.	21	500	1,000
38	§ 170.315(f)(7)	Transmission to Public Health Agencies—health care surveys.	21	500	1,000
39	§ 170.315(g)(1)	Automated Numerator Recording	113.4	400	800
40	§ 170.315(g)(2)	Automated Measure Calculation	264.6	600	1,200
41	§ 170.315(g)(3)	Safety-enhanced Design	266	300	600

[266] For the purposes of estimating development hours, we are currently characterizing the 2015 Edition ''automatic access time-out'' (§ 170.315(d)(5)) and ''end-user device encryption'' certification criterion (§ 170.315(d)(7)) as unchanged despite clarifying edits to the criteria and updates.

TABLE 6—ESTIMATED HEALTH IT DEVELOPERS AND DEVELOPMENT AND PREPARATION HOURS FOR PROPOSED CERTIFICATION CRITERIA—CRITERIA ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3—Continued

[Stage 3 Criteria]

Item No.	CFR text	Certification criterion name	Number of health IT developers who develop product(s) for certification to criterion	Hourly development effort by health IT developer	
				Low Avg	High Avg
42	§ 170.315(g)(4)	Quality Management System	401.8	400	800
43	§ 170.315(g)(6)	Consolidated CDA Creation Performance	242	400	1,000
44	§ 170.315(g)(7)	Application Access to Common Clinical Data Set.	242	500	1,000
45	§ 170.315(g)(8)	Accessibility-Centered Design	401.8	50	100
46	§ 170.315(h)(1)	Direct Project	140	0	50
47	§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM.	70	0	50

TABLE 7—ESTIMATED HEALTH IT DEVELOPERS AND DEVELOPMENT AND PREPARATION HOURS FOR PROPOSED CERTIFICATION CRITERIA—CRITERIA NOT ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3

[''Independent Criteria'']

Item No.	CFR text	Certification criterion name	Number of health IT developers who develop product(s) for certification to criterion	Hourly development effort by health IT developer	
				Low Avg	High Avg
1	§ 170.315(a)(6)	Vital Signs, BMI, and Growth Charts	16	614	922
2	§ 170.315(a)(13)	Image Results	16	0	20
3	§ 170.315(a)(16)	Patient List Creation	16	0	20
4	§ 170.315(a)(18)	Electronic Medication Administration Record	16	0	20
5	§ 170.315(a)(21)	Social, Psychological, and Behavioral Data	16	235	470
6	§ 170.315(a)(22)	Decision Support—knowledge artifact	16	394	788
7	§ 170.315(a)(23)	Decision Support—service	16	229	458
8	§ 170.315(b)(4)	Incorporate Laboratory Tests and Values/Results	16	313	626
9	§ 170.315(b)(5)	Transmission of Laboratory Test Reports	16	360	720
10	§ 170.315(b)(7)	Data Segmentation for Privacy—send	16	450	900
11	§ 170.315(b)(8)	Data Segmentation for Privacy—receive	16	450	900
12	§ 170.315(b)(9)	Care Plan	16	300	500
13	§ 170.315(c)(2)	CQMs—import and calculate	16	0	200
14	§ 170.315(c)(4)	CQMs—filter	16	316	632
15	§ 170.315(d)(9)	Accounting of Disclosures	16	0	20
16	§ 170.315(g)(5)	Accessibility Technology Compatibility	16	800	1,400
17	§ 170.315(h)(3)	SOAP Transport and Security Specification and XDR/XDR for Direct Messaging.	16	0	20
18	§ 170.315(h)(4)	Healthcare Provider Directory—query request	16	120	240
19	§ 170.315(h)(5)	Healthcare Provider Directory—query response	16	120	240
20	§ 170.315(i)(1)	Electronic Submission of Medical Documentation	16	1,000	2,000

Estimated Cost Per Criterion for Health IT Developers

TABLE 8—TOTAL DEVELOPMENT AND PREPARATION COSTS PER CRITERION FOR HEALTH IT DEVELOPERS—CRITERIA ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3

[''Stage 3 Criteria'']

Item No.	CFR text	Certification criterion name	Average cost estimates ($)	
			Average low ($)	Average high ($)
1	§ 170.315(a)(1)	CPOE—medications	0	254,065
2	§ 170.315(a)(2)	CPOE—laboratory	508,1300	1,0162,600
3	§ 170.315(a)(3)	CPOE—diagnostic imaging	0	254,065
4	§ 170.315(a)(4)	DD/DAI Checks for CPOE	5,909,680	11,819,360
5	§ 170.315(a)(5)	Demographics	8,198,400	16,396,800

TABLE 8—TOTAL DEVELOPMENT AND PREPARATION COSTS PER CRITERION FOR HEALTH IT DEVELOPERS—CRITERIA ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3—Continued

[“Stage 3 Criteria”]

Item No.	CFR text	Certification criterion name	Average cost estimates ($)	
			Average low ($)	Average high ($)
6	§ 170.315(a)(7)	Problem List	1,567,090	3,134,180
7	§ 170.315(a)(8)	Medication List	0	777,140
8	§ 170.315(a)(9)	Medication Allergy List	0	770,735
9	§ 170.315(a)(10)	Clinical Decision Support	8,608,320	17,216,640
10	§ 170.315(a)(11)	Drug-formulary and Preferred Drug List Checks	4,407,921	8,815,842
11	§ 170.315(a)(12)	Smoking Status	1,626,870	3,253,740
12	§ 170.315(a)(14)	Family Health History	1,317,600	2,635,200
13	§ 170.315(a)(15)	Family Health History—pedigree	732,000	1,756,800
14	§ 170.315(a)(17)	Patient-specific Education Resources	9,120,720	18,241,440
15	§ 170.315(a)(19)	Patient Health Information Capture	2,711,450	5,422,900
16	§ 170.315(a)(20)	Implantable Device List	6,039,000	9,333,000
17	§ 170.315(b)(1)	Transitions of Care	22,966,195	45,932,390
18	§ 170.315(b)(2)	Clinical Information Reconciliation and Incorporation	8,198,400	16,396,800
19	§ 170.315(b)(3)	Electronic Prescribing	14,392,035	28,784,070
20	§ 170.315(b)(6)	Data Portability	1,117,0320	22,340,640
21	§ 170.315(c)(1)	CQMs—record and export	3,006,080	7,515,200
22	§ 170.315(d)(1)	Authentication, Access Control, Authorization	0	1,018,395
23	§ 170.315(d)(2)	Auditable Events and Tamper-resistance	0	830,515
24	§ 170.315(d)(3)	Audit Report(s)	0	854,000
25	§ 170.315(d)(4)	Amendments	0	742,980
26	§ 170.315(d)(5)	Automatic Access Time-out	0	1,018,395
27	§ 170.315(d)(6)	Emergency Access	0	941,535
28	§ 170.315(d)(7)	End-User Device Encryption	0	815,570
29	§ 170.315(d)(8)	Integrity	0	952,210
30	§ 170.315(e)(1)	View, Download, and Transmit to 3rd party	15,628,200	31,256,400
31	§ 170.315(e)(2)	Secure Messaging	0	751,520
32	§ 170.315(f)(1)	Transmission to Immunization Registries	9,146,340	18,292,680
33	§ 170.315(f)(2)	Transmission to Public Health Agencies—syndromic surveillance.	6,251,280	12,502,560
34	§ 170.315(f)(3)	Transmission to Public Health Agencies—reportable laboratory tests and values/results.	1,554,280	3,108,560
35	§ 170.315(f)(4)	Transmission to Cancer Registries	683,200	1,366,400
36	§ 170.315(f)(5)	Transmission to Public Health Agencies—case reporting	640,500	1,281,000
37	§ 170.315(f)(6)	Transmission to Public Health Agencies—antimicrobial use and resistance reporting.	640,500	1,281,000
38	§ 170.315(f)(7)	Transmission to Public Health Agencies—health care surveys	640,500	1,281,000
39	§ 170.315(g)(1)	Automated Numerator Recording	2,766,960	5,533,920
40	§ 170.315(g)(2)	Automated Measure Calculation	9,684,360	19,368,720
41	§ 170.315(g)(3)	Safety-enhanced Design	4867800	9,735,600
42	§ 170.315(g)(4)	Quality Management System	9,803,920	19,607,840
43	§ 170.315(g)(6)	Consolidated CDA Creation Performance	5,904,800	14,762,000
44	§ 170.315(g)(7)	Application Access to Common Clinical Data Set	7,381,000	14,762,000
45	§ 170.315(g)(8)	Accessibility-Centered Design	1,225,490	2,450,980
46	§ 170.315(h)(1)	Direct Project	0	427,000
47	§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM	0	213,500

TABLE 9—TOTAL DEVELOPMENT AND PREPARATION COSTS PER CRITERION FOR HEALTH IT DEVELOPERS—CRITERIA NOT ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3

[“Stage 3 Criteria”]

Item No.	CFR text	Certification criterion name	Average cost estimates ($)	
			Average low ($)	Average high ($)
1	§ 170.315(a)(6)	Vital Signs, BMI, and Growth Charts	599,264	899,872
2	§ 170.315(a)(13)	Image Results	0	19,520
3	§ 170.315(a)(16)	Patient List Creation	0	19,520
4	§ 170.315(a)(18)	Electronic Medication Administration Record	0	19,520
5	§ 170.315(a)(21)	Social, Psychological, and Behavioral Data	229,360	458,720
6	§ 170.315(a)(22)	Decision Support—knowledge artifact	384,544	769,088
7	§ 170.315(a)(23)	Decision Support—service	223,504	447,008
8	§ 170.315(b)(4)	Incorporate Laboratory Tests and Values/Results	305,488	610,976
9	§ 170.315(b)(5)	Transmission of Laboratory Test Reports	351,360	702,720

TABLE 9—TOTAL DEVELOPMENT AND PREPARATION COSTS PER CRITERION FOR HEALTH IT DEVELOPERS—CRITERIA NOT ASSOCIATED WITH THE EHR INCENTIVE PROGRAMS STAGE 3—Continued

[“Stage 3 Criteria”]

Item No.	CFR text	Certification criterion name	Average cost estimates ($)	
			Average low ($)	Average high ($)
10	§ 170.315(b)(7)	Data Segmentation for Privacy—send	439,200	878,400
11	§ 170.315(b)(8)	Data Segmentation for Privacy—receive	439,200	878,400
12	§ 170.315(b)(9)	Care Plan	292,800	488000
13	§ 170.315(c)(2)	CQMs—import and calculate	0	195,200
14	§ 170.315(c)(4)	CQMs—filter	308,416	616,832
15	§ 170.315(d)(9)	Accounting of Disclosures	0	19,520
16	§ 170.315(g)(5)	Accessibility Technology Compatibility	780,800	1,366,400
17	§ 170.315(h)(3)	SOAP Transport and Security Specification and XDR/XDR for Direct Messaging.	0	19,520
18	§ 170.315(h)(4)	Healthcare Provider Directory—query request	117,120	234,240
19	§ 170.315(h)(5)	Healthcare Provider Directory—query response	117,120	234,240
20	§ 170.315(i)(1)	Electronic Submission of Medical Documentation	976,000	1,952,000

ii. Overall Development and Preparation Costs Over a Four-Year Period

We estimate the development and preparation costs over a four-year period because a four-year period aligns with our estimated publication date for a subsequent final rule (Summer 2015) and the year in which CMS proposes that participants in the EHR Incentive Programs *must* use health IT certified to the 2015 Edition (2018) (see the EHR Incentive Programs Stage 3 proposed rule published elsewhere in this issue of the **Federal Register**).

In total, we estimate the overall costs to develop and prepare health IT for certification over a four-year period to be $197.43 million to $407.20 million, with a cost mid-point of approximately $302.32 million. Evenly distributed over calendar years 2015 through 2018, the cost range would be $49.36 million to $101.80 per year with an annual cost mid-point of approximately $75.58. However, we project these costs to be unevenly distributed. We estimate the distribution as follows: 2015 (25%); 2016 (30%); 2017 (30%); and 2018 (15%). We reached this distribution based on these assumptions and information:

- We expect a subsequent 2015 Edition final rule to be published in the summer of 2015 and for health IT developers to spend the rest of the year preparing and developing their health IT to meet the 2015 Edition.
- We expect health IT developers to aggressively work in 2016 and 2017 to prepare and develop their health IT to meet the 2015 Edition as the compliance date for the EHR Incentive Programs CEHRT definition draws near (*i.e.,* 2018) and because health IT certified to the 2015 Edition *could* be used in 2017 under the EHR Incentive Programs Stage 3 proposal for the CEHRT definition.
- We expect health IT developers to continue to prepare and develop health IT to the 2015 Edition in 2018 based on their approach to the 2014 Edition.

Table 10 below represents the costs attributable to this proposed rule distributed as discussed above. The dollar amounts expressed in Table 10 are expressed in 2013 dollars.

TABLE 10—DISTRIBUTED TOTAL DEVELOPMENT AND PREPARATION COSTS FOR HEALTH IT DEVELOPERS (4-YEAR PERIOD)—TOTALS ROUNDED

Year	Ratio (%)	Total low cost estimate ($M)	Total high cost estimate ($M)	Total average cost estimate ($M)
2015	25	49.36	101.80	75.58
2016	30	59.23	122.16	90.70
2017	30	59.23	122.16	90.70
2018	15	29.61	61.08	45.35
4-Year Totals		197.43	407.20	302.32

iii. Testing and Certification Costs for the 2015 Edition

In the RIA of the Permanent Certification Program final rule, we estimated the costs for testing and certification of technologies that would be used for providers to attempt to achieve EHR Incentive Programs Stages 1–3.[267] These costs were based on the requirements of the certification program and a two-year rulemaking cycle for the CEHRT definition and each EHR Incentive Programs stage. We believe the costs we attributed to testing and certification of technologies in support of EHR Incentive Programs Stage 2 in the Permanent Certification Program final rule would encompass the actual testing and certification of technologies to both the 2014 and 2015 Editions. This assessment is based on the number of technologies currently certified to the 2014 Edition and our projections in this proposed rule for the number of technologies that would likely be tested and certified to the 2015 Edition. Further, we note that the estimated costs in the Permanent Certification Program final rule included costs for surveillance of technologies and also estimated the costs for testing and certification above what we understand are the cost ranges

[267] 76 FR 1318

charged by ONC–ACBs today. We welcome comments on our determination and our cost estimates.

b. Benefits

We believe that there will be several significant benefits that may arise from this proposed rule for patients, health care providers, and health IT developers. The 2015 Edition continues to improve health IT interoperability through the adoption of new and updated standards and implementation specifications. For example, many proposed certification criteria include standards and implementation specifications for interoperability that directly support the EHR Incentive Programs, which include objectives and measures for the interoperable exchange of health information and for providing patients electronic access to their health information in structured formats. In addition, proposed certification criteria that support the collection of patient data that could be used to address health disparities would not only benefit patients, but the entire health care delivery system through improved quality of care. The 2015 Edition also supports usability and patient safety through new and enhanced certification requirements for health IT.

Our proposals to make the ONC Health IT Certification Program open and accessible to more types of health IT and for health IT that supports a variety of care and practice settings should benefit health IT developers, providers practicing in other care/practice settings, and consumers through the availability and use of certified health IT that includes capabilities that promote interoperability and enhanced functionality.[268]

We welcome comment on other benefits, including monetary savings, which could be achieved through the proposals we have put forth in this proposed rule.

2. Regulatory Flexibility Act (RFA)

The RFA requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities.

The Small Business Administration (SBA) establishes the size of small businesses for federal government programs based on average annual receipts or the average employment of a firm. While health IT developers that pursue certification under the ONC Health IT Certification Program represent a small segment of the overall information technology industry, we believe that the entities impacted by this proposed rule most likely fall under the North American Industry Classification System (NAICS) code 541511 ''Custom Computer Programming Services'' specified at 13 CFR 121.201 where the SBA publishes ''Small Business Size Standards by NAICS Industry.'' The SBA size standard associated with this NAICS code is set at $27.5 million in annual receipts[269] which ''indicates the maximum allowed for a concern and its affiliates to be considered small entities.''

Based on our analysis, we believe that there is enough data generally available to establish that between 75% and 90% of entities that are categorized under the NAICS code 541511 are under the SBA size standard, but note that the available data does not show how many of these entities will develop a health IT product that will be certified to the 2015 Edition under the ONC Health IT Certification Program. We also note that with the exception of aggregate business information available through the U.S. Census Bureau and the SBA related to NAICS code 541511, it appears that many health IT developers that pursue certification under the ONC Health IT Certification Program are privately held or owned and do not regularly, if at all, make their specific annual receipts publicly available. As a result, it is difficult to locate empirical data related to many of these health IT developers to correlate to the SBA size standard. However, although not correlated to the size standard for NAICS code 541511, we do have information indicating that over 60% of health IT developers that have had Complete EHRs and/or EHR Modules certified to the 2011 Edition have less than 51 employees.

We estimate that this proposed rule would have effects on health IT developers that are likely to pursue certification under the ONC Health IT Certification Program, some of which may be small entities. However, we believe that we have proposed the minimum amount of requirements necessary to accomplish our policy goals, including a reduction in regulatory burden and additional flexibility for the regulated community, and that no additional appropriate regulatory alternatives could be developed to lessen the compliance burden associated with this proposed rule. We note that this proposed rule does not impose the costs cited in the RIA as compliance costs, but rather as investments which these health IT developers voluntarily take on and expect to recover with an appropriate rate of return. Accordingly, we do not believe that the proposed rule will create a significant impact on a substantial number of small entities, but request comment on whether there are small entities that we have not identified that may be affected in a significant way by this proposed rule. Additionally, the Secretary certifies that this proposed rule will not have a significant impact on a substantial number of small entities.

3. Executive Order 13132—Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. Nothing in this proposed rule imposes substantial direct compliance costs on state and local governments, preempts state law or otherwise has federalism implications. We are not aware of any State laws or regulations that are contradicted or impeded by any of the standards, implementation specifications, or certification criteria that we propose for adoption.

4. Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates require spending in any one year of $100 million in 1995 dollars, updated annually for inflation. The current inflation-adjusted statutory threshold is approximately $141 million. This proposed rule will not impose an unfunded mandate on State, local, and tribal governments or on the private sector that will reach the threshold level.

OMB reviewed this proposed rule.

List of Subjects in 45 CFR Part 170

Computer technology, Electronic health record, Electronic information system, Electronic transactions, Health, Health care, Health information technology, Health insurance, Health records, Hospitals, Incorporation by

[268] We note that, in general, these benefits will be realized only if health care providers actually adopt new technology. As discussed elsewhere in this RIA, we believe that such adoption—and thus the benefits noted in this section—would be overwhelmingly attributable to CMS's proposed rulemaking.

[269] The SBA references that annual receipts means ''total income'' (or in the case of a sole proprietorship, ''gross income'') plus ''cost of goods sold'' as these terms are defined and reported on Internal Revenue Service tax return forms. *http://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf*

reference, Laboratories, Medicaid, Medicare, Privacy, Reporting and recordkeeping requirements, Public health, Security.

For the reasons set forth in the preamble, 45 CFR subtitle A, subchapter D, part 170, is proposed to be amended as follows:

PART 170—HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY

■ 1. The authority citation for part 170 continues to read as follows:

Authority: 42 U.S.C. 300jj–11; 42 U.S.C. 300jj–14; 5 U.S.C. 552.

■ 2. Amend § 170.102 by:

■ a. Removing the ''Base EHR'', ''Certified EHR Technology'', ''Common MU Data Set'', and ''EHR Module'' definitions; and

■ b. Adding in alphanumeric order the definitions for ''2014 Edition Base EHR'', ''2015 Edition Base EHR'', ''2015 Edition health IT certification criteria'', ''Common Clinical Data Set'', ''Device identifier'', ''Global Unique Device Identification Database (GUDID)'', ''Health IT Module'', ''Implantable device'', ''Production identifier'', and ''Unique device identifier''.

The revisions read as follows:

§ 170.102 Definitions.

2014 Edition Base EHR means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to health care quality;

(iv) To exchange electronic health information with, and integrate such information from other sources;

(v) To protect the confidentiality, integrity, and availability of health information stored and exchanged; and

(3) Has been certified to the certification criteria adopted by the Secretary:

(i) For at least one of the four criteria adopted at § 170.314(a)(1), (18), (19), or (20);

(ii) At § 170.314(a)(3);

(iii) At § 170.314(a)(5) through (8);

(iv) Both § 170.314(b)(1) and (2); or, both § 170.314(b)(8) and (h)(1); or § 170.314(b)(1) and (2) combined with either § 170.314(b)(8) or (h)(1), or both § 170.314(b)(8) and (h)(1);

(v) At § 170.314(b)(7);

(vi) At § 170.314(c)(1) through (3);

(vii) At § 170.314(d)(1) through (8);

(4) Has been certified to the certification criteria at § 170.314(c)(1) and (2):

(i) For no fewer than 9 clinical quality measures covering at least 3 domains from the set selected by CMS for eligible professionals, including at least 6 clinical quality measures from the recommended core set identified by CMS; or

(ii) For no fewer than 16 clinical quality measures covering at least 3 domains from the set selected by CMS for eligible hospitals and critical access hospitals.

* * * * *

2015 Edition Base EHR means an electronic record of health-related information on an individual that:

(1) Includes patient demographic and clinical health information, such as medical history and problem lists;

(2) Has the capacity:

(i) To provide clinical decision support;

(ii) To support physician order entry;

(iii) To capture and query information relevant to health care quality;

(iv) To exchange electronic health information with, and integrate such information from other sources; and

(3) Has been certified to the certification criteria adopted by the Secretary at § 170.315(a)(1), (2), or (3); (a)(5); (a)(7) through (10); (a)(12); (a)(20); (b)(1) and (6); (c)(1); (g)(7) and (h)(1) or (2);

(4) [Reserved]

2015 Edition health IT certification criteria means the certification criteria at § 170.315.

* * * * *

Common Clinical Data Set means the following data expressed, where indicated, according to the specified standard(s):

(1) *Patient name.* For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(2) *Sex.* (i) No required standard for certification to the 2014 Edition EHR certification criteria.

(ii) The standard specified in § 170.207(n)(1) for certification to the 2015 Edition health IT certification criteria.

(3) *Date of birth.* For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(4) *Race.* (i) The standard specified in § 170.207(f)(1) for certification to the 2014 Edition EHR certification criteria.

(ii) For certification to the 2015 Edition health IT certification criteria:

(A) The standard specified in § 170.207(f)(2);

(B) The standard specified in § 170.207(f)(1) for each race identified in accordance § 170.207(f)(2).

(5) *Ethnicity.* (i) The standard specified in § 170.207(f)(1) for certification to the 2014 Edition EHR certification criteria.

(ii) For certification to the 2015 Edition health IT certification criteria:

(A) The standard specified in § 170.207(f)(2);

(B) The standard specified in § 170.207(f)(1) for each ethnicity identified in accordance § 170.207(f)(2).

(6) *Preferred language.* (i) The standard specified in § 170.207(g)(1) for certification to the 2014 Edition EHR certification criteria.

(ii) The standard specified in § 170.207(g)(2) for certification to the 2015 Edition Health IT certification criteria.

(7) *Smoking status.* For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria: The standard specified in § 170.207(h).

(8) *Problems.* (i) At a minimum, the standard specified in § 170.207(a)(3) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(a)(4) for certification to the 2015 Edition Health IT certification criteria.

(9) *Medications.* (i) At a minimum, the standard specified in § 170.207(d)(2) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(d)(3) for certification to the 2015 Edition Health IT certification criteria.

(10) *Medication allergies.* (i) At a minimum, the standard specified in § 170.207(d)(2) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(d)(3) for certification to the 2015 Edition Health IT certification criteria.

(11) *Laboratory test(s).* (i) At a minimum, the standard specified in § 170.207(c)(2) for certification to the 2014 Edition EHR certification criteria.

(ii) At a minimum, the standard specified in § 170.207(c)(3) for certification to the 2015 Edition Health IT certification criteria.

(12) *Laboratory value(s)/result(s).* For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(13) *Vital signs.* (i) Height/length, weight, blood pressure, and BMI for

certification to the 2014 Edition EHR certification criteria.

(ii) For certification to the 2015 Edition Health IT certification criteria:

(A) The patient's body height, body weight measured, diastolic blood pressure, systolic blood pressure, heart rate, respiratory rate, body temperature, oxygen saturation in arterial blood by pulse oximetry, body mass index (ratio), and mean blood pressure must be recorded in numerical values only;

(B) In accordance with the standard specified in § 170.207(k)(1) and with the associated applicable unit of measure for the vital sign in the standard specified in § 170.207(m)(1); and including

(*1*) Date and time of vital sign measurement or end time of vital sign measurement;

(*2*) The measuring- or authoring-type source of the vital sign measurement; and

(*3*) *Optional.* Date and time of vital sign measurement or end time of vital sign measurement in accordance with the standard in § 170.210(g).

(14) *Care plan field(s), including goals and instructions.* For certification to the 2014 Edition EHR certification criteria.

(15) Procedures—

(i)(A) At a minimum, the version of the standard specified in § 170.207(a)(3) for certification to the 2014 Edition EHR certification criteria and § 170.207(a)(4) for certification to the 2015 Edition health IT certification criteria, or § 170.207(b)(2); or

(B) For technology primarily developed to record dental procedures, the standard specified in § 170.207(b)(3) for certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(ii) *Optional.* The standard specified at § 170.207(b)(4) for certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(16) *Care team member(s).* For certification to both the 2014 Edition EHR certification criteria and the 2015 Edition health IT certification criteria.

(17) *Immunizations.* In accordance with, at a minimum, the standards specified in § 170.207(e)(3) and (4) for certification to the 2015 Edition health IT certification criteria.

(18) *Unique device identifier(s) for a patient's implantable device(s).* For certification to the 2015 Edition health IT certification criteria.

(19) *Assessment and plan of treatment.* For certification to the 2015 Edition health IT certification criteria:

(i) In accordance with the ''Assessment and Plan Section (V2)'' of the standard specified in § 170.205(a)(4); or

(ii) In accordance with the ''Assessment Section (V2)'' and ''Plan of Treatment Section (V2)'' of the standard specified in § 170.205(a)(4).

(20) *Goals.* In accordance with the ''Goals Section'' of the standard specified in § 170.205(a)(4) for certification to the 2015 Edition health IT certification criteria.

(21) *Health concerns.* In accordance with the ''Health Concerns Section'' of the standard specified in § 170.205(a)(4) for certification to the 2015 Edition health IT certification criteria.

* * * * *

Device identifier is defined as it is in 21 CFR 801.3.

* * * * *

Global Unique Device Identification Database (GUDID) is defined as it is in 21 CFR 801.3.

Health IT Module means any service, component, or combination thereof that can meet the requirements of at least one certification criterion adopted by the Secretary.

* * * * *

Implantable device is defined as it is in 21 CFR 801.3.

* * * * *

Production identifier is defined as it is in 21 CFR 801.3.

* * * * *

Unique device identifier is defined as it is in 21 CFR 801.3.

§ 170.200 [Amended]

■ 3. In § 170.200, remove the term ''EHR Modules'' and add in its place ''Health IT Modules.''

■ 4. In § 170.202, revise the section heading and add paragraphs (e) and (f) to read as follows:

§ 170.202 Transport standards and other protocols.

* * * * *

(e) *Delivery notification*—(1) *Standard.* ONC Implementation Guide for Delivery Notification in Direct.

(2) [Reserved]

(f) *Provider directories*—(1) *Standard.* Healthcare Provider Directory, Trial Implementation, October 13, 2014.

(2) [Reserved]

■ 5. Amend § 170.204 by—

■ a. Revising paragraphs (a) and (b)(2); and

■ b. Adding paragraphs (b)(3) and (4), (d), and (e).

The additions and revisions read as follows:

§ 170.204 Functional standards.

* * * * *

(a) *Accessibility*—(1) *Standard.* Web Content Accessibility Guidelines (WCAG) 2.0, Level A Conformance (incorporated by reference in § 170.299).

(2) [Reserved]

(b) * * *

(2) *Implementation specifications.* HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Draft Standard for Trial Use, Release 1.

(3) *Standard.* HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application. (''Infobutton''), Knowledge Request, Release 2. *Implementation specifications.* HL7 Implementation Guide: Service-Oriented Architecture Implementations of the Context-aware Knowledge Retrieval (Infobutton) Domain, Release 1.

(4) *Standard.* HL7 Version 3 Standard: Context Aware Knowledge Retrieval Application (''Infobutton''), Knowledge Request, Release 2. *Implementation specifications.* HL7 Version 3 Implementation Guide: Context-Aware Knowledge Retrieval (Infobutton), Release 4.

* * * * *

(d) *Clinical decision support knowledge artifacts*—(1) *Standard.* HL7 Version 3 Standard: Clinical Decision Support Knowledge Artifact Specification, Release 1.2, Draft Standard for Trial Use.

(2) [Reserved]

(e) *Clinical decision support service.* (1) HL7 Implementation Guide: Decision Support Service, Release 1.1, US Realm, Draft Standard for Trial Use.

(2) [Reserved]

■ 6. Amend § 170.205 by—

■ a. Adding paragraphs (a)(4) and (5), (d)(4), and (e)(4);

■ b. Revising paragraphs (g), (i), and (j); and

■ c. Adding paragraphs (l), (m), (n), (o), (p), (q), (r), and (s).

The additions and revisions read as follows:

§ 170.205 Content exchange standards and implementation specifications for exchanging electronic health information.

* * * * *

(a) * * *

(4) *Standard.* HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.0.

(5) *Implementation specifications.* (i) HL7 Implementation Guide for CDA® Release 2: Additional CDA R2 Templates—Clinical Documents for Payers—Set 1, Release 1—US Realm.

(ii) HL7 Implementation Guide for CDA Release 2: Digital Signatures and Delegation of Rights, Release 1.

(iii) Author of Record Level 1: Implementation Guide.

(iv) Provider Profiles Authentication: Registration Implementation Guide.

* * * * *

(d) * * *

(4) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Ambulatory Care, and Inpatient Settings, Release 2.0.

(e) * * *

(4) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* HL7 2.5.1 Implementation Guide for Immunization Messaging, Release 1.5.

* * * * *

(g) *Electronic transmission of lab results to public health agencies*—(1) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (incorporated by reference in § 170.299) with Errata and Clarifications, (incorporated by reference in § 170.299) and ELR 2.5.1 Clarification Document for EHR Technology Certification (incorporated by reference in § 170.299).

(2) *Standard.* HL7 2.5.1 (incorporated by reference in § 170.299). *Implementation specifications.* HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 2 (US Realm), Draft Standard for Trial Use, Release 1.1.

* * * * *

(i) *Cancer information*—(1) *Standard.* HL7 Clinical Document Architecture (CDA), Release 2.0, Normative Edition (incorporated by reference in § 170.299). *Implementation specifications.* Implementation Guide for Ambulatory Healthcare Provider Reporting to Central Cancer Registries, HL7 Clinical Document Architecture (CDA), Release 1.0 (incorporated by reference in § 170.299).

(2) *Standard.* HL7 Clinical Document Architecture (CDA), Release 2.0, Normative Edition (incorporated by reference in § 170.299). *Implementation specifications.* HL7 Implementation Guide for CDA © Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1.

(j) *Electronic incorporation and transmission of lab results*—(1) *Standard.* HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface (incorporated by reference in § 170.299).

(2) *Standard.* HL7 Version 2.5.1 Implementation Guide: S&I Framework Lab Results Interface, Draft Standard for Trial Use, Release 2—US Realm (S&I Framework LRI).

* * * * *

(l) *Laboratory orders*—(1) *Standard.* HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Orders from EHR, Draft Standard for Trial Use, Release 2—US Realm.

(2) *Standard.* HL7 Version 2.5.1 Implementation Guide: S&I Framework Laboratory Test Compendium Framework, Release 2, Version 1.2.

(m) *Family health history.* (1) HL7 Version 3 Standard: Clinical Genomics; Pedigree (incorporated by reference in § 170.299). *Implementation specifications.* HL7 Version 3 Implementation Guide: Family History/Pedigree Interoperability.

(2) [Reserved]

(n) *Drug formulary checking*—(1) *Standard.* The standard specified at 42 CFR 423.160(b)(5)(iii).

(2) [Reserved]

(o) *Data segmentation for privacy*—(1) *Standard.* HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

(2) [Reserved]

(p) *XDM package processing*—(1) *Standard.* IHE IT Infrastructure Technical Framework Volume 2b (ITI TF–2b).

(2) [Reserved]

(q) *Public health—case reporting information*—(1) *Standard.* IHE Quality, Research, and Public Health Technical Framework Supplement, Structured Data Capture, Trial Implementation.

(2) [Reserved]

(r) *Public health—antimicrobial use and resistance information*—(1) *Standard.* The following sections of HL7 Implementation Guide for CDA® Release 2—Level 3: Healthcare Associated Infection Reports, Release 1, U.S. Realm. Technology is only required to conform to the following sections of the implementation guide:

(i) HAI Antimicrobial Use and Resistance (AUR) Antimicrobial Resistance Option (ARO) Report (Numerator) specific document template in Section 2.1.2.1 (pages 69–72);

(ii) Antimicrobial Resistance Option (ARO) Summary Report (Denominator) specific document template in Section 2.1.1.1 (pages 54–56); and

(iii) Antimicrobial Use (AUP) Summary Report (Numerator and Denominator) specific document template in Section 2.1.1.2 (pages 56–58).

(2) [Reserved]

(s) *Public health—health care survey information*—(1) *Standard.* HL7 Implementation Guide for CDA Release 2: National Health Care Surveys (NHCS), Release 1—US Realm, Draft Standard for Trial Use.

(2) [Reserved]

■ 7. Amend § 170.207 by—

■ a. Adding paragraphs (a)(4), (c)(3), (d)(3), (e)(3) and (4);

■ b. Revising paragraphs (f) and (g); and

■ c. Adding paragraph (k), reserved paragraph (l), and paragraphs (m), (n), and (o).

The additions and revisions read as follows:

§ 170.207 Vocabulary standards for representing electronic health information.

* * * * *

(a) * * *

(4) *Standard.* IHTSDO SNOMED CT®, U.S. Edition, September 2014 Release.

* * * * *

(c) * * *

(3) *Standard.* Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.50, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc.

(d) * * *

(3) *Standard.* RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, February 2, 2014 Release.

(e) * * *

(3) *Standard.* HL7 Standard Code Set CVX—Vaccines Administered, updates through February 2, 2015.

(4) *Standard.* National Drug Code Directory—Vaccine Codes, updates through January 15, 2015.

(f) *Race and Ethnicity*—(1) *Standard.* The Office of Management and Budget Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity, Statistical Policy Directive No. 15, as revised, October 30, 1997.

(2) *Standard.* ''Race & Ethnicity—CDC'' code system in the PHIN Vocabulary Access and Distribution System (VADS), Release 3.3.9.

(g) *Preferred language*—(1) *Standard.* As specified by the Library of Congress, ISO 639–2 alpha-3 codes limited to those that also have a corresponding alpha-2 code in ISO 639–1 (incorporated by reference in § 170.299).

(2) *Standard.* Request for Comments (RFC) 5646.

* * * * *

(k) *Vital signs*—(1) *Standard.* Vital signs must be identified, at a minimum, with the version of LOINC® codes adopted at paragraph (c)(3) of this section attributed as follows:

(i) *Systolic blood pressure.* 8480–6

(ii) *Diastolic blood pressure.* 8462–4

(iii) *Body height.* 8302–2

(iv) *Body weight measured.* 3141–9

(v) *Heart rate.* 8867–4

(vi) *Respiratory rate.* 9279–1

(vii) *Body temperature.* 8310–5

(viii) O*xygen saturation in arterial blood by pulse oximetry.* 59408–5

(ix) *Body mass index (BMI) [ratio].* 39156–5

(x) *Mean blood pressure.* 8478–0

(2) [Reserved]

(l) [Reserved]

(m) *Numerical references*—(1) *Standard.* The Unified Code of Units of Measure, Revision 1.9.

(2) [Reserved]

(n) *Sex*—(1) *Standard.* Birth sex must be coded in accordance with HL7 Version 3 attributed as follows:

(i) *Male.* M

(ii) *Female.* F

(iii) *Unknown.* UNK

(2) [Reserved]

(o) *Social, psychological, and behavioral data*—(1) *Standard.* Sexual orientation must be coded in accordance with, at a minimum, the version of SNOMED CT® codes adopted at paragraph (a)(4) of this section for paragraphs (o)(1)(i) through (iii) of this section and HL7 Version 3 for paragraphs (o)(1)(iv) through (vi) of this section, attributed as follows:

(i) *Homosexual.* 38628009

(ii) *Heterosexual.* 20430005

(iii) *Bisexual.* 42035005

(iv) *Other.* nullFlavor OTH

(v) *Asked but unknown.* nullFlavor ASKU

(vi) *Unknown.* nullFlavor UNK

(2) *Standard.* Gender identity must be coded in accordance with, at a minimum, the version of SNOMED CT® codes adopted at paragraph (a)(4) of this section for paragraphs (o)(2)(i) through (v) of this section and HL7 Version 3 for paragraphs (o)(2)(vi) and (vii) of this section, attributed as follows:

(i*) Identifies as male gender.* 446151000124109

(ii) *Identifies as female gender.* 446141000124107

(iii) *Female-to-male transsexual.* 407377005

(iv) *Male-to-female transsexual.* 407376001

(v) *Identifies as non-conforming gender.* 446131000124102

(vi) *Other.* nullFlavor OTH

(vii) *Asked but unknown.* nullFlavor ASKU

(3) *Financial resource strain.* Financial resource strain must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with the LOINC® code and LOINC® answer list ID.

(4) *Education.* Education must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with LOINC® code 63504–5 and LOINC® answer list ID LL1069–5.

(5) *Stress.* Stress must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with the LOINC® code and LOINC® answer list ID.

(6) *Depression.* Depression must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with LOINC® codes 55757–9, 44250–9 (with LOINC® answer list ID LL358–3), 44255–8 (with LOINC® answer list ID LL358–3), and 55758–7 (with the answer coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(1)).

(7) *Physical activity.* Physical activity must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with LOINC® codes 68515–6 and 68516–4. The answers must be coded with the associated applicable unit of measure in the standard specified in § 170.207(m)(1).

(8) *Alcohol use.* Alcohol use must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with LOINC® codes 72109–2, 68518–0 (with LOINC® answer list ID LL2179–1), 68519–8 (with LOINC® answer list ID LL2180–9), 68520–6 (LOINC® answer list ID LL2181–7), and 75626–2.

(9) *Social connection and isolation.* Social connection and isolation must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with the LOINC® code and LOINC® answer list ID.

(10) *Exposure to violence (intimate partner violence).* Exposure to violence: intimate partner violence must be coded in accordance with, at a minimum, the version of LOINC® codes adopted at paragraph (c)(3) of this section and attributed with the LOINC® code and LOINC® answer list ID.

■ 8. In § 170.210:

■ a. Amend paragraphs (e)(1)(i) and (e)(3) by removing the term ''EHR technology'' and adding in its place ''health IT''; and

■ b. Add paragraph (a)(3).

The addition reads as follows:

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

* * * * *

(a) * * *

(3) *General.* Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2, October 8, 2014.

* * * * *

■ 9. In § 170.300, revise paragraph (d) to read as follows:

§ 170.300 Applicability.

* * * * *

(d) In §§ 170.314 and 170.315, all certification criteria and all capabilities specified within a certification criterion have general applicability (*i.e.,* apply to any health care setting) unless designated as ''inpatient setting only'' or ''ambulatory setting only.''

(1) *Inpatient setting only* means that the criterion or capability within the criterion is only required for certification of technology designed for use in an inpatient setting.

(2) *Ambulatory setting only* means that the criterion or capability within the criterion is only required for certification of technology designed for use in an ambulatory setting.

§ 170.314 [Amended]

■ 10. In § 170.314:

■ a. In paragraph (a)(3)(i)(A), remove ''§ 170.207(f)'' and add in its place ''§ 170.207(f)(1)'';

■ b. In paragraph (a)(3)(i)(B), remove ''§ 170.207(g)'' and add in its place ''§ 170.207(g)(1)'';

■ c. In paragraph (a)(8)(iii)(B)(*2*), remove ''paragraph (b)(1)(iii)'' and add in its place ''paragraph (b)(1)(iii)(B) or (b)(9)(ii)(D)'';

■ d. In paragraphs (b)(2)(i) introductory test, (b)(7) introductory text, (b)(8)(iii) introductory text, (e)(1)(i)(A)(*1*), and (e)(2)(iii)(A), remove the term ''Common MU Data Set'' and add in its place ''Common Clinical Data Set'';

■ e. In paragraph (b)(5)(i)(A)(*1*), remove ''§ 170.205(j)'' and add in its place ''§ 170.205(j)(1)'';

■ f. In paragraph (b)(6), remove ''§ 170.205(j)'' and add in its place ''§ 170.205(j)(1)'';

■ g. In paragraph (e)(1)(i)(A) introductory text, remove ''§ 170.204(a)'' and add in its place ''§ 170.204(a)(1)'';

■ h. In paragraph (f)(4)(i), remove ''§ 170.205(g)'' and add in its place ''§ 170.205(g)(1)''; and

■ i. In paragraph (f)(6)(i), remove ''§ 170.205(i)'' and add in its place '' § 170.205(i)(1)''.

■ 11. Add § 170.315 to read as follows:

§ 170.315 2015 Edition health IT certification criteria.

The Secretary adopts the following certification criteria for health IT. Health IT must be able to electronically perform the following capabilities in accordance with all applicable standards and implementation specifications adopted in this part:

(a) *Clinical*—(1) *Computerized provider order entry—medications.* Technology must enable a user to record, change, and access medication orders.

(2) *Computerized provider order entry—laboratory.* (i) Technology must enable a user to record, change, and access laboratory orders.

(ii) Technology must be able to receive and incorporate a new or updated laboratory order compendium in accordance with the standard specified in § 170.205(l)(2) and, at a minimum, the version of the standard in § 170.207(c)(3).

(iii) *Ambulatory setting only.* Technology must enable a user to create laboratory orders for electronic transmission in accordance with the standard specified in § 170.205(l)(1) and, at a minimum, the version of the standard in § 170.207(c)(3).

(3) *Computerized provider order entry—diagnostic imaging.* Technology must enable a user to record, change, and access diagnostic imaging orders.

(4) *Drug-drug, drug-allergy interaction checks for CPOE*—(i) *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.

(ii) *Adjustments.* (A) Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.

(B) Limit the ability to adjust severity levels to an identified set of users or available as a system administrative function.

(iii) *Interaction check response documentation.* (A) Technology must be able to record at least one action taken and by whom in response to drug-drug or drug-allergy interaction checks.

(B) Technology must be able to generate either a human readable display or human readable report of actions taken and by whom in response to drug-drug or drug-allergy interaction checks.

(5) *Demographics.* (i) Enable a user to record, change, and access patient demographic data including preferred language, sex, race, ethnicity, and date of birth.

(A) *Race and ethnicity.* (*1*) Enable each one of a patient's races to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(2) and whether a patient declines to specify race.

(*2*) Enable each one of a patient's ethnicities to be recorded in accordance with, at a minimum, the standard specified in § 170.207(f)(2) and whether a patient declines to specify ethnicity.

(*3*) Aggregate each one of the patient's races and ethnicities recorded in accordance with paragraphs (a)(5)(i)(A)(*1*) and (*2*) of this section to the categories in the standard specified in § 170.207(f)(1).

(B) Enable preferred language to be recorded in accordance with the standard specified in § 170.207(g)(2) and whether a patient declines to specify a preferred language.

(C) Enable sex to be recorded in accordance with the standard specified in § 170.207(n)(1).

(ii) *Inpatient setting only.* Enable a user to record, change, and access the preliminary cause of death and date of death in the event of mortality.

(6) *Vital signs, body mass index, and growth charts*—(i) *Vital signs.* Enable a user to record, change, and access, at a minimum, a patient's height, weight, diastolic blood pressure, systolic blood pressure, heart rate, respiratory rate, temperature, oxygen saturation in arterial blood by pulse oximetry, body mass index [ratio], and mean blood pressure in accordance with the following (The patient's height/length, weight, diastolic blood pressure, systolic blood pressure, heart rate, respiratory rate, temperature, oxygen saturation in arterial blood by pulse oximetry, body mass index [ratio], and mean blood pressure must be recorded in numerical values only.):

(A) The standard specified in § 170.207(k)(1) and with the associated applicable unit of measure for the vital sign in the standard specified in § 170.207(m)(1);

(B) *Metadata.* For each vital sign in paragraph (a)(6)(i) of this section, the technology must also record the following:

(*1*) Date and time of vital sign measurement or end time of vital sign measurement;

(*2*) The measuring- or authoring-type source of the vital sign measurement; and

(*3*) *Optional.* Date and time of vital sign measurement or end time of vital sign measurement in accordance with the standard in § 170.210(g); and

(C) *Metadata for* oxygen saturation in arterial blood by pulse oximetry. For the oxygen saturation in arterial blood by pulse oximetry, the technology must enable a user to record, change, and access the patient's inhaled oxygen concentration identified, at a minimum, with the version of the standard adopt in § 170.207(c)(3) and attributed with LOINC® code 8478–0.

(ii) *Optional—Body mass index percentile per age and sex.* Enable a user to record, change, and access a patient's body mass index [percentile] per age and sex for patients two to twenty years of age in accordance with the following (The patient's body mass index [percentile] per age and sex must be recorded in numerical values only.):

(A) Identified, at a minimum, with the version of the standard adopt in § 170.207(c)(3) and attributed with LOINC® code 59576–9 and with the associated applicable unit of measure in the standard specified in § 170.207(m)(1); and

(B) *Metadata.* The technology must also record the following:

(*1*) Date and time of vital sign measurement or end time of vital sign measurement;

(*2*) The measuring- or authoring-type source of the vital sign measurement;

(*3*) The patient's date of birth;

(*4*) The patient's sex in accordance with the standard specified in § 170.207(n)(1); and

(*5*) *Optional.* Date and time of vital sign measurement or end time of vital sign measurement in accordance with the standard in § 170.210(g).

(iii) *Optional—Weight for length per age and sex.* Enable a user to record, change, and access a patient's weight for length per age and sex for patients less than three years of age in accordance with the following (The patient's weight for length per age and sex must be recorded in numerical values only.):

(A) Identified, at a minimum, with the version of the standard adopt in § 170.207(c)(3) and attributed with the LOINC® code and with the associated applicable unit of measure in the standard specified in § 170.207(m)(1); and

(B) *Metadata.* The technology must record the following:

(*1*) Date and time of vital sign measurement or end time of vital sign measurement;

(*2*) The measuring- or authoring-type source of the vital sign measurement;

(*3*) The patient's date of birth;

(*4*) The patient's sex in accordance with the standard specified in § 170.207(n)(1); and

(*5*) *Optional.* Date and time of vital sign measurement or end time of vital sign measurement in accordance with the standard in § 170.210(g).

(iv) *Optional—Head occipital-frontal circumference.* Enable a user to record, change, and access a patient's head occipital-frontal circumference for patients less than three years of age in accordance with the following (The patient's head occipital-frontal circumference must be recorded in numerical values only.):

(A) Identified, at a minimum, with the version of the standard adopt in § 170.207(c)(3) and attributed with LOINC® code 8287–5 and with the associated applicable unit of measure in the standard specified in § 170.207(m)(1); and

(B) *Metadata.* The technology must also record the following:

(*1*) Date and time of vital sign measurement or end time of vital sign measurement;

(*2*) The measuring- or authoring-type source of the vital sign measurement;

(*3*) The patient's date of birth;

(*4*) The patient's age in accordance with the standard specified in § 170.207(n)(1); and

(*5*) *Optional.* Date and time of vital sign measurement or end time of vital sign measurement in accordance with the standard in § 170.210(g).

(v) *Optional—Calculate body mass index.* Automatically calculate and display body mass index based on a patient's height and weight.

(vi) *Optional—Plot and display growth charts.* Plot and display, upon request, growth charts for patients.

(7) *Problem list.* Enable a user to record, change, and access a patient's active problem list:

(i) *Ambulatory setting.* Over multiple encounters in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4); or

(ii) *Inpatient setting.* For the duration of an entire hospitalization in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4).

(8) *Medication list.* Enable a user to record, change, and access a patient's active medication list as well as medication history:

(i) *Ambulatory setting.* Over multiple encounters; or

(ii) *Inpatient setting.* For the duration of an entire hospitalization.

(9) *Medication allergy list.* Enable a user to record, change, and access a patient's active medication allergy list as well as medication allergy history:

(i) *Ambulatory setting.* Over multiple encounters; or

(ii) *Inpatient setting.* For the duration of an entire hospitalization.

(10) *Clinical decision support*—(i) *Evidence-based decision support interventions.* Enable a limited set of identified users to select (*i.e.,* activate) one or more electronic clinical decision support interventions (in addition to drug-drug and drug-allergy contraindication checking) based on each one and at least one combination of the following data:

(A) Problem list;

(B) Medication list;

(C) Medication allergy list;

(D) At least one demographic specified in paragraph (a)(5)(i) of this section;

(E) Laboratory tests; and

(F) Vital signs.

(ii) *Linked referential clinical decision support.* (A) Technology must be able to identify for a user diagnostic and therapeutic reference information in accordance with the standard and implementation specifications at § 170.204(b)(3) or (4).

(B) For paragraph (a)(10)(ii)(A) of this section, technology must be able to identify for a user diagnostic or therapeutic reference information based on each one and at least one combination of the data referenced in paragraphs (a)(10)(i)(A), (B), and (D) of this section.

(iii) *Clinical decision support configuration.* (A) Enable interventions and reference resources specified in paragraphs (a)(10)(i) and (ii) of this section to be configured by a limited set of identified users (*e.g.,* system administrator) based on a user's role.

(B) Technology must enable interventions to be:

(*1*) Based on the data referenced in paragraphs (a)(10)(i)(A) through (F) of this section.

(*2*) When a patient's medications, medication allergies, problems, and laboratory tests and values/results are incorporated from a transition of care/referral summary received and pursuant to paragraph (b)(2)(iii)(D) of this section.

(*3*) *Ambulatory setting only.* When a patient's laboratory tests and values/results are incorporated pursuant to paragraph (b)(4) of this section.

(iv) *CDS intervention interaction.* Interventions provided to a user in paragraphs (a)(10)(i) through (iii) of this section must occur when a user is interacting with technology.

(v) *Source attributes.* Enable a user to review the attributes as indicated for all clinical decision support resources:

(A) For evidence-based decision support interventions under paragraph (a)(10)(i) of this section:

(*1*) Bibliographic citation of the intervention (clinical research/guideline);

(*2*) Developer of the intervention (translation from clinical research/guideline);

(*3*) Funding source of the intervention development technical implementation; and

(*4*) Release and, if applicable, revision date(s) of the intervention or reference source.

(B) For linked referential clinical decision support in paragraph (a)(10)(ii) of this section and drug-drug, drug-allergy interaction checks in paragraph (a)(4) of this section, the developer of the intervention, and where clinically indicated, the bibliographic citation of the intervention (clinical research/guideline).

(vi) *Intervention response documentation.* (A) Technology must be able to record at least one action taken and by whom in response to clinical decision support interventions.

(B) Technology must be able to generate either a human readable display or human readable report of actions taken and by whom in response to clinical decision support interventions.

(11) *Drug-formulary and preferred drug list checks.* Technology must either meet paragraph (a)(11)(i) or (ii) of this section.

(i) *Drug formulary checks.* (A) Automatically check whether a drug formulary exists for a given patient and medication.

(B) Indicate for a user the last update of the drug formulary; and

(C) Receive and incorporate a formulary and benefit file in accordance with the standard specified in § 170.205(n)(1).

(ii) *Preferred drug list checks.* (A) Automatically check whether a preferred drug list exists for a given patient and medication.

(B) Indicate for a user the last update of the preferred drug list.

(12) *Smoking status.* Enable a user to record, change, and access the smoking status of a patient in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4).

(13) *Image results.* Indicate to a user the availability of a patient's images and narrative interpretations (relating to the radiographic or other diagnostic test(s)) and enable electronic access to such images and narrative interpretations.

(14) *Family health history.* Enable a user to record, change, and access a patient's family health history in accordance with the familial concepts or expressions included in, at a minimum, the version of the standard in § 170.207(a)(4).

(15) *Family health history—pedigree.* Technology must be able to create and incorporate a patient's family health history in accordance with the standard

and implementation specification specified in § 170.205(m)(1).

(16) *Patient list creation.* Enable a user to dynamically select, sort, access, and create patient lists by: date and time; and based on each one and at least one combination of the following data:

(i) Problems;

(ii) Medications;

(iii) Medication allergies;

(iv) At least one demographic specified in paragraph (a)(5)(i) of this section;

(v) Laboratory tests and values/results; and

(vi) *Ambulatory setting only.* Patient communication preferences.

(17) *Patient-specific education resources.* Technology must be able to:

(i) Identify patient-specific education resources based on data included in the patient's problem list and medication list in accordance with the standard (and implementation specifications) specified in § 170.204(b)(3) or (4); and

(ii) Request that patient-specific education resources be identified in accordance with the standard in § 170.207(g)(2).

(18) *Electronic medication administration record.* (i) In combination with an assistive technology that provides automated information on the ''rights'' specified in paragraphs (a)(18)(i)(A) through (E) of this section, enable a user to verify the following before administering medication(s):

(A) *Right patient.* The patient to whom the medication is to be administered matches the medication to be administered.

(B) *Right medication.* The medication to be administered matches the medication ordered for the patient.

(C) *Right dose.* The dose of the medication to be administered matches the dose of the medication ordered for the patient.

(D) *Right route.* The route of medication delivery matches the route specified in the medication order.

(E) *Right time.* The time that the medication was ordered to be administered compared to the current time.

(ii) *Right documentation.* Record the time and date in accordance with the standard specified in § 170.210(g), and user identification when a medication is administered.

(19) *Patient health information capture.* Technology must be able to enable a user to:

(i) Identify, record, and access patient health information documents;

(ii) Reference and link to patient health information documents; and

(iii) Record and access information directly shared by a patient.

(20) *Implantable device list.* (i) Enable a user to record, change, and access, a list of Unique Device Identifiers associated with a patient's Implantable Device(s).

(ii) Parse the following data elements from a Unique Device Identifier:

(A) Device Identifier;

(B) Batch/lot number;

(C) Expiration date;

(D) Production date; and

(E) Serial number.

(iii) Retrieve the ''Device Description'' attribute associated with a Unique Device Identifier in the Global Unique Device Identification Database.

(iv) For each Unique Device Identifier in a patient's list of implantable devices, enable a user to access the following:

(A) The parsed data elements specified under paragraph (a)(20)(ii) of this section that are associated with the UDI; and

(B) The retrieved data element specified under paragraph (a)(20)(iii) of this section.

(21) *Social, psychological, and behavioral data.* Enable a user to record, change, and access, at a minimum, one of the following patient social, psychological, and behavioral data.

(i) *Sexual orientation.* Enable sexual orientation to be recorded in accordance with the standard specified in § 170.207(o)(1) and whether a patient declines to specify sexual orientation.

(ii) *Gender identity.* Enable gender identity to be recorded in accordance with the standard specified in § 170.207(o)(2) and whether a patient declines to specify gender identity.

(iii) *Financial resource strain.* Enable financial resource strain to be recorded in accordance with the standard specified in § 170.207(o)(3) and whether a patient declines to specify financial resource strain.

(iv) *Education.* Enable education to be recorded in accordance with the standard specified in § 170.207(o)(4) and whether a patient declines to specify education.

(v) *Stress.* Enable stress to be recorded in accordance with the standard specified in § 170.207(o)(5) and whether a patient declines to specify stress.

(vi) *Depression.* Enable depression to be recorded in accordance with the standard specified in § 170.207(o)(6) and whether a patient declines to specify stress.

(vii) *Physical activity.* Enable physical activity to be recorded in accordance with the standard specified in § 170.207(o)(7) and whether a patient declines to specify physical activity.

(viii) *Alcohol use.* Enable alcohol use to be recorded in accordance with the standard specified in § 170.207(o)(8) and whether a patient declines to specify alcohol use.

(ix) *Social connection and isolation.* Enable social connection and isolation to be recorded in accordance the standard specified in § 170.207(o)(9) and whether a patient declines to specify social connection and isolation.

(x) *Exposure to violence (intimate partner violence).* Enable exposure to violence (intimate partner violence) to be recorded in accordance with the standard specified in § 170.207(o)(10) and whether a patient declines to specify exposure to violence (intimate partner violence).

(22) *Decision support—knowledge artifact.* Enable a user to send and receive clinical decision support knowledge artifacts in accordance with the standard specified in § 170.204(d)(1).

(23) *Decision support—service.* Enable a user to send and receive electronic clinical guidance in accordance with the standard specified in § 170.204(e)(1).

(b) *Care coordination*—(1) *Transitions of care*—(i) *Send and receive via edge protocol.* Technology must be able to:

(A) Send transitions of care/referral summaries through a method that conforms to the standard specified in § 170.202(d); and

(B) Receive transitions of care/referral summaries through a method that conforms to the standard specified in § 170.202(d) from a service that has implemented the standard specified in § 170.202(a).

(C) *XDM processing.* Receive and make available the contents of a XDM package formatted in accordance with the standard adopted in § 170.205(p)(1) if the technology is also being certified using an SMTP-based edge protocol.

(ii) *Validate and display*—(A) *Validate C–CDA conformance—system performance.* Technology must demonstrate its ability to detect valid and invalid transition of care/referral summaries received and formatted in accordance with both of the standards specified in § 170.205(a)(3) and (4). This includes the ability to:

(*1*) Parse each of the document types formatted according to the following document templates: CCD; Consultation Note; History and Physical; Progress Note; Care Plan; Transfer Summary; Referral Note, and Discharge Summary.

(*2*) Detect errors in corresponding ''document-templates,'' ''section-templates,'' and ''entry-templates,'' including invalid vocabulary standards and codes not specified in either of the standards adopted in § 170.205(a)(3) and (4);

(*3*) Identify valid document-templates and process the data elements required in the corresponding section-templates and entry-templates from either of the standards adopted in § 170.205(a)(3) and (4);

(*4*) Correctly interpret empty sections and null combinations; and

(*5*) Record errors encountered and allow for a user to be notified of or review the errors produced.

(B) Technology must be able to display in human readable format the data included in transition of care/referral summaries received and formatted according to the standards specified in § 170.205(a)(3) and (4).

(C) *Section views.* Allow for individual display each additional section or sections (and the accompanying document header information) that were included in a transition of care/referral summary received and formatted in accordance with either of the standards adopted in § 170.205(a)(3) and (4).

(iii) *Create.* (A) Enable a user to create a transition of care/referral summary:

(*1*) Formatted according to the standards adopted in § 170.205(a)(3);

(*2*) Formatted according to the standards adopted in § 170.205(a)(4); and

(*3*) Includes, at a minimum, the Common Clinical Data Set and the following data expressed, where applicable, according to the specified standard(s):

(*i*) *Encounter diagnoses.* The standard specified in § 170.207(i) or, at a minimum, the version of the standard specified in § 170.207(a)(4);

(*ii*) Cognitive status;

(*iii*) Functional status;

(*iv*) *Ambulatory setting only.* The reason for referral; and referring or transitioning provider's name and office contact information; and

(*v*) *Inpatient setting only.* Discharge instructions.

(B) *Patient matching data quality.* Technology must be capable of creating a transition of care/referral summary that includes the following data and, where applicable, represent such data according to the additional constraints specified below:

(*1*) *Data.* first name, last name, maiden name, middle name (including middle initial), suffix, date of birth, place of birth, current address, historical address, phone number, and sex.

(*2*) *Constraint.* Represent last/family name according to the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0.

(*3*) *Constraint.* Represent suffix according to the CAQH Phase II Core 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule version 2.1.0 (JR, SR, I, II, III, IV, V, RN, MD, Ph.D., ESQ). If no suffix exists, the field should be entered as null.

(*4*) *Constraint.* Represent the year, month and date of birth are required fields while hour, minute and second should be optional fields. If hour, minute and second are provided then either time zone offset should be included unless place of birth (city, region, country) is provided; in latter local time is assumed. If date of birth is unknown, the field should be marked as null.

(*5*) *Constraint.* Represent phone number (home, business, cell) in the ITU format specified in ITU–T E.123 and ITU–T E.164. If multiple phone numbers are present, all should be included.

(*6*) *Constraint.* Represent sex in accordance with the standard adopted at § 170.207(n)(1).

(2) *Clinical information reconciliation and incorporation*—(i) *General requirements.* Paragraphs (b)(2)(ii) and (iii) of this section must be completed based on the receipt of a transition of care/referral summary formatted in accordance with the standard adopted in § 170.205(a)(3) as well as separately to the standard adopted in § 170.205(a)(4) using the Continuity of Care Document, Discharge Summary Document and Referral Summary document templates.

(ii) *Correct patient.* Upon receipt of a transition of care/referral summary formatted according to either of the standards adopted at § 170.205(a)(3) or (4), technology must be able to demonstrate that the transition of care/referral summary received is or can be properly matched to the correct patient.

(iii) *Reconciliation.* Enable a user to reconcile the data that represent a patient's active medication list, medication allergy list, and problem list as follows. For each list type:

(A) Simultaneously display (*i.e.,* in a single view) the data from at least two sources in a manner that allows a user to view the data and their attributes, which must include, at a minimum, the source and last modification date;

(B) Enable a user to create a single reconciled list of medications, medication allergies, or problems;

(C) Enable a user to review and validate the accuracy of a final set of data; and

(D) Upon a user's confirmation, automatically update the list, and incorporate the following data expressed according to the specified standard(s):

(*1*) *Medications.* At a minimum, the version of the standard specified in § 170.207(d)(3);

(*2*) *Medication allergies.* At a minimum, the version of the standard specified in § 170.207(d)(3); and

(*3*) *Problems.* At a minimum, the version of the standard specified in § 170.207(a)(4).

(iv) *System verification.* Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard adopted at § 170.205(a)(4) using the Continuity of Care Document document template.

(3) *Electronic prescribing.* (i) Enable a user to prescribe, send, and respond to prescription-related transactions for electronic transmission in accordance with the standard specified at § 170.205(b)(2), and, at a minimum, the version of the standard specified in § 170.207(d)(3), as follows:

(A) Create new prescriptions (NEWRX);

(B) Change prescriptions (RXCHG, CHGRES);

(C) Cancel prescriptions (CANRX, CANRES);

(D) Refill prescriptions (REFREQ, REFRES);

(E) Receive fill status notifications (RXFILL); and

(F) Request and receive medication history information (RXHREQ, RXHRES).

(ii) Enable a user to enter, receive, and transmit structured and codified prescribing instructions for the transactions listed in paragraph (b)(3)(i) of this section for electronic transmission in accordance with the standard specified at § 170.205(b)(2) and, at a minimum, for at least the following component composites:

(A) Repeating Sig;

(B) Code System;

(C) Sig Free Text String;

(D) Dose;

(E) Dose Calculation;

(F) Vehicle;

(G) Route of Administration;

(H) Site of Administration;

(I) Sig Timing;

(J) Duration;

(K) Maximum Dose Restriction;

(L) Indication; and

(M) Stop.

(iii) Technology must limit a user's ability to prescribe all medications in only the metric standard.

(iv) Technology must 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.

(4) *Incorporate laboratory tests and values/results*—(i) *Receive results*—(A) *Ambulatory setting only.* (*1*) Receive and incorporate clinical laboratory tests and

values/results in accordance with the standard specified in § 170.205(j)(2); and, at a minimum, the version of the standard specified in § 170.207(c)(3).

(*2*) Display the tests and values/results received in human readable format.

(B) *Inpatient setting only.* Receive clinical laboratory tests and values/results in a structured format and display such tests and values/results in human readable format.

(ii) Display the test report information:

(A) Specified in 42 CFR 493.1291(a)(1) through (3) and (c)(1) through (7);

(B) Related to reference intervals or normal values as specified in 42 CFR 493.1291(d);

(C) For alerts and delays as specified in 42 CFR 493.1291(g) and (h); and

(D) For corrected reports as specified in 42 CFR 493.1291(k)(2).

(iii) Attribute, associate, or link a laboratory test and value/result with a laboratory order or patient record.

(5) *Transmission of laboratory test reports.* Technology must be able to electronically create laboratory test reports for electronic transmission in accordance with the standard specified in § 170.205(j)(2) and, at a minimum, the version of the standard specified in § 170.207(c)(3).

(6) *Data portability*—(i) *General requirements for export summary configuration.* A user must be able to set the following configuration options when using technology to create an export summary or set of export summaries for patients whose information is stored in the technology. A user must be able to execute these capabilities at any time the user chooses and without subsequent developer assistance to operate.

(ii) *Document creation configuration*—(A) *Document-template types.* A user must be able to configure the technology to create an export summary or export summaries formatted according to the standard adopted at § 170.205(a)(4) for any of the following document-template types.

(*1*) *Generally applicable.* CCD; Consultation Note; History and Physical; Progress Note; Care Plan; Transfer Summary; and Referral Note.

(*2*) *Inpatient setting only.* Discharge Summary.

(B) For any document-template selected the technology must be able to include, at a minimum, the Common Clinical Data Set and the following data expressed, where applicable, according to the specified standard(s):

(*1*) *Encounter diagnoses.* The standard specified in § 170.207(i) or, at a minimum, the version of the standard at § 170.207(a)(4);

(*2*) Cognitive status;

(*3*) Functional status;

(*4*) *Ambulatory setting only.* The reason for referral; and referring or transitioning provider's name and office contact information; and

(*5*) *Inpatient setting only.* Discharge instructions.

(C) Use of the ''unstructured document'' document-level template is prohibited for compliance with the standard adopted at § 170.205(a)(4)).

(iii) *Timeframe configuration.* A user must be able to configure the technology to set the time period within which data would be used to create the export summary or summaries. This must include the ability to enter in a start and end date range as well as the ability to set a date at least three years into the past from the current date.

(iv) *Event configuration.* A user must be able to configure the technology to create an export summary or summaries based on the following user selected events:

(A) A relative date or time (*e.g.,* the first of every month);

(B) A specific date or time (*e.g.,* on 10/24/2015); and

(C) When a user signs a note or an order.

(v) *Location configuration.* A user must be able to configure and set the storage location to which the export summary or export summaries are intended to be saved.

(7) *Data segmentation for privacy—send.* Technology must enable a user to create a summary record formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

(8) *Data segmentation for privacy—receive.* Technology must enable a user to:

(i) Receive a summary record that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1);

(ii) Apply document-level tagging and sequester the document from other documents received; and

(iii) View the restricted document (or data), without incorporating the document (or data).

(9) *Care plan.* Technology must enable a user to record, change, access, create, and receive care plan information in accordance with the Care Plan document template in the standard adopted in § 170.205(a)(4).

(c) *Clinical quality measures*—(1) *Clinical quality measures—record and export*—(i) *Record.* For each and every CQM for which the technology is presented for certification, the technology must be able to record all of the data that would be necessary to calculate each CQM. Data required for CQM exclusions or exceptions must be codified entries, which may include specific terms as defined by each CQM, or may include codified expressions of ''patient reason,'' ''system reason,'' or ''medical reason.''

(ii) *Export.* A user must be able to export a data file formatted in accordance with the standard specified at § 170.205(h) for one or multiple patients that includes all of the data captured for each and every CQM to which technology was certified under paragraph (c)(1)(i) of this section. A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(2) *Clinical quality measures—import and calculate*—(i) *Import.* Enable a user to import a data file in accordance with the standard specified at § 170.205(h) for one or multiple patients and use such data to perform the capability specified in paragraph (c)(2)(ii) of this section. A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(ii) Technology must be able to calculate each and every clinical quality measure for which it is presented for certification.

(3) [Reserved]

(4) *Clinical quality measures—filter.* (i) Technology must be able to record the data listed in paragraph (c)(4)(iii) of this section in accordance with the identified standards, where specified.

(ii) Technology must be able to filter CQM results at the patient and aggregate levels by each one and any combination of the data listed in paragraph (c)(4)(iii) of this section.

(iii) *Data.* (A) TIN;

(B) NPI;

(C) Provider type;

(D) Patient insurance;

(E) Patient age;

(F) Patient sex in accordance with, at a minimum, the version of the standard specified in § 170.207(n)(1);

(G) Patient race and ethnicity in accordance with, at a minimum, the version of the standard specified in § 170.207(f)(2);

(H) Patient problem list data in accordance with, at a minimum, the version of the standard specified in § 170.207(a)(4); and

(I) Practice site address.

(d) *Privacy and security*—(1) *Authentication, access control, and* *authorization.* (i) Verify against a unique identifier(s) (*e.g.,* username or number) that a person seeking access to electronic health information is the one claimed; and

(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

(2) *Auditable events and tamper-resistance*—(i) *Record actions.* Technology must be able to:

(A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1);

(B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and

(C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section).

(ii) *Default setting.* Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraph (d)(2)(i)(B) or (C) of this section, or both paragraphs (d)(2)(i)(B) and (C).

(iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users.

(iv) *Audit log protection.* Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the technology.

(v) *Detection.* Technology must be able to detect whether the audit log has been altered.

(3) *Audit report(s).* Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in § 170.210(e).

(4) *Amendments.* Enable a user to select the record affected by a patient's request for amendment and perform the capabilities specified in paragraph (d)(4)(i) or (ii) of this section.

(i) *Accepted amendment.* For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location.

(ii) *Denied amendment.* For a denied amendment, at a minimum, append the request and denial of the request to the affected record or include a link that indicates this information's location.

(5) *Automatic access time-out.* (i) Automatically stop user access to health information after a predetermined period of inactivity.

(ii) Require user authentication in order to resume or regain the access that was stopped.

(6) *Emergency access.* Permit an identified set of users to access electronic health information during an emergency.

(7) *End-user device encryption.* Paragraph (d)(7)(i) or (ii) of this section must be met to satisfy this certification criterion.

(i) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(3).

(B) *Default setting.* Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

(8) *Integrity.* (i) Create a message digest in accordance with the standard specified in § 170.210(c).

(ii) Verify in accordance with the standard specified in § 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.

(9) *Accounting of disclosures.* Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).

(e) *Patient engagement*—(1) *View, download, and transmit to 3rd party.* (i) Patients (and their authorized representatives) must be able to use technology to view, download, and transmit their health information to a 3rd party in the manner specified below. Access to these capabilities must be online and through a secure channel that ensures all content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f).

(A) *View.* Patients (and their authorized representatives) must be able to use health IT to view in accordance with the standard adopted at § 170.204(a)(1), at a minimum, the following data:

(*1*) The Common Clinical Data Set (which should be in their English (*i.e.,* non-coded) representation if they associate with a vocabulary/code set).

(*2*) *Ambulatory setting only.* Provider's name and office contact information.

(*3*) *Inpatient setting only.* Admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization.

(*4*) *Laboratory test report(s).* Laboratory test report(s), including:

(*i*) The information for a test report as specified all the data specified in 42 CFR 493.1291(c)(1) through (7);

(*ii*) The information related to reference intervals or normal values as specified in 42 CFR 493.1291(d); and

(*iii*) The information for corrected reports as specified in 42 CFR 493.1291(k)(2).

(*5*) Diagnostic image report(s).

(B) *Download.* (*1*) Patients (and their authorized representatives) must be able to use technology to download an ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) in only human readable format, in only the format specified in accordance to the standard adopted at § 170.205(a)(4), or in both formats. The use of the ''unstructured document'' document-level template is prohibited for compliance with the standard adopted at § 170.205(a)(4).

(*2*) When downloaded according to the standard adopted at § 170.205(a)(4), the ambulatory summary or inpatient summary must include, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set):

(*i*) *Ambulatory setting only.* All of the data specified in paragraph (e)(1)(i)(A)(*1*), (*2*), (*4*), and (*5*) of this section.

(*ii*) *Inpatient setting only.* All of the data specified in paragraphs (e)(1)(i)(A)(*1*), and (*3*) through (*5*) of this section.

(*3*) *Inpatient setting only.* Patients (and their authorized representatives) must be able to download transition of care/referral summaries that were created as a result of a transition of care (pursuant to the capability expressed in the certification criterion adopted at paragraph (b)(1) of this section.

(C) *Transmit to third party.* Patients (and their authorized representatives) must be able to:

(*1*) Transmit the ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) created in paragraph (e)(1)(i)(B)(*2*) of this section in accordance with at least one of the following:

(*i*) The standard specified in § 170.202(a).

(*ii*) Through a method that conforms to the standard specified at § 170.202(d) and leads to such summary being processed by a service that has implemented the standard specified in § 170.202(a).

(*2*) *Inpatient setting only.* Transmit transition of care/referral summaries (as a result of a transition of care/referral) selected by the patient (or their authorized representative) in accordance with at least one of the following:

(*i*) The standard specified in § 170.202(a).

(*ii*) Through a method that conforms to the standard specified at § 170.202(d) and leads to such summary being processed by a service that has implemented the standard specified in § 170.202(a).

(ii) *Activity history log.* (A) When electronic health information is viewed, downloaded, or transmitted to a third-party using the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section or when an application requests electronic health information using the capability specified at paragraph (e)(1)(iii) of this section, the following information must be recorded and made accessible to the patient:

(*1*) The action(s) (*i.e.,* view, download, transmission, API response) that occurred;

(*2*) The date and time each action occurred in accordance with the standard specified at § 170.210(g);

(*3*) The user who took the action; and

(*4*) Where applicable, the addressee to whom an ambulatory summary or inpatient summary was transmitted.

(B) Technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) of this section if it is also certified to the certification criterion adopted at § 170.315(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.

(iii) *Application access.* Patients (and their authorized representatives) must be able to use an application that can interact with the following capabilities. Additionally, the following technical outcomes and conditions must be met through the demonstration of an application programming interface (API) that can respond to requests from other applications for data specified within the Common Clinical Data Set.

(A) *Security.* The API must include a means to establish a trusted connection with the application requesting patient data, including a means for the requesting application to register with the data source, be authorized to request data, and log all interactions between the application and the data source.

(B) *Patient selection.* The API must include a means for the application to query for an ID or other token of a patient's record in order to subsequently execute data requests for that record in accordance with (e)(1)(iii)(C) of this section.

(C) *Data requests, response scope, and return format.* The API must enable and support both of the following data request interactions:

(*1*) *Data-category request.* The API must support syntax that allows it to respond to requests for each of the individual data categories specified in the Common Clinical Data Set and return the full set of data for that data category (according to the specified standards, where applicable) in either XML or JSON.

(*2*) *All-request.* The API must support syntax that allows it to respond to a request for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard adopted at § 170.205(a)(4).

(D) *Documentation.* The API must include accompanying documentation that contains, at a minimum:

(*1*) API syntax, function names, required and optional parameters 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).

(E) *Terms of use.* The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(2) *Secure messaging.* Enable a user to send messages to, and receive messages from, a patient in a manner that ensures:

(i) Both the patient (or authorized representative) and technology user are authenticated; and

(ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f).

(f) *Public health*—(1) *Transmission to immunization registries.* (i) Technology must be able to create immunization information for electronic transmission in accordance with:

(A) The standard and applicable implementation specifications specified in § 170.205(e)(4);

(B) At a minimum, the version of the standard specified in § 170.207(e)(3) for historical vaccines; and

(C) At a minimum, the version of the standard specified in § 170.207(e)(4) for administered vaccines.

(ii) Technology must enable a user to request, access, and display a patient's evaluated immunization history and the immunization forecast from an immunization registry in accordance with the standard at § 170.205(e)(4).

(2) *Transmission to public health agencies—syndromic surveillance*—(i) *Ambulatory setting only.* (A) Technology must be able to create syndrome-based public health surveillance information for electronic transmission.

(B) *Optional.* Technology must be able to create syndrome-based public health surveillance information for electronic transmission that contains the following data:

(*1*) Patient demographics;

(*2*) Provider specialty;

(*3*) Provider address;

(*4*) Problem list;

(*5*) Vital signs;

(*6*) Laboratory test values/results;

(*7*) Procedures;

(*8*) Medication list; and

(*9*) Insurance.

(ii) *Inpatient setting only.* Technology must be able to create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

(3) *Transmission to public health agencies—reportable laboratory tests and values/results.* Technology must be able to create reportable laboratory tests and values/results for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(g)(2); and

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(4) and (c)(3).

(4) *Transmission to cancer registries.* Technology must be able to create cancer case information for electronic transmission in accordance with:

(i) The standard (and applicable implementation specifications) specified in § 170.205(i)(2); and

(ii) At a minimum, the versions of the standards specified in § 170.207(a)(4) and (c)(3).

(5) *Transmission to public health agencies—case reporting.* Technology must be able to create case reporting information for electronic transmission in accordance with the standard specified in § 170.205(q)(1).

(6) *Transmission to public health agencies—antimicrobial use and resistance reporting.* Technology must be able to create antimicrobial use and resistance reporting information for electronic transmission in accordance with the standard specified in § 170.205(r)(1).

(7) *Transmission to public health agencies—health care surveys.* Technology must be able to create health care survey information for electronic transmission in accordance with the standard specified in § 170.205(s)(1).

(g) *Design and performance*—(1) *Automated numerator recording.* For each meaningful use objective with a percentage-based measure, technology must be able to create a report or file that enables a user to review the patients or actions that would make the patient or action eligible to be included in the measure's numerator. The information in the report or file created must be of sufficient detail such that it enables a user to match those patients or actions to meet the measure's denominator limitations when necessary to generate an accurate percentage.

(2) *Automated measure calculation.* For each meaningful use objective with a percentage-based measure that is supported by a capability included in a technology, record the numerator and denominator and create a report including the numerator, denominator, and resulting percentage associated with each applicable meaningful use measure.

(3) *Safety-enhanced design.* (i) User-centered design processes must be applied to each capability technology includes that is specified in the following certification criteria: paragraphs (a)(1) through (10) and (18), (20), (22), (23), and (b)(2) through (4) of this section.

(ii) The following information must be submitted on the user-centered design processed used:

(A) Name, description and citation (ULR and/or publication citation) for an industry or federal government standard; or

(B) Name the process(es), provide an outline of the process(es), a short description of the process(es), and an explanation of the reason(s) why use of any of the existing user-centered design standards was impractical.

(iii) The following information/sections from NISTIR 7742 must be submitted for each capability to which user-centered design processes were applied:

(A) Name and version of the product; date and location of the test; test environment; description of the intended users; and total number of participants;

(B) Description of participants, including: sex; age; education; occupation/role; professional experience; computer experience; and product experience;

(C) Description of the user tasks that were tested and association of each task to corresponding certification criteria;

(D) List of the specific metrics captured during the testing, including: task success (%); task failures (%); task standard deviations (%); task performance time; and user satisfaction rating (based on a scale with 1 as very difficult and 5 as very easy);

(E) Test results for each task using metrics listed above in paragraphs (g)(3)(ii)(A) through (D) of this section;

(F) Results and data analysis narrative, including: major test finding; effectiveness; efficiency; satisfaction; and areas for improvement.

(iv) Submit test scenarios used in summative usability testing.

(4) *Quality management system.* (i) For each capability that a technology includes and for which that capability's certification is sought, the use of a Quality Management System (QMS) in the development, testing, implementation, and maintenance of that capability must be identified that is:

(A) Compliant with a QMS established by the Federal government or a standards developing organization; or

(B) Mapped to one or more QMS established by the Federal government or standards developing organization(s).

(ii) If a single QMS was used for applicable capabilities, it would only need to be identified once.

(iii) If different QMS were applied to specific capabilities, each QMS applied would need to be identified.

(5) *Accessibility technology compatibility.* For each capability technology includes that is specified in the certification criteria at paragraphs (a), (b), and (e) of this section, the capability must be compatible with at least one accessibility technology that includes text-to-speech functionality.

(6) *Consolidated CDA creation performance.* The following technical and performance outcomes must be demonstrated related to Consolidated CDA creation. The capabilities required under paragraphs (g)(6)(i) through (iii) of this section can be demonstrated in tandem and do not need to be individually addressed in isolation or sequentially.

(i) *Reference C–CDA match.* Upon the entry of clinical data consistent with the Common Clinical Data Set, the technology must be able to create a data file formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that matches a gold-standard, reference data file.

(ii) *Document-template conformance.* Upon the entry of clinical data consistent with the Common Clinical Data Set, the technology must be able to create a data file formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that demonstrates a valid implementation of each of the following document templates (as applicable to the adopted standard):

(A) *Generally applicable.* CCD; Consultation Note; History and Physical; Progress Note; Care Plan; Transfer Summary; and Referral Note.

(B) *Inpatient setting only.* Discharge Summary.

(iii) *Vocabulary conformance.* Upon the entry of clinical data consistent with the Common Clinical Data Set, the technology must be able to create a data file formatted in accordance with each of the standards adopted in § 170.205(a)(3) and (4) that demonstrates the required vocabulary standards (and value sets) are properly implemented.

(7) *Application access to Common Clinical Data Set.* The following technical outcomes and conditions must be met through the demonstration of an application programming interface (API) that can respond to requests from other applications for data specified within the Common Clinical Data Set.

(i) *Security.* The API must include a means to establish a trusted connection with the application requesting patient data, including a means for the requesting application to register with the data source, be authorized to request data, and log all interactions between the application and the data source.

(ii) *Patient selection.* The API must include a means for the application to query for an ID or other token of a patient's record in order to subsequently execute data requests for that record in accordance with paragraph (g)(7)(iii) of this section.

(iii) *Data requests, response scope, and return format.* The API must enable and support both of the following data request interactions:

(A) *Data-category request.* The API must support syntax that allows it to respond to requests for each of the individual data categories specified in the Common Clinical Data Set and return the full set of data for that data category (according to the specified standards, where applicable) in either XML or JSON.

(B) *All-request.* The API must support syntax that allows it to respond to a request for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard adopted at § 170.205(a)(4).

(iv) *Documentation.* The API must include accompanying documentation that contains, at a minimum:

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

(B) 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).

(v) *Terms of use.* The terms of use for the API must be provided, including, at a minimum, any associated developer policies and required developer agreements.

(8) *Accessibility-centered design.* For each capability that a Health IT Module includes and for which that capability's certification is sought, the use of a health IT accessibility-centered design standard or law in the development, testing, implementation and maintenance of that capability must be identified.

(i) If a single accessibility-centered design standard or law was used for applicable capabilities, it would only need to be identified once.

(ii) If different accessibility-centered design standards and laws were applied to specific capabilities, each accessibility-centered design standard or law applied would need to be identified. This would include the application of an accessibility-centered design standard or law to some capabilities and none to others.

(iii) If no accessibility-centered design standard or law was applied to all applicable capabilities such a response is acceptable to satisfy this certification criterion.

(h) *Transport methods and other protocols*—(1) *Direct Project*—(i) *Applicability Statement for Secure Health Transport.* Technology must be able to send and receive health information in accordance with the standards specified in § 170.202(a).

(ii) *Optional—Applicability Statement for Secure Health Transport and Delivery Notification in Direct.* Technology must be able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

(2) *Direct Project, Edge Protocol, and XDR/XDM.* Technology must be able to send and receive health information in accordance with:

(i) The standards specified in § 170.202(a);

(ii) The standard specified in § 170.202(b); and

(iii) Both edge protocol methods specified by the standard in § 170.202(d).

(3) *SOAP Transport and Security Specification and XDR/XDM for Direct Messaging.* Technology must be able to send and receive health information in accordance with the standards specified in § 170.202(b) and (c).

(4) *Healthcare provider directory—query request.* In accordance with the standard specified in § 170.202(f)(1), technology must be able to make, at a minimum, the following queries to a directory and subsequently process the response returned:

(i) Query for an individual provider;

(ii) Query for an organizational provider;

(iii) Query for both individual and organizational providers in a single query; and

(iv) Query for relationships between individual and organizational providers.

(v) *Optional—federation.* In accordance with the standard specified in § 170.202(f)(1), technology must be able to process federated responses.

(5) *Healthcare provider directory—query response.* In accordance with the standard specified in § 170.202(f)(1), technology must be able to, at a minimum, respond to the following queries to a directory:

(i) Query for an individual provider;

(ii) Query for an organizational provider;

(iii) Query for both individual and organizational providers in a single query; and

(iv) Query for relationships between individual and organizational providers.

(v) *Optional—federation.* In accordance with the standard specified in § 170.202(f)(1), technology must be able to federate queries to other directories.

(i) *Administrative*—(1) *Electronic submission of medical documentation*—(i) *Document templates.* Health IT must be able to create electronic documents for transmission formatted according to the following standard and applicable implementation specifications adopted at § 170.205(a)(4) and (a)(5)(i). With respect to § 170.205(a)(5)(i):

(A) Health IT must be able to create the following document types regardless of the setting for which it is designed: Diagnostic Imaging Report; Unstructured Document; Enhanced Operative Note Document; Enhanced Procedure Note Document; and Interval Document.

(B) *Ambulatory setting only.* Health IT must be able to create an Enhanced Encounter Document.

(C) *Inpatient setting only.* Health IT must be able to create an Enhanced Hospitalization Document.

(ii) *Digital signature.* (A) *Applying a digital signature.* Technology must be able to apply a digital signature in accordance with the implementation specification adopted at § 170.205(a)(5)(ii) to a document formatted according to the following standard and applicable implementation specifications adopted at § 170.205(a)(4) and (a)(5)(i). It must also be able to demonstrate that it can support the method for delegation of right assertions.

(*1*) The cryptographic module used as part of the technology must: Be validated to meet or exceed FIPS 140–2 Level 1; include a digital signature system and hashing that are compliant with FIPS 186–2 and FIPS 180–2; and store the private key in a FIPS–140–2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm. This requirement may be satisfied through documentation only.

(*2*) Technology must support multi-factor authentication that meets or exceeds Level 3 assurance as defined in NIST Special Publication 800–63–2.

(*3*) After ten minutes of inactivity, technology must require the certificate holder to re-authenticate to access the private key.

(*4*) If implemented as a software function, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use of, the private key when the signing module is deactivated.

(*5*) Technology must record time and date consistent with the standard adopted at § 170.210(g).

(B) *Validating a digital signature.* Technology must be able validate a digital signature that has been applied to a document according to the implementation specification adopted at § 170.205(a)(5)(ii).

(iii) *Author of record level 1.* Using the same system capabilities expressed in paragraph (i)(1)(ii), technology must be able to apply a digital signature according to the implementation specification adopted at § 170.205(a)(5)(iii) to sign single or bundles of documents a document formatted according to the following standard and applicable implementation specifications adopted at § 170.205(a)(4) and (a)(5)(i).

(iv) *Transactions.* Using the same system capabilities expressed in paragraph (i)(1)(ii) of this section, technology must be able to apply a digital signature according to the implementation specification adopted at § 170.205(a)(5)(iv) to a transaction and include the signature as accompanying metadata in the signed transaction.

(2) [Reserved]

§§ 170.500, 170.501, 170.502, 170.503, 170.504, 170.505, 170.510, 170.520, 170.523, 170.525, 170.530, 170.535, 170.540, 170.545, 170.550, 170.553, 170.555, 170.557, 170.560, 170.565, 170.570, 170.575, and 170.599 [Amended]

■ 12. In subpart E, consisting of §§ 170.500 through 170.599:

■ a. Remove the term ''ONC HIT Certification Program'' and add in its place ''ONC Health IT Certification Program'' wherever it may appear;

■ b. Remove the acronym ''HIT'' and add in its place ''health IT'' wherever it may appear;

■ c. Remove the term ''EHR Module'' and add in its place ''Health IT Module'' wherever it may appear;

■ d. Remove the term ''EHR Modules'' and add in its place ''Health IT Modules'' wherever it may appear; and

■ e. Remove the term ''EHR Module(s)'' and add in its place ''Health IT Module(s)'' wherever it may appear.

■ 13. In § 170.503, revise paragraph (e)(4) to read as follows:

§ 170.503 Requests for ONC–AA status and ONC–AA ongoing responsibilities.

* * * * *

(e) * * *

(4) Verify that ONC–ACBs are performing surveillance as required by and in accordance with § 170.556, § 170.523(k), and their respective annual plans; and

* * * * *

■ 14. Amend § 170.523 by—

■ a. Revising paragraphs (f), (g), (i), and (k); and

■ b. Adding paragraphs (m) and (n).

The additions and revisions read as follows:

§ 170.523 Principles of proper conduct for ONC–ACBs.

* * * * *

(f) Provide ONC, no less frequently than weekly, a current list of Health IT Modules, Complete EHRs, and/or EHR Modules that have been certified that includes, at a minimum:

(1) For the 2015 Edition health IT certification criteria and subsequent editions of health IT certification criteria:

(i) The Health IT Module developer name; product name; product version; developer Web site, physical address, email, phone number, and contact name;

(ii) The ONC–ACB Web site, physical address, email, phone number, and contact name, contact function/title;

(iii) The ATL Web site, physical address, email, phone number, and contact name, contact function/title;

(iv) Location and means by which the testing was conducted (*e.g.*, remotely with health IT developer at its headquarters location);

(v) The date(s) the Health IT Module was tested;

(vi) The date the Health IT Module was certified;

(vii) The unique certification number or other specific product identification;

(viii) The certification criterion or criteria to which the Health IT Module has been certified, including the test procedure and test data versions used, test tool version used, and whether any test data was altered (*i.e.*, a yes/no) and for what purpose;

(ix) The way in which each privacy and security criterion was addressed for the purposes of certification;

(x) The standard or mapping used to meet the quality management system certification criterion;

(xi) The standard(s) or lack thereof used to meet the accessibility-centered design certification criterion;

(xii) *Where applicable*, the hyperlink to access an application programming interface (API)'s documentation and terms of use;

(xiii) *Where applicable*, which certification criteria were gap certified;

(xiv) *Where applicable*, if a certification issued was a result of an inherited certified status request;

(xv) *Where applicable*, the clinical quality measures to which the Health IT Module has been certified;

(xvi) *Where applicable*, any additional software a Health IT Module relied upon to demonstrate its compliance with a certification criterion or criteria adopted by the Secretary;

(xvii) *Where applicable*, the standard(s) used to meet a certification criterion where more than one is permitted;

(xviii) *Where applicable*, any optional capabilities within a certification criterion to which the Health IT Module was tested and certified;

(xix) *Where applicable*, and for each applicable certification criterion, all of the information required to be submitted by Health IT Module developers to meet the safety-enhanced design certification criterion. Each user-centered design element required to be reported must be at a granular level (*e.g.*, task success/failure)); and

(xx) *Where applicable*, for each instance in which a Health IT Module failed to conform to its certification and for which corrective action was instituted under § 170.556 (provided no provider or practice site is identified):

(A) The specific certification criterion to which the technology failed to conform as determined by the ONC–ACB;

(B) The dates surveillance was initiated and when available, completed;

(C) The results of the surveillance (pass rate for each criterion);

(D) The number of sites that were used in surveillance;

(E) The date corrective action began;

(F) When available, the date correction action ended;

(G) A summary of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformance; and

(H) When available, the health IT developer's explanation of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformance.

(2) For the 2014 Edition EHR certification criteria:

(i) The Complete EHR or EHR Module developer name (if applicable);

(ii) The date certified;

(iii) The product version;

(iv) The unique certification number or other specific product identification;

(v) The clinical quality measures to which a Complete EHR or EHR Module has been certified;

(vi) Where applicable, any additional software a Complete EHR or EHR Module relied upon to demonstrate its compliance with a certification criterion or criteria adopted by the Secretary;

(vii) Where applicable, the certification criterion or criteria to which each EHR Module has been certified; and

(viii) A hyperlink to the test results used to certify the Complete EHRs and/or EHR Modules that can be accessed by the public.

(ix) *Where applicable*, for each instance in which a Complete EHR or EHR Module failed to conform to its certification and for which corrective action was instituted under § 170.556 (provided no provider or practice site is identified):

(A) The specific certification criterion to which the technology failed to conform as determined by the ONC–ACB;

(B) The dates surveillance was initiated and when available, completed;

(C) The results of the surveillance (pass rate for each criterion);

(D) The number of sites that were used in surveillance;

(E) The date corrective action began;

(F) When available, the date corrective action ended;

(G) A summary of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformance; and

(H) When available, the developer's explanation of the deficiency or deficiencies identified by the ONC–ACB as the basis for its determination of non-conformance.

(g) Retain all records related to the certification of Complete EHRs and Health IT Modules for a minimum of 6 years and make them available to HHS upon request;

* * * * *

(i) Submit an annual surveillance plan to the National Coordinator and, in accordance with its surveillance plan, its accreditation, and § 170.556:

(1) Conduct surveillance of certified Complete EHRs and Health IT Modules; and

(2) Report, at a minimum, on a quarterly basis to the National Coordinator the results of its surveillance.

* * * * *

(k) Ensure adherence to the following requirements when issuing any certification and during surveillance of Complete EHRs and Health IT Modules the ONC–ACB has certified:

(1) A Health IT developer must conspicuously include the following on its Web site and in all marketing materials, communications statements, and other assertions related to the Complete EHR or Health IT Module's certification:

(i) The disclaimer "This [Complete EHR or Health IT Module] is [specify Edition of EHR certification criteria] compliant and has been certified by an ONC–ACB in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services. Complaints related to this [Complete EHR or Health IT Module]'s certified capabilities or health IT developer's disclosures should be submitted to *ONC.Certification@hhs.gov*."

(ii) The information an ONC–ACB is required to report to the National Coordinator under paragraphs (f)(1) and (2) of this section as applicable for the specific Complete EHR or Health IT Module.

(iii) In plain language, a detailed description of all known material information concerning:

(A) Additional types of costs that a user may be required to pay to implement or use the Complete EHR or Health IT Module's capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification.

(B) Limitations that a user may encounter in the course of implementing and using the Complete EHR or Health IT Module's capabilities, whether to meet meaningful use objectives and measures or to achieve any other use within the scope of the health IT's certification.

(iv) The types of information required to be disclosed under paragraph (k)(iii) of this section include but are not limited to:

(A) Additional types of costs or fees (whether fixed, recurring, transaction-based, or otherwise) imposed by a health IT developer (or any third-party from whom the developer purchases, licenses, or obtains any technology, products, or services in connection with its certified health IT) to purchase, license, implement, maintain, upgrade, use, or otherwise enable and support the use of capabilities to which health IT is certified; or in connection with any data generated in the course of using any capability to which health IT is certified.

(B) Limitations, whether by contract or otherwise, on the use of any capability to which technology is certified for any purpose within the scope of the technology's certification; or in connection with any data generated in the course of using any capability to which health IT is certified.

(C) Limitations, including but not limited to technical or practical limitations of technology or its capabilities, that could prevent or impair the successful implementation, configuration, customization, maintenance, support, or use of any capabilities to which technology is certified; or that could prevent or limit the use, exchange, or portability of any data generated in the course of using any capability to which technology is certified.

(vi) Health IT self-developers are excluded from the requirements of paragraph (k)(1)(iii) of this section.

(2) A health IT developer must attest as a condition of certification to any certification criterion that it will timely provide in plain writing, conspicuously, and in sufficient detail:

(i) To all customers, prior to providing or entering into any agreement to provide any certified health IT or related product or service (including subsequent updates, add-ons, or additional products or services during the course of an on-going agreement), the information required to be disclosed under paragraph (k)(1) of this section;

(ii) To any person who requests or receives a quotation, estimate, description of services, or other assertion or information from the developer in connection with any certified health IT or any capabilities thereof, the information required to be disclosed under paragraph (k)(1) of this section; and

(iii) To any person, upon request, all or any part of the information required to be disclosed under paragraph (k)(1) of this section.

(3) A certification issued to a pre-coordinated, integrated bundle of Health IT Modules shall be treated the same as a certification issued to a Complete EHR for the purposes of paragraph (k)(1) of this section, except that the certification must also indicate each Health IT Module that is included in the bundle; and

(4) A certification issued to a Complete EHR or Health IT Module based solely on the applicable certification criteria adopted by the Secretary at subpart C of this part must be separate and distinct from any other certification(s) based on other criteria or requirements.

* * * * *

(m) Obtain a record of all adaptations and updates, including changes to user-facing aspects, made to certified Complete EHRs and certified Health IT Modules, on a monthly basis each calendar year.

(n) Submit a list of complaints received to the National Coordinator on a quarterly basis that includes the number of complaints received, the nature/substance of each complaint, and the type of complainant.

■ 15. Amend § 170.550 by—

■ a. Redesignating paragraph (g) as paragraph (k);

■ b. Adding paragraphs (g) and (h); and

■ c. Adding reserved paragraph (i) and paragraph (j).

The additions read as follows:

§ 170.550 Health IT Module certification.

* * * * *

(g) When certifying a Health IT Module to the 2015 Edition health IT certification criteria, an ONC–ACB must certify the Health IT Module in accordance with the certification criteria at:

(1) Section 170.315(g)(3) if the Health IT Module is presented for certification to one or more listed certification criteria in § 170.315(g)(3);

(2) Section 170.315(g)(4);

(3) Section 170.315(g)(5) if the Health IT Module is presented for certification to one or more of the certification criteria referenced in § 170.315(g)(5);

(4) Section 170.315(g)(6) if the Health IT Module is presented for certification with C–CDA creation capabilities within its scope. If the scope of certification sought includes multiple certification criteria that require C–CDA creation, § 170.315(g)(6) need only be tested in association with one of those certification criteria and would not be expected or required to be tested for each; and

(5) Section 170.315(g)(8).

(h) *Privacy and security certification*—(1) *General rule.* When certifying a Health IT Module to the 2015 Edition health IT certification criteria, an ONC–ACB can only issue a certification to a Health IT Module if the following adopted privacy and security certification criteria have also been met as applicable to the specific capabilities included for certification:

(i) Section 170.315(a) is also certified to the certification criteria adopted at § 170.315(d)(1) through (7);

(ii) Section 170.315(b) is also certified to the certification criteria adopted at § 170.315(d)(1) through (3) and (d)(5) through (8);

(iii) Section 170.315(c) is also certified to the certification criteria adopted at § 170.315(d)(1) through (3);

(iv) Section 170.315(e) is also certified to the certification criteria adopted at § 170.315(d)(1) through (3), (5), and (7);

(v) Section 170.315(f) is also certified to the certification criteria adopted at § 170.315(d)(1) through (3) and (7);

(vi) Section 170.315(h) is also certified to the certification criteria adopted at § 170.315(d)(1) through (3); and

(vii) Section 170.315(i) is also certified to the certification criteria adopted at § 170.315(d)(1) through (3) and (d)(5) through (8).

(2) *Methods to demonstrate compliance with each privacy and security criterion.* One of the following methods must be used to meet each applicable privacy and security criterion listed in paragraph (h)(1) of this section:

(i) Directly, by demonstrating a technical capability to satisfy the applicable certification criterion or certification criteria; or

(ii) Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

(i) [Reserved]

(j) *Direct Project transport method.* An ONC–ACB can only issue a certification to a Health IT Module for § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1).

* * * * *

§ 170.553 [Removed and Reserved]

■ 16. Remove and reserve § 170.553.

■ 17. Add § 170.556 to read as follows:

§ 170.556 In-the-field surveillance and maintenance of certification for Health IT.

(a) *In-the-field surveillance.* Consistent with its accreditation to ISO/IEC 17065 and the requirements of this subpart, an ONC–ACB must initiate surveillance ''in the field'' as necessary to assess whether a certified Complete EHR or certified Health IT Module continues to conform to the requirements of its certification once the certified Complete EHR or certified Health IT Module has been implemented and is in use in a production environment.

(1) *Production environment.* An ONC–ACB's assessment of a certified capability in the field must be based on the use of the capability in a production environment, which means a live environment in which the capabilities have been implemented and are in use.

(2) *Production data.* An ONC–ACB's assessment of a certified capability in the field must be based on the use of the capability with production data unless the use of test data is specifically approved by the National Coordinator.

(b) *Reactive surveillance.* An ONC–ACB must initiate in-the-field surveillance whenever it becomes aware of facts or circumstances that would cause a reasonable person to question a certified Complete EHR or certified Health IT Module's continued conformance to the requirements of its certification.

(1) *Prioritized certification criteria.* An ONC–ACB must initiate in-the-field surveillance if it identifies a trend of non-conformance complaints associated with any certification criteria prioritized by the National Coordinator.

(2) *Review of required disclosures.* When an ONC–ACB performs reactive surveillance under this paragraph (b), it must verify that the requirements of § 170.523(k)(1) have been followed as applicable to the issued certification.

(c) *Randomized surveillance.* An ONC–ACB must initiate in-the-field surveillance for at least 10% of the Complete EHRs and Health IT Modules to which it has issued a certification. Such surveillance must occur on a rolling basis throughout each calendar year.

(1) *Scope.* When an ONC–ACB selects a certified Complete EHR or certified Health IT Module for randomized surveillance under this paragraph, its evaluation of the certified Complete EHR or certified Health IT Module must include all certification criteria prioritized by the National Coordinator under paragraph (b)(1) of this section that are part of the scope of the certification issued to the Complete EHR or Health IT Module.

(2) *Rolling surveillance.* Randomized surveillance required by this paragraph must be completed on an ongoing basis throughout the calendar year.

(3) *Random selection.* An ONC–ACB must randomly select certified Complete EHRs and certified Health IT Modules for surveillance under this paragraph.

(4) *Number and types of locations for in-the-field surveillance.* For each certified Compete EHR or certified Health IT Module selected for randomized surveillance under this paragraph (c), an ONC–ACB must evaluate the certified Complete EHR or certified Health IT Module's capabilities at the lesser of 10 or 5% of locations where the certified Complete EHR or certified Health IT Module is implemented and in use in the field.

(5) *Results of randomized surveillance*—(i) *Successful surveillance results.* A certified Complete EHR or certified Health IT Module will be deemed successful under this paragraph if and only if an ONC–ACB determines that, for each and every certification criterion evaluated, the certified Complete EHR or certified Health IT Module demonstrated continued conformance at 80% or more locations.

(ii) *Deficient surveillance results.* A certified Complete EHR or certified Health IT Module will be deemed deficient under this paragraph if an ONC–ACB determines that, for any certification criterion evaluated, the Complete EHR or Health IT Module demonstrated continued conformance at less than 80% of locations.

(6) *Corrective action plan*—(i) Whenever a Complete EHR or Health IT Module is deemed deficient pursuant to paragraph (c)(5)(ii) of this section, the ONC–ACB must notify the developer of the deficiency and require the developer

to submit a proposed corrective action plan for the applicable certification criterion or certification criteria within 30 days of the date of said notice.

(ii) The ONC–ACB shall provide direction to the developer as to the required elements of the corrective action plan.

(iii) The ONC–ACB shall determine the required elements of the corrective action plan, consistent with its accreditation and any elements specified by the National Coordinator. At a minimum, any corrective action plan submitted by a developer to an ONC–ACB must include:

(A) A description of the identified deficiencies;

(B) An assessment of how widespread or isolated the identified deficiencies may be across the developer's install base for certified Complete EHR or certified Health IT Module;

(C) How the developer will address the identified conformance deficiencies in general and at the locations under which surveillance occurred; and

(D) The timeframe under which corrective action will be completed.

(7) *Certificate suspension procedures in the context of randomized surveillance and corrective action plans.* Under this section and consistent with an ONC–ACB's accreditation to ISO/IEC 17065 and procedures for suspending a certification, an ONC–ACB is permitted to initiate certificate suspension procedures for the Complete EHR or Health IT Module if the developer thereof:

(i) Does not submit a proposed corrective action plan to the ONC–ACB within 30 days of being notified of its deficient surveillance results;

(ii) Does not comply with the ONC–ACB's directions for addressing any aspects of the proposed corrective action plan that do not meet the requirements of the ONC–ACB or the ONC Health IT Certification Program; or

(iii) Does not complete an approved corrective action plan within 6 months of approval of the plan by the ONC–ACB.

(8) *Certificate termination procedures in the context of randomized surveillance.* If a certified Complete EHR or certified Health IT Module's certification has been suspended in the context of randomized surveillance under this paragraph, an ONC–ACB is permitted to initiate certification termination procedures for the Complete EHR or Health IT Module (consistent with its accreditation to ISO/IEC 17065 and procedures for terminating a certification) when the developer has not completed the actions necessary to reinstate the suspended certification.

(9) *Prohibition on consecutive selection for randomized surveillance.* An ONC–ACB is prohibited from selecting a certified Complete EHR or certified Health IT Module for randomized surveillance under this paragraph more than once during any consecutive 12 month period. This limitation does not apply to reactive and other forms of surveillance required under this subpart and the ONC–ACB's accreditation.

(d) *Reporting of surveillance results requirements*—(1) *Rolling submission of in-the-field surveillance results.* The results of in-the-field surveillance under this section must be submitted to the National Coordinator on an ongoing basis throughout the calendar year.

(2) *Confidentiality of locations evaluated.* The contents of an ONC–ACB's surveillance results submitted to the National Coordinator must not include any information that would identify any user or location that participated in or was subject to surveillance.

(3) *Reporting of corrective action plans.* When a corrective action plan is initiated for a Complete EHR or Health IT Module, an ONC–ACB must report the Complete EHR or Health IT Module (and its product identification information) to the National Coordinator in accordance with § 170.523(f)(1)(xix) or (f)(2)(ix), as applicable.

(e) *Relationship to other surveillance requirements.* Nothing in this section shall be construed to limit or constrain an ONC–ACB's general ability to perform surveillance, including in-the-field surveillance, on any certified Complete EHR or certified Health IT Module at any time, as determined appropriate by the ONC–ACB.

Dated: March 18, 2015.

Sylvia M. Burwell,

Secretary.

Note: The following appendix will not appear in the Code of Federal Regulations.

APPENDIX A—2015 EDITION HEALTH IT CERTIFICATION CRITERIA

Proposed CFR citation	Certification criterion	Estimated average developmental hours[270] av. low/av. high	Proposed privacy and security certification requirements[271] (Approach 1)	Conditional certification requirements (§ 170.550)	Gap certification eligibility	Proposed inclusion in 2015 edition base EHR definition	Relationship to the proposed CEHRT[272] definition and proposed EHR Incentive Programs Stage 3 objectives
§ 170.315(a)(1)	Computerized Provider Order Entry (CPOE)—medications.	0/50	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(1) § 170.314(a)(18)	Included[273]	Objective 4.
§ 170.315(a)(2)	CPOE—laboratory	1,000/2,000	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included[274]	Objective 4.
§ 170.315(a)(3)	CPOE—diagnostic imaging.	0/50	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(1) § 170.314(a)(20)	Included[275]	Objective 4.
§ 170.315(a)(4)	Drug-drug, Drug-allergy Interaction Checks for CPOE.	400/800	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 3.
§ 170.315(a)(5)	Demographics	500/1,000	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(a)(6)	Vital Signs, BMI, and Growth Charts.	614/922	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(a)(7)	Problem List	100/200	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(a)(8)	Medication List	0/50	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(6)	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(a)(9)	Medication Allergy List	0/50	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(7)	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(a)(10)	Clinical Decision Support	600/1,200	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included	Objective 3.
§ 170.315(a)(11)	Drug-formulary and Preferred Drug List Checks.	310/620	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 2.
§ 170.315(a)(12)	Smoking Status	100/200	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(a)(13)	Image Results	0/20	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(12)	Not included	No relationship.
§ 170.315(a)(14)	Family Health History	100/200	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	CEHRT.[276]
§ 170.315(a)(15)	Family Health History—pedigree.	500/1,200	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	CEHRT.[277]
§ 170.315(a)(16)	Patient List Creation	0/20	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(14)	Not included	No relationship.
§ 170.315(a)(17)	Patient-specific Education Resources.	600/1,200	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 5.
§ 170.315(a)(18)	Electronic Medication Administration Record.	0/20	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	§ 170.314(a)(16)	Not included	No relationship.
§ 170.315(a)(19)	Patient Health Information Capture.	500/1,000	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	CEHRT Objective 6.
§ 170.315(a)(20)	Implantable Device List	1,100/1,700	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(a)(21)	Social, Psychological, and Behavioral Data.	235/470	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(a)(22)	Decision Support—knowledge artifact.	394/788	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(a)(23)	Decision Support—service.	229/458	§ 170.315(d)(1) through (d)(7).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(b)(1)	Transitions of Care	1,550/3,100	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Included	Objective 7.
§ 170.315(b)(2)	Clinical Information Reconciliation and Incorporation.	600/1,200	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Not included	Objective 7.
§ 170.315(b)(3)	Electronic Prescribing	1,050/2,100	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 2.
§ 170.315(b)(4)	Incorporate Laboratory Tests and Values/Results.	313/626	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(b)(5)	Transmission of Laboratory Test Reports.	360/720	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(b)(6)	Data Portability	800/1,200	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Included	No additional relationship beyond the Base EHR Definition.
§ 170.315(b)(7)	Data Segmentation for Privacy—send.	450/900	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Not included	No relationship.

APPENDIX A—2015 EDITION HEALTH IT CERTIFICATION CRITERIA—Continued

Proposed CFR citation	Certification criterion	Estimated average developmental hours[270] av. low/av. high	Proposed privacy and security certification requirements[271] (Approach 1)	Conditional certification requirements (§ 170.550)	Gap certification eligibility	Proposed inclusion in 2015 edition base EHR definition	Relationship to the proposed CEHRT[272] definition and proposed EHR Incentive Programs Stage 3 objectives
§ 170.315(b)(8)	Data Segmentation for Privacy—receive.	450/900	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(b)(9)	Care Plan	300/500	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(c)(1)	Clinical Quality Measures—record and export.	200/500	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Included	CEHRT.
§ 170.315(c)(2)	Clinical Quality Measures—import and calculate.	0/200	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(c)(3)	Reserved for Clinical Quality Measures—record.	Reserved	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	Reserved	Reserved	Reserved.[278]
§ 170.315(c)(4)	Clinical Quality Measures—filter.	316/632	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(d)(1)	Authentication, Access Control, Authorization.	0/50	Not applicable (N/A)	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(1)	Not included	No relationship.
§ 170.315(d)(2)	Auditable Events and Tamper-resistance.	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(2)	Not included	No relationship.
§ 170.315(d)(3)	Audit Report(s)	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(3)	Not included	No relationship.
§ 170.315(d)(4)	Amendments	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(4)	Not included	No relationship.
§ 170.315(d)(5)	Automatic Access Time-out.	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(5)	Not included	No relationship.
§ 170.315(d)(6)	Emergency Access	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(6)	Not included	No relationship.
§ 170.315(d)(7)	End-User Device Encryption.	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(7)	Not included	No relationship.
§ 170.315(d)(8)	Integrity	0/50	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(8)	Not included	No relationship.
§ 170.315(d)(9)	Accounting of Disclosures	0/20	N/A	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(d)(9)	Not included	No relationship.
§ 170.315(e)(1)	View, Download, and Transmit to 3rd Party.	1,000/2,000	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(7).	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Not included	Objective 5 Objective 6.
§ 170.315(e)(2)	Secure Messaging	0/50	§ 170.315(d)(1) through (d)(3), (d)(5), and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(e)(3)	Not included	Objective 6.
§ 170.315(f)(1)	Transmission to Immunization Registries.	680/1,360	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.[279]
§ 170.315(f)(2)	Transmission to Public Health Agencies—syndromic surveillance.	480/960	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.
§ 170.315(f)(3)	Transmission to Public Health Agencies—reportable laboratory tests and values/results.	520/1,040	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.
§ 170.315(f)(4)	Transmission to Cancer Registries.	500/1,000	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.
§ 170.315(f)(5)	Transmission to Public Health Agencies—case reporting.	500/1,000	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.
§ 170.315(f)(6)	Transmission to Public Health Agencies—antimicrobial use and resistance reporting.	500/1,000	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.
§ 170.315(f)(7)	Transmission to Public Health Agencies—health care surveys.	500/1,000	§ 170.315(d)(1) through (d)(3) and (d)(7).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	Objective 8.
§ 170.315(g)(1)	Automated Numerator Recording.	400/800	N/A	§ 170.315(g)(4)	Fact-specific	Not included	CEHRT.
§ 170.315(g)(2)	Automated Measure Calculation.	600/1,200	N/A	§ 170.315(g)(4)	Fact-specific	Not included	CEHRT.
§ 170.315(g)(3)	Safety-Enhanced Design	300/600	N/A	N/A	Fact-specific	Not included	No relationship.
§ 170.315(g)(4)	Quality Management System.	400/800	N/A	N/A	Not eligible	Not included	No relationship.
§ 170.315(g)(5)	Accessibility Technology Compatibility.	800/1400	N/A	N/A	Not eligible	Not included	No relationship.
§ 170.315(g)(6)	Consolidated CDA Creation Performance.	400/1,000	N/A	N/A	Not eligible	Not included	No relationship.
§ 170.315(g)(7)	Application Access to Common Clinical Data Set.	500/1,000	N/A	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Included	Objective 5 Objective 6.
§ 170.315(g)(8)	Accessibility-Centered Design.	50/100	N/A	N/A	Not eligible	Not included	No relationship.
§ 170.315(h)(1)	Direct Project	0/50	§ 170.315(d)(1) through (d)(3).	§ 170.315(b)(1) § 170.315(g)(4) § 170.315(g)(8)	§ 170.314(b)(1)(i)(A) and § 170.314(b)(2)(ii)(A) § 170.314(h)(1)	Included[280]	No relationship beyond the Base EHR Definition.

APPENDIX A—2015 EDITION HEALTH IT CERTIFICATION CRITERIA—Continued

Proposed CFR citation	Certification criterion	Estimated average developmental hours[270] av. low/av. high	Proposed privacy and security certification requirements[271] (Approach 1)	Conditional certification requirements (§ 170.550)	Gap certification eligibility	Proposed inclusion in 2015 edition base EHR definition	Relationship to the proposed CEHRT[272] definition and proposed EHR Incentive Programs Stage 3 objectives
§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM.	0/50	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(b)(1)(i)(B), § 170.314(b)(2)(ii)(B), and § 170.314(b)(8)[281] 170.314(b)(8)[283] and 170.314(h)(2)	Included[282]	No relationship beyond the Base EHR Definition.
§ 170.315(h)(3)	SOAP Transport and Security Specification and XDR/XDR for Direct Messaging.	0/20	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	§ 170.314(b)(1)(i)(C) and § 170.314(b)(2)(ii)(C) § 170.314(h)(3)	Not included	No relationship.
§ 170.315(h)(4)	Healthcare Provider Directory—query request.	120/240	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(h)(5)	Healthcare Provider Directory—query response.	120/240	§ 170.315(d)(1) through (d)(3).	§ 170.315(g)(4) § 170.315(g)(8)	Not eligible	Not included	No relationship.
§ 170.315(j)(1)	Electronic Submission of Medical Documentation.	1000/200	§ 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8).	§ 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8)	Not eligible	Not included	No relationship.

[FR Doc. 2015–06612 Filed 3–20–15; 3:00 pm]

BILLING CODE 4150–45–P

[270] Please see section VIII (''Regulatory Impact Statement'') of the preamble for information on how estimated development hours were calculated. To note, certification to the 2014 Edition serves as a foundation for estimating costs. For unchanged certification criteria, in establishing our cost estimates for this proposed rule, we used burden hours multiplied by all health IT developers previously certified to the 2014 Edition version of the certification criteria to account for new entrants. These burden hour estimates are not estimates for development of a new product to meet one or more of these certification criteria. For certification criteria not associated with the EHR Incentive Programs Stage 3, there is a 60% reduction in burden hours. This reduction is due to our estimate that health IT developers would develop 1 product instead of 2.5 products to each of the certification criteria.

[271] We propose to require that an ONC–ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into the regulatory functional categories of § 170.315 for which privacy and security certification requirements apply either pursues approach 1 (detailed in the table) or approach 2: Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

[272] CMS' CEHRT definition would include the criteria adopted in the Base EHR definition. For more details on the CEHRT definition, please see the CMS EHR Incentive Programs proposed rule published elsewhere in this issue of the **Federal Register.**

[273] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[274] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[275] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[276] Technology needs to be certified to § 170.315(a)(14) or (a)(15).

[277] Technology needs to be certified to § 170.315(a)(14) or (a)(15).

[278] As discussed in the preamble for the ''clinical quality measures—report'' criterion, additional CQM certification policy may be proposed in or with CMS payment rules in CY15. As such, additional CQM certification criteria may be proposed for the Base EHR and/or CEHRT definitions.

[279] For the public health certification criteria in § 170.315(f), technology would only need to be certified to those criteria that are required to meet the options the provider intends to report in order to meet the proposed Objective 8: Public Health and Clinical Data Registry Reporting.

[280] Technology needs to be certified to § 170.315(h)(1) or (h)(2).

[281] Technology must have been certified to both edge protocol methods specified by the standard in § 170.202(d) to be gap certification eligible.

[282] Technology needs to be certified to § 170.315(h)(1) or (h)(2).

[283] Technology must have been certified to both edge protocol methods specified by the standard in § 170.202(d) to be gap certification eligible.