Test Procedure for §170.314 (e)(1) View, download, and transmit to a 3rd party

This document describes the test procedure for evaluating conformance of EHR technology to the certification criteria defined in 45 CFR Part 170 Subpart C of the 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, Final Rule. The document[1] is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at http://www.healthit.gov/certification (navigation: 2014 Edition Test Method). The test procedures may be updated to reflect on-going feedback received during the certification activities.

The Department of Health and Human Services (HHS)/Office of the National Coordinator for Health Information Technology (ONC) has defined the standards, implementation guides and certification criteria used in this test procedure. Applicability and interpretation of the standards, implementation guides and certification criteria to EHR technology is determined by ONC. Testing of EHR technology in the Permanent Certification Program, henceforth referred to as the ONC Health Information Technology (HIT) Certification Program[2], is carried out by National Voluntary Laboratory Accreditation Program (NVLAP)-Accredited Testing Laboratories (ATLs) as set forth in the final rule establishing the Permanent Certification Program (*Establishment of the Permanent Certification Program for Health Information Technology, 45 CFR Part 170; February 7, 2011*).

Questions or concerns regarding the ONC HIT Certification Program should be directed to ONC at ONC.Certification@hhs.gov.

CERTIFICATION CRITERIA

This certification criterion is from the 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, Final Rule issued by the Department of Health and Human Services (HHS) on September 4, 2012.

§170.314(e)(1) View, download, and transmit to 3rd party.

(i) EHR technology must provide patients (and their authorized representatives) with an online means to view, download, and transmit to a 3rd party the data specified below. Access to these capabilities must be through a secure channel that ensures all content is encrypted and integrity-

[1] Disclaimer: Certain commercial products may be identified in this document. Such identification does not imply recommendation or endorsement by ONC.

[2] 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, Final Rule.

protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f).

(A) View. Electronically view in accordance with the standard adopted at § 170.204(a), at a minimum, the following data:

(1) The Common MU 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.

(B) Download.

(1) Electronically download an ambulatory summary or inpatient summary (as applicable to the EHR technology setting for which certification is requested) in human readable format or formatted according to the standard adopted at § 170.205(a)(3) that includes, 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) and (e)(1)(i)(A)(2) of this section.

(ii) Inpatient setting only. All of the data specified in paragraphs (e)(1)(i)(A)(1) and (e)(1)(i)(A)(3) of this section.

(2) Inpatient setting only. Electronically 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)(2) of this section).

(C) Transmit to third party.

(1) Electronically transmit the ambulatory summary or inpatient summary (as applicable to the EHR technology setting for which certification is requested) created in paragraph (e)(1)(i)(B)(1) of this section in accordance with the standard specified in § 170.202(a).

(2) Inpatient setting only. Electronically 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 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, the following information must be recorded and made accessible to the patient:

(1) The action(s) (i.e., view, download, transmission) that occurred;

(2) The date and time each action occurred in accordance with the standard specified at § 170.210(g); and

(3) The user who took the action.

(B) EHR 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 § 170.314(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.

Per Section III.A of the preamble of the 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, Final Rule, the 2014 Edition of this Certification Criterion is classified as new from the 2011 Edition. This certification criterion meets at least one of the factors of new certification criteria: (1) The certification criterion only specifies capabilities that have never been included in previously adopted certification criteria; or, (2) The certification criterion was previously adopted as "mandatory" for a particular setting and subsequently adopted as "mandatory" or "optional" for a different setting.

2014 EDITION PREAMBLE LANGUAGE

Per Section III.A of the preamble of the 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, Final Rule where view, download, and transmit to a 3rd party certification criterion is discussed:

- "…this final rule requires that in order for EHR technology to be certified to a certification criterion that references "procedures" data, it must demonstrate compliance with the use of SNOMED CT® or CPT/HCPCS … However, in recognition that it may be beneficial for inpatient EHR technology developers to demonstrate compliance with, and support for the use of, ICD-10-PCS to represent procedures in the various certification criteria that reference procedures, we have adopted ICD-10-PCS as an "optional" vocabulary standard to which EHR technology developers can seek certification for their EHR technology."
- "In order to be certified, EHR technology must be capable of permitting a patient or their authorized representative access to all of the data specified by the certification criterion. What information is actually made available by an EP, EH, or CAH and how it is displayed to a patient or their authorized representative should be determined by the EP, EH or CAH."
- "We also clarify, as requested, that the WCAG standards apply to the information that is viewable to the patient or their authorized representative through the capabilities EHR technology includes that would enable them to electronically view, download, and transmit their health information to a 3rd party."
- "In order to demonstrate conformance with the certification criterion, EHR technology will need to meet WCAG Level A. So long as the EP, EH, or CAH (as the customer) can appropriately configure the EHR technology for the patient, then that is sufficient. The certification criterion does not specify that certain design elements be predefined or preset."
- "…in response to questions about the meaning of human readable, the use of a style sheet associated with a document formatted according to the Consolidated CDA would be permitted."
- "…the data itself must be downloaded and transmitted. A hyperlink to the data would not be sufficient for EHR technology to demonstrate compliance with this certification criterion."
- "…we clarify that, with respect to the Consolidated CDA, certification will not focus on a specific document-level template because none are particularly suited to support MU's policy objectives and the data elements specified across the different certification criteria that reference the

Consolidated CDA. Rather, certification will focus on an EHR technology's ability to properly implement the US Realm header and the associated section-level templates necessary to support each certification criterion in which the Consolidated CDA is referenced and for the appropriate data specified in each of those certification criteria."

- "…in all instances where we have adopted a vocabulary standard in § 170.207 the accompanying section-template implemented must be done so using the section-template with required structured data, coded entries required."
- "…we have finalized this portion [Activity Log] of the proposed certification criterion by changing the paragraph heading and making clear that the actions that need to be tracked are simply "views," "downloads," and/or "transmissions" that have occurred and by whom and when."

INFORMATIVE TEST DESCRIPTION

This section provides an informative description of how the test procedure is organized and conducted. It is not intended to provide normative statements of the certification requirements.

This test procedure evaluates the capabilities of EHR technology) to 1) allow patients and their authorized representatives to access their health information through a secure, online channel and to view, download, and transmit their health information to a third party; and 2) record the date and time when health information is viewed, downloaded, and transmitted, as well as the user who performed those actions.

The test procedure will evaluate that the Vendor's EHR technology provides secure, encrypted online access to health information for patients and authorized representatives to view, download, and transmit in accordance with Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2[i]. Encrypted online access will be verified by confirming that access was obtained using a secure connection (for example, browser access using HTTPS/TLS, inspection of web certificate to verify encryption settings).

EHR technology certified for 170.314(d)(2), Auditable Events and Tamper Resistance, is not required to include a separate capability for a patient accessible log in 170.314(e)(1)(ii)(A), if the EHR is able to provide patients with access to this information (log of the time, date, and users who view, download, and transmit patient health information).

The test procedure will evaluate the capability of the EHR technology to permit patients and their authorized representative(s) to view the ambulatory summary (provider's name and office contact information and Common MU Data Set) using ambulatory EHR technology; and the inpatient summary (admission and discharge dates and locations, discharge instructions, and reason(s) for hospitalization, and the Common MU Data Set) using inpatient EHR technology, in conformance with the Web Content Accessibility Guidelines (WCAG) 2.0, Level A Conformance standard (http://www.w3.org/TR/2008/REC-WCAG20-20081211/#conformance-reqs). Any capabilities of the EHR technology that permit patients and

their authorized representatives to download and transmit health information must also be in conformance with WCAG 2.0 Level A.

This test procedure will evaluate the capability of EHR technology to allow patients and their authorized representatives to electronically download an ambulatory or inpatient summary of the patient health information viewed in human readable format and in a format in conformance with the Consolidated CDA, with the English (that is, non-coded) representation if they associate with a vocabulary/code set. For the inpatient setting only, the EHR technology must also allow patients and authorized representatives to download a transition of care/referral summary [see (b)(2)] that was created as a result of a transition of care. The EHR technology must make a minimum of two types of documents available for download and transmission in the inpatient setting: an inpatient summary with a minimum of the required elements listed in the 170.314(e)(1) View, download and transmit to a 3rd party certification criterion; and inpatient transition of care/referral summaries that were created as a result of a transition of care with a minimum of the required elements listed in the 170.314(b)(2) Transitions of care - create and transmit summary care records certification criterion.

This test procedure will evaluate the capability of EHR technology to allow patients and authorized representatives to download and transmit the ambulatory summary for ambulatory EHRs, or for inpatient EHRs, the inpatient summary and transition of care/referral summary. EHRs must be able to provide these documents for download and transmit in both human readable format and in conformance with the Consolidated Clinical Document Architecture (C-CDA) standard. The transmission of the C-CDA and human readable document formats may occur as separate transactions or both documents may be transmitted within a single transmission. Accessibility of human readable information must be human readable within a single download and transmission per the ONC definition of human readable: “Human readable format means a format that enables a human to read and easily comprehend the information presented to him or her regardless of the method of presentation (e.g., computer screen, handheld device, electronic document).” For example, a C-CDA conformant document and an associated style sheet must be downloaded or transmitted together in a single transmission. If multiple documents are required for human readable format, these documents must be sent as separate attachments in any order within a single transmission. Vendors may provide additional attachments (e.g. XDM package) in the transmission if desired. These documents must be able to be transmitted to a third-party (by the patient and the patient’s authorized representative(s) in conformance with the ONC Applicability Statement for Secure Health Transport (Direct) specification to a third party.

In evaluating the capability of the EHR technology to transmit information to a third party, this test procedure will test the ability for EHR technology to correctly discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP using the Direct Certificate Discovery Tool (DCDT).

Using the Transport Testing Tool (TTT), this test procedure will verify that the Direct message is encrypted using the recipient’s Public Key and is signed using the sender’s Private Key. In keeping with the Direct specification, CEHRT must maintain an association with a supported address (sender or

recipient) and a collection of Trusted Anchors[3]. The TTT requires manual upload of Trust Anchors and certificates for testing purposes and is not linked to the DCDT at this time. The Trust Anchor uploaded to the TTT mimics the certificate discovery capability tested using the DCDT to support testing of transport capabilities. This test procedure will evaluate the capability of EHR technology to create a list of individual Direct recipients that can receive documents sent using Direct.

This test procedure will evaluate the capability of EHR technology to allow patients and authorized representatives to access activity history information about the health information that has been viewed, downloaded, and transmitted.

This test procedure will evaluate the conformance of web pages used to access and conduct view, download, and transmit functions using guidance on how to meet WCAG 2.0 from the World Wide Web Consortium (W3C). As all test tools listed on the W3C site do not adequately test all applicable success criteria, multiple tools, including tools other than those published by W3C, may need to be selected to support all applicable success criteria. This test procedure will evaluate the submitted results of conformance testing tools and evaluate aspects of conformance from Items 1-5 of WCAG2.0 Conformance not verified by testing tools - http://www.w3.org/TR/2008/REC-WCAG20-20081211/#conformance-reqs. WCC provides WCAG 2.0 guidance at:

- WCAG Overview http://www.w3.org/WAI/intro/wcag
- WCAG 2 at a Glance http://www.w3.org/WAI/WCAG20/glance/
- How to Meet WCAG 2.0: A customizable quick reference http://www.w3.org/WAI/WCAG20/quickref/

This test procedure includes a Network Time Protocol (NTP) test to verify synchronization of the EHR and the system clock to the named standards, (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4.

ONC provides the test data for this test procedure. This test procedure is organized into five sections:

- View Health Information – Evaluates the capability for the EHR to provide patients and authorized representatives a secure, electronic view of the following information:
    - For both ambulatory and inpatient settings: the Common MU Data Set data with named standards as appropriate (in their English representation if they associate with a vocabulary/code set):
        1) Patient name
        2) Sex
        3) Date of birth
        4) Race
        5) Ethnicity

[3] Section 4.2.3 of the ONC Applicability Statement for Secure Health Transport: "Each implementation MUST maintain an association with a supported address (sender or recipient) and a collection of Trusted Anchors. The address trusts any valid leaf certificate whose certificate chain contains at least one certificate from the address's Anchor list."

6) Preferred language
7) Smoking status
8) Problems
9) Medications
10) Medication Allergies
11) Laboratory test(s)
12) Laboratory value(s)/result(s)
13) Vital signs – height, weight, blood pressure, BMI
14) Care plan field(s), including goals and instructions
15) Procedures
16) Care team member(s)

- For ambulatory settings only: the provider's name and office contact information
- For inpatient settings only: admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization
- The Vendor creates an existing patient record in the EHR technology with health information based on the ONC-provided test data
- Tester, logs into the online application as a patient (and authorized representative) and electronically views information relevant to inpatient and/or ambulatory settings
- Tester verifies all required information can be viewed
  - Tester verifies the information associated with a vocabulary/code set in human readable format is its in English representation (description)
- The Vendor tells the Tester which authentication method(s) and which encryption and hashing 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) the Vendor is using for this test
- Tester verifies the ability for an authorized patient representative to log into the online application and view the same information viewed by the patient

- Download Health Information – Evaluates the capability to electronically download the information that was viewed as part of the "View" step in a human readable format and a format in accordance with the Implementation Guide for CDA® Release 2.0, Consolidated CDA Templates
  - The Tester remains logged into EHR technology's online channel established in the previous "View" step
  - Using the Vendor-identified EHR function(s) in the EHR's online technology and the provided test data, the Tester causes the EHR to download the health information viewed in the "View" step as an ambulatory or inpatient summary; and in inpatient settings only, a transition of care/referral summary created as a result of a transition of care
  - The Tester validates that the downloaded health information is in human readable format and in C-CDA format
  - The Tester imports the downloaded C-CDA clinical summary into the Transport Testing Tool
  - Using the Validation Report produced by the C-CDA Transport Testing Tool, the Tester verifies that the Implementation Guide conformance requirements tested are met, and that

the named standard vocabularies have been used where applicable in the required test data elements

- Tester verifies the health information is downloaded through a secure channel that ensures all information is encrypted and integrity protected in compliance with Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 [170.210(f)]

- Transmit – Evaluates the capability of EHR technology to allow a patient and a patient's authorized representative to electronically transmit the health information available for download in the "Download" section of the test procedure to a third party as an ambulatory or inpatient summary (as applicable to the setting for which the EHR technology will be tested); and for inpatient settings only, a transition of care/referral summary
  - The Tester logs in to the EHR's online technology as the patient who downloaded the information from the "View" step in the "Download" step
  - The Tester verifies that the EHR can discover certificates from other parties in DNS CERT records and LDAP servers[4]
  - Using the Vendor-identified function(s), the Tester verifies that the EHR is able to create and store a listing of Direct recipient address(es) (This may be accomplished as a system administration function and is not required to be an end-user capability.)
  - Using the Vendor-identified function(s), the Tester causes the health information available for download in human readable format and C-CDA format to be transmitted to a third party using the Direct transport standard, based on ONC supplied test information
  - The Tester verifies successful transmission and receipt of the health information, and that the health information can be successfully decrypted
  - The Tester verifies that the information transmitted is in conformance with the C-CDA
    - Using the Vendor-identified EHR function(s), the Tester imports the health information into the NIST Transport Test Tool
    - Using the Validation Report produced by the NIST Transport Test Tool, the Tester verifies that the Implementation Guide conformance requirements tested are met, and that the named standard vocabularies have been used where applicable for data in the required test data elements
  - Using the provided test data, the Tester verifies that the data rendered in the transmitted human readable and C-CDA conformant documents are complete and accurate, and that the required data elements are shown in their English representation (description) if they associate with a vocabulary/code set

- Record and Display Actions – Evaluate the capability of the EHR technology to capture date, time, and user who views, downloads, and transmits health information and make it accessible to the patient (and their authorized representative)

[4] Section 2.3 of the ONC Applicability Statement for Secure Health Transport v1.1: "For universal digital certificate distribution, STAs MUST be able to discover certificates using both the DNS as specified in Section 5 of this applicability statement and LDAP as described by the S&I Framework Certificate Discovery for Direct Project Implementation Guide."

- The Vendor creates a test patient record that includes, at a minimum, the health information, based on ONC-supplied test data
- For each instance of view, download, and transmit of health information conducted previously in this test procedure:
  - Tester verifies that the action of viewed [downloaded/transmitted] information is recorded and conformant with the named security protocols and standards, and that the information was viewed/downloaded/transmitted is complete and accurate (Viewing of at least one item of the Ambulatory/Inpatient Summary should cause an action to be recorded in the activity history log)
  - Tester verifies recorded action, with user information and date/time of the action is accessible to the patient (via access to audit log information or other capability)

- Submit and Verify Summative Testing Results for WCAG Conformance – Evaluates Vendor-supplied documentation of referenced practice, testing tools, tool results, and accompanying documentation to ensure the Vendor has achieved conformance with Web Content Accessibility Guidelines (WCAG) 2.0 Level "A" for each EHR technology capability submitted for testing for viewing of health information by a patient and their authorized representative
  - The Tester will verify that for each EHR technology capability submitted for testing for viewing, downloading, and transmitting of health information, the Vendor has defined the scope and use of web pages for testing
  - The Tester will verify that each web page associated with a "WCAG2.0-conformant version" of EHR functionality to view, download, and transmit health information is includes submitted documentation for WCAG Level "A" conformance
  - The Tester shall examine each Vendor-provided report to ensure the existence and adequacy of test report(s) submitted by the vendor
  - The Tester shall inspect the acceptability of the following reporting areas:
    - Web pages associated with "WCAG2.0-conformant version" of related functionality
    - Tool(s) used to test each web page
    - Results/outputs of each tool
    - Description of Pass/Fail scoring for applicable web pages
    - Description of rationale for over-ruling of any tool output
    - Description of aspects of conformance not verified using testing tools
    - Report of evaluation findings

  Note: This Test Procedure evaluates conformance to the WCAG 2.0 Level "A" standard. Any additional links or documents referenced in the test procedure that are not normative aspects of the WCAG 2.0 Level "A" standard are provided only as additional resources and will not result in failure of this test if not met by the Vendor.

REFERENCED STANDARDS

§170.202 Transport standards.	Regulatory Referenced Standard
The Secretary adopts the following transport standards:	
(a) Standard. ONC Applicability Statement for Secure Health Transport (incorporated by reference in § 170.299).	

§170.204 Functional standards.	Regulatory Referenced Standard
The Secretary adopts the following functional standards:	
(a) Accessibility. Standard. Web Content Accessibility Guidelines (WCAG) 2.0, Level A Conformance (incorporated by reference in § 170.299).	

§170.205 Content exchange standards and implementation specifications for exchanging electronic health information.	Regulatory Referenced Standard
The Secretary adopts the following content exchange standards and associated implementation specifications:	
(a)(3) Standard. HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, (incorporated by reference in § 170.299). The use of the "unstructured document" document-level template is prohibited.	

§170.207 Vocabulary standards for representing electronic health information.	Regulatory Referenced Standard
The Secretary adopts the following code sets, terminology, and nomenclature as the vocabulary standards for the purpose of representing electronic health information:	
(a)(3) Standard. IHTSDO SNOMED CT® International Release July 2012 (incorporated by reference in § 170.299) and US Extension to SNOMED CT® March 2012 Release (incorporated by reference in § 170.299).	
(b)(2) Standard. The code set specified at 45 CFR 162.1002(a)(5).	45 CFR 162.1002 Medical data code sets The Secretary adopts the following code set maintaining organization's code sets as the standard medical data code sets: (a) International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2 (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions: (5) The combination of *Health Care Financing Administration Common Procedure Coding System (HCPCS),* as maintained and distributed by HHS, and *Current Procedural Terminology, Fourth Edition (CPT–4),* as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following:
(b)(3) Standard. The code set specified at 45 CFR 162.1002(a)(4).	45 CFR 162.1002 Medical data code sets The Secretary adopts the following code set maintaining organization's code sets as the standard medical data code sets: (a) International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2 (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions: (4) *Code on Dental Procedures and Nomenclature,* as maintained and distributed by the American Dental Association, for dental services.

§170.207 Vocabulary standards for representing electronic health information.	Regulatory Referenced Standard
(4) Standard. The code set specified at 45 CFR 162.1002(c)(3) for the indicated procedures or other actions taken.	45 CFR 162.1002 Medical data code sets The Secretary adopts the following code set maintaining organization's code sets as the standard medical data code sets: (c)(3) International Classification of Diseases, 10th Revision, Procedure Coding System (ICD–10–PCS) (including The Official ICD–10–PCS Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals: (i) Prevention. (ii) Diagnosis. (iii) Treatment. (iv) Management.
(c) Laboratory tests. (2) Standard. Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.40, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (incorporated by reference in § 170.299).	
(d) Medications. (2) Standard. RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine, August 6, 2012 Release (incorporated by reference in § 170.299).	
(e) Immunizations. (2) Standard. HL7 Standard Code Set CVX -- Vaccines Administered, updates through July 11, 2012 (incorporated by reference in § 170.299).	
(f) Race and Ethnicity. 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 (see "Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity," available at http://www.whitehouse.gov/omb/fedreg_1997standards).	
(g) Preferred language. 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).	
(h) Smoking status. Standard. Smoking status must be coded in one of the following SNOMED CT® codes: (1) Current every day smoker. 449868002 (2) Current some day smoker. 428041000124106 (3) Former smoker. 8517006 (4) Never smoker. 266919005 (5) Smoker, current status unknown. 77176002 (6) Unknown if ever smoked. 266927001 (7) Heavy tobacco smoker. 428071000124103 (8) Light tobacco smoker. 428061000124105	

§170.207 Vocabulary standards for representing electronic health information.	Regulatory Referenced Standard
Encounter diagnoses. Standard. The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions.	45 CFR 162.1002 Medical data code sets. The Secretary adopts the following maintaining organization's code sets as the standard medical data code sets: (c)(2) International Classification of Diseases, 10th Revision, Clinical Modification (ICD–10–CM) (including The Official ICD–10–CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions: (i) Diseases. (ii) Injuries. (iii) Impairments. (iv) Other health problems and their manifestations. (v) Causes of injury, disease, impairment, or other health problems.

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged	Regulatory Referenced Standard
The Secretary adopts the following standard to protect electronic health information created, maintained, and exchanged:	
(f) Encryption and hashing of electronic health information. Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the FIPS Publication 140-2 (incorporated by reference in § 170.299).	
(g) Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in § 170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in § 170.299).	

REFERENCED CERTIFICATION CRITERIA

§170.314 2014 Edition electronic health record certification criteria.	Referenced Standards
The Secretary adopts the following certification criteria for Complete EHRs or EHR Modules. Complete EHRs or EHR Modules must include the capability to perform the following functions electronically, unless designated as optional, and in accordance with all applicable standards and implementation specifications adopted in this part:	

§170.314 2014 Edition electronic health record certification criteria.	Referenced Standards
(b)(2) Transitions of care - create and transmit summary care records. (i) Create. Enable a user to electronically create a transition of care/referral summary formatted according to the standard adopted at § 170.205(a)(3) that includes, at a minimum, the Common MU Data Set and the following data expressed, where applicable, according to the specified standard(s): (A) Encounter diagnoses. The standard specified in § 170.207(i) or, at a minimum, the version of the standard specified § 170.207(a)(3); (B) Immunizations. The standard specified in § 170.207(e)(2); (C) Cognitive status; (D) Functional status; and (E) Ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information. (F) Inpatient setting only. Discharge instructions.	See Referenced Standards section for associated standards

§170.314 2014 Edition electronic health record certification criteria.	Referenced Standards
(d)(2) Auditable events and tamper-resistance. (i) Record actions. EHR 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 EHR technology in accordance with the standard specified in § 170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see 170.314(d)(7) of this section). (ii) Default setting. EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (d)(2)(i)(C), 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), (B), and (C) of this section that EHR technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users. (iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) must not be capable of being changed, overwritten, or deleted by the EHR technology. (v) Detection. EHR technology must be able to detect whether the audit log has been altered.	§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged. The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged: (e)(1) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (i) The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified at § 170.210(h) when EHR technology is in use. (ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g). (e)(2) (i) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at § 170.210(h) when the audit log status is changed. (ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g). (e)(3)The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at § 170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at § 170.210(g). (g) Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in § 170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in § 170.299). (h) Audit log content. ASTM E2147-01 (Reapproved 2009), (incorporated by reference in § 170.299).

NORMATIVE TEST PROCEDURES

Network Time Protocol (NTP) Test

The test steps below must be performed by the Vendor and the results validated by the Tester prior to beginning the test steps in the Derived Test Requirements.

NTP170.314(e)(1) – 1.01: The Vendor shall choose a time server from the list below, used by the NIST Internet Time Service (ITS), and shall add it to their NTP software configuration

Note: All users should ensure that their software NEVER queries a server more frequently than once every 4 seconds. Systems that exceed this rate will be refused service. In extreme cases, systems that exceed this limit may be considered as attempting a denial-of-service attack.

Name	IP Address	Location
nist1-ny.ustiming.org	64.90.182.55	New York City, NY
nist1-nj.ustiming.org	96.47.67.105	Bridgewater, NJ
nist1-pa.ustiming.org	206.246.122.250	Hatfield, PA
time-a.nist.gov	129.6.15.28	NIST, Gaithersburg, Maryland
time-b.nist.gov	129.6.15.29	NIST, Gaithersburg, Maryland
nist1.aol-va.symmetricom.com	64.236.96.53	Reston, Virginia
nist1.columbiacountyga.gov	216.119.63.113	Columbia County, Georgia
nist1-atl.ustiming.org	64.250.177.145	Atlanta, Georgia
nist1-chi.ustiming.org	216.171.120.36	Chicago, Illinois
nist-chicago (No DNS)	38.106.177.10	Chicago, Illinois
nist.time.nosc.us	96.226.123.117	Carrollton, Texas
nist.expertsmi.com	50.77.217.185	Monroe, Michigan
nist.netservicesgroup.com	64.113.32.5	Southfield, Michigan
nisttime.carsoncity.k12.mi.us	66.219.116.140	Carson City, Michigan
nist1-lnk.binary.net	216.229.0.179	Lincoln, Nebraska
wwv.nist.gov	24.56.178.140	WWV, Fort Collins, Colorado
time-a.timefreq.bldrdoc.gov	132.163.4.101	NIST, Boulder, Colorado
time-b.timefreq.bldrdoc.gov	132.163.4.102	NIST, Boulder, Colorado
time-c.timefreq.bldrdoc.gov	132.163.4.103	NIST, Boulder, Colorado
time.nist.gov	global address for all servers	Multiple locations
utcnist.colorado.edu	128.138.140.44	University of Colorado, Boulder
utcnist2.colorado.edu	128.138.141.172	University of Colorado, Boulder
ntp-nist.ldsbc.edu	198.60.73.8	LDSBC, Salt Lake City, Utah

nist1-lv.ustiming.org	64.250.229.100	Las Vegas, Nevada
time-nw.nist.gov	131.107.13.100	Microsoft, Redmond, Washington
nist-time-server.eoni.com	216.228.192.69	La Grande, Oregon
nist1.aol-ca.symmetricom.com	207.200.81.113	Mountain View, California
nist1.symmetricom.com	69.25.96.13	San Jose, California
nist1-sj.ustiming.org	216.171.124.36	San Jose, California
nist1-la.ustiming.org	64.147.116.229	Los Angeles, California

NTP170.314(e)(1) – 1.02: After configuring NTP, the Vendor shall wait the amount of time necessary to ensure synchronization occurs

NTP170.314(e)(1) – 1.03: Using the NTP logs, the Vendor and Tester shall verify that the system time is accurate within five seconds of the NIST time server chosen in NTP170.314(e)(1) – 1.01

NTP170.314(e)(1) – 1.04: The Vendor shall construct or use an existing display in the EHR system that shows the time from the system clock and the EHR time for comparison (these times should be synchronized to within five seconds)

NTP170.314(e)(1) – 1.05: The Tester shall verify, via the NTP logs, that the system time is synchronized to the NIST time server to within five seconds; and then the Tester shall verify, via the EHR display, that the EHR time is synchronized to the system time to within five seconds

NTP170.314(e)(1) – 1.06: The Vendor shall identify the protocol used for synchronizing the EHR system clock (i.e., (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4)

The test procedure assumes the operating system synchronizes to the NTP server and the EHR then synchronizes to the operating system; however, the EHR could synchronize directly to the NTP server. The EHR technology may use either method to demonstrate that the synchronization has occurred. Use of internal NTP servers are allowed, but the EHR technology must demonstrate that the internal servers are synced to a NIST timeserver for accuracy.

Derived Test Requirements

DTR170.314(e)(1) – 1: View Health Information

DTR170.314(e)(1) – 2: Download Health Information

DTR170.314(e)(1) – 3: Transmit Health Information to a Third Party Using Direct

DTR170.314(e)(1) – 4: Record and Display Actions

DTR170.314(e)(1) – 5: Submit and Verify Summative Testing Results for WCAG Conformance

DTR170.314(e)(1) – 1: View Health Information

Required Vendor Information

VE170.314(e)(1) – 1.01: Using ONC-supplied test data, the Vendor shall create a test patient with an existing record in the EHR to be used for this test as indicated in TD170.314(e)(1) – Ambulatory (ambulatory only) or TD170.314(e)(1) – Inpatient (inpatient only)

VE170.314(e)(1) – 1.02: Vendor shall identify a patient with the ability to access records online

VE170.314(e)(1) – 1.03: Vendor shall identify an authorized patient representative with access to the patient's health information online (patient identified in VE170.314(e)(1) – 1.02)

VE170.314(e)(1) – 1.04: Vendor shall identify a user who is not an authorized patient representative and does not have access to the patient's health information online (patient identified in VE170.314(e)(1) – 1.02)

VE170.314(e)(1) – 1.05: Vendor shall identify the EHR function(s) that are available for a patient (and their authorized representative) to view health information including the named data elements as well as the Common MU Data Set with associated vocabulary standards

VE170.314(e)(1) – 1.06: The Vendor shall identify the authentication methods and the encryption and hashing algorithm from Annex A of FIPS 140-2 to be used for this test (e.g. Encrypted online access may be verified by confirming that access was obtained using a secure connection (browser access using HTTPS/TLS, inspection of web certificate to verify encryption settings, etc.))

Required Test Procedure

TE170.314(e)(1) – 1.01: Using the Vendor-identified EHR function(s), the Tester shall access the ONC-supplied test patient's record as the patient

TE170.314(e)(1) – 1.02: Using the Vendor-identified EHR function(s), the Tester shall view patient information (and record the user, date, time. and action performed) that includes:

- Ambulatory Summary: Common MU Data Set and the following data elements: provider's name and office contact information (Ambulatory EHR Only)
- Inpatient Summary: Common MU Data Set and the following data elements: admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization (Inpatient EHR Only)

TE170.314(e)(1) – 1.03: Using the Inspection Test Guide, the Tester shall verify that the summary information is complete and accurate and in accordance with TD170.314(e)(1) – Ambulatory (ambulatory only) or TD170.314(e)(1) – Inpatient (inpatient only)

TE170.314(e)(1) – 1.04: Using the Vendor-identified EHR function(s), the Tester shall access the ONC-supplied test patient's record as an authorized patient representative

TE170.314(e)(1) – 1.05: Using the Vendor-identified EHR function(s), the Tester shall be prevented from accessing the ONC-supplied test patient's record as an unauthorized patient representative

TE170.314(e)(1) – 1.06: Using the Vendor-identified EHR function(s), the Tester shall access the patient information viewed in TE170.314(e)(1) – 1.02

TE170.314(e)(1) – 1.07: Using the Inspection Test Guide, the Tester shall verify that the summary information is complete and accurate

Inspection Test Guide

IN170.314(e)(1) – 1.01: Using the ONC-provided test data, the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that the patient's ambulatory summary is created in human readable format, including, at a minimum, the following data elements (Ambulatory Only):

1) Provider's name
2) Provider's office contact information
3) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language
    7) Smoking status
    8) Problems
    9) Medications
    10) Medication Allergies
    11) Laboratory test(s)
    12) Laboratory value(s)/result(s)
    13) Vital signs – height, weight, blood pressure, BMI
    14) Care plan field(s), including goals and instructions
    15) Procedures
    16) Care team member(s)

IN170.314(e)(1) – 1.02: Using the ONC-provided test data, the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that the patient's inpatient summary is created in human readable format, including, at a minimum, the following data elements (Inpatient Only):

1) Patient admission date
2) Patient discharge date
3) Admission/discharge location
4) Discharge instructions
5) Reason(s) for hospitalization

6) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language
    7) Smoking status
    8) Problems
    9) Medications
    10) Medication Allergies
    11) Laboratory test(s)
    12) Laboratory value(s)/result(s)
    13) Vital signs – height, weight, blood pressure, BMI
    14) Care plan field(s), including goals and instructions
    15) Procedures
    16) Care team member(s)

IN170.314(e)(1) – 1.03: The Tester shall verify that only authorized patient representatives are able to access a patient's record, and that unauthorized patient representatives are prevented from accessing a patient's health information

DTR170.314(e)(1) – 2: Download Health Information

Required Vendor Information

VE170.314(e)(1) – 2.01: As defined in DTR170.314(e)(1) – 1, no additional information is required

Required Test Procedure

TE170.314(e)(1) – 2.01: Using the Vendor-identified EHR function(s), the Tester shall access the ONC-supplied test patient's record as the patient

TE170.314(e)(1) – 2.02: Using the Vendor-identified EHR function(s), the Tester shall cause the EHR to download patient information (and record the user, date, time. and action performed) in a human-readable format that includes:

- Ambulatory Summary: Common MU Data Set and the following data elements: provider's name and office contact information (Ambulatory EHR Only)
- Inpatient Summary: Common MU Data Set and the following data elements: admission and discharge dates and locations; discharge instructions; and reason(s) for hospitalization (Inpatient EHR Only)
- Inpatient Referral Summary/Transition of Care: Common MU Data Set and the following data elements: Encounter diagnoses, Immunizations, Cognitive status, Functional status and Discharge instructions (Inpatient EHR Only)

TE170.314(e)(1) – 2.03: Using the Vendor-identified EHR function(s), the Tester shall cause the EHR to download the patient information downloaded in TE1701.314(e)(1)-2.02 according to the Consolidated CDA standard and named vocabulary standards for the following data elements indicated in TE1701.314(e)(1)-2.02 and record the user, date, time, and action performed

TE170.314(e)(1) – 2.04: The Vendor shall provide the Tester with the C-CDA document(s) downloaded in TE170.314(e)(1)-2.03 for the Tester to validate C-CDA conformance using the C-CDA Document Validator within the Transport Testing Tool

TE170.314(e)(1) – 2.05: Using the Inspection Test Guide, the Tester shall verify that the (Ambulatory or Inpatient) summary and Referral Summary/Transition of Care (Inpatient Only) is downloaded in human readable format, and is complete and accurate

TE170.314(e)(1) – 2.06: Using the Inspection Test Guide, the Tester shall verify that the (Ambulatory or Inpatient) summary and Referral Summary/Transition of Care (Inpatient Only) is downloaded according to the Consolidated CDA standard tested and the named vocabulary standards, and is complete and accurate

Inspection Test Guide

IN170.314(e)(1) – 2.01: Using the ONC-provided test data, the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that the patient's ambulatory summary is downloaded in human readable format, including, at a minimum, the following data elements (Ambulatory Only):

1) Provider's name
2) Provider's office contact information
3) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language
    7) Smoking status
    8) Problems
    9) Medications
    10) Medication Allergies
    11) Laboratory test(s)
    12) Laboratory value(s)/result(s)
    13) Vital signs – height, weight, blood pressure, BMI
    14) Care plan field(s), including goals and instructions
    15) Procedures
    16) Care team member(s)

IN170.314(e)(1) – 2.02: Using the ONC-provided test data, the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that the patient's inpatient summary is downloaded in human readable format, including, at a minimum, the following data elements (Inpatient Only):

1) Patient admission date
2) Patient discharge date
3) Admission/discharge location
4) Discharge instructions
5) Reason(s) for hospitalization
6) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language
    7) Smoking status
    8) Problems
    9) Medications
    10) Medication Allergies
    11) Laboratory test(s)
    12) Laboratory value(s)/result(s)
    13) Vital signs – height, weight, blood pressure, BMI
    14) Care plan field(s), including goals and instructions
    15) Procedures
    16) Care team member(s)

IN170.314(e)(1) – 2.03: Using the ONC-provided test data the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, the Tester shall verify that the patient's Referral Summary/Transition of Care is downloaded in human readable format, including, at a minimum, the following data elements (Inpatient Only):

1) Encounter diagnoses
2) Immunizations
3) Cognitive status
4) Functional status
5) Discharge instructions
6) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name

2) Sex
3) Date of birth
4) Race
5) Ethnicity
6) Preferred language
7) Smoking status
8) Problems
9) Medications
10) Medication Allergies
11) Laboratory test(s)
12) Laboratory value(s)/result(s)
13) Vital signs – height, weight, blood pressure, BMI
14) Care plan field(s), including goals and instructions
15) Procedures
16) Care team member(s)

IN170.314(e)(1) – 2.04: The Tester may need to parse the .xml and use the MIME part to inspect the header to identify the C-CDA documents (vs. style sheet)

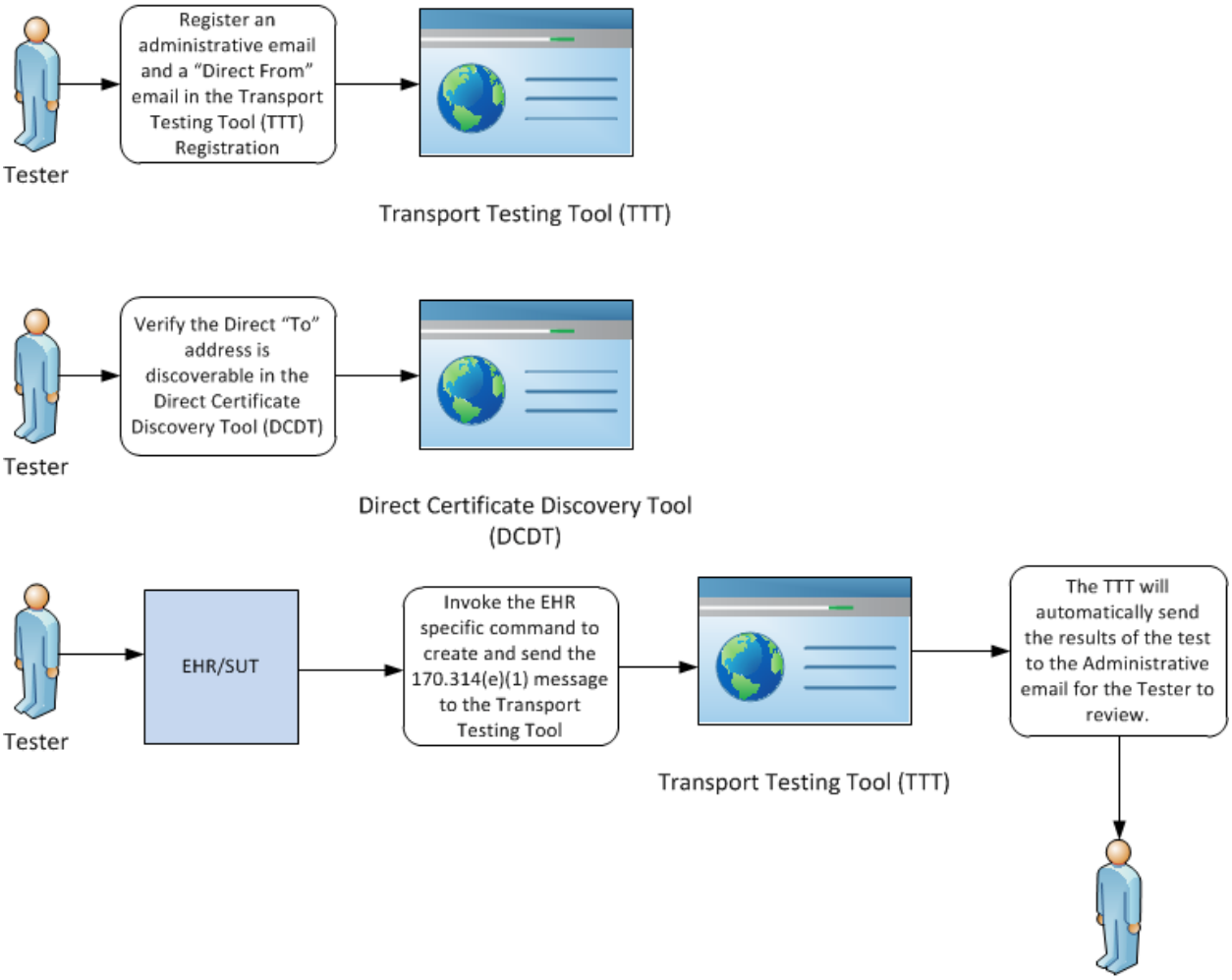
IN170.314(e)(1) – 2.05: Using the provided test data, the Vendor-identified authentication method, the Vendor-identified encryption and hashing algorithm, and the NIST-identified encryption and hashing algorithms listed as an approved security function in Annex A of the FIPS Publication 140-2, and the results of the C-CDA Document Validator within Transport Testing Tool identified in the Conformance Test Tools section of this test procedure**,** the Tester shall verify that

- The C-CDA Implementation Guide conformance requirements tested are met by the electronically generated (Ambulatory/Inpatient) summary and Transition of Care/Referral Summary (Inpatient Only)
- The standards for the named vocabularies for the Common MU Data Set are met by the electronically generated summary (Ambulatory/Inpatient) and Transition of Care/Referral Summary (Inpatient Only)

IN170.314(e)(1) – 2.06: Using the ONC-provided test data, the Tester shall visually inspect the C-CDA .xml to verify that the content of the C-CDAs is complete and accurate

DTR170.314(e)(1)–3: Transmit Health Information to a Third Party Using Direct

Figure 1



Required Vendor Information

VE170.314(e)(1) – 3.01: The Vendor shall identify a Direct address and a registered domain for sending of Direct messages for certificate discovery testing for enabling of testing using the Direct Certificate Discovery Tool

VE170.314(e)(1) – 3.02: The Vendor shall identify a non-Direct email address to be used for delivery of results of certificate discovery testing for enabling of testing using the Direct Certificate Discovery Tool

VE170.314(e)(1) – 3.03: The Vendor shall identify a Contact Email address to be used for receipt of the validation report generated by the Transport Testing Tool

VE170.314(e)(1) – 3.04: The Vendor shall identify the Direct address for registering within the Transport Testing Tool

VE170.314(e)(1) – 3.05: The Vendor shall obtain the Transport Testing Tool's Public Key and Trust Anchor from the Transport Testing Tool and store it within EHR technology for encrypting Direct message(s) to be sent to the 3rd party[5]

VE170.314(e)(1) – 3.06: The Vendor shall identify its signing certificate to sign message content with its Private Key and include the Public Key in messages sent to the Transport Testing Tool

Required Test Procedures

TE170.314(e)(1) – 3.01: The Tester shall download the Direct Certificate Discovery Tool's Trust Anchor and import it into the EHR technology's trust store

TE170.314(e)(1) – 3.02: The Tester shall use the Direct (From) address provided in VE170.314(e)(1)-3.01 to execute the test using the Direct Certificate Discovery Tool

TE170.314(e)(1) – 3.03: The Tester shall use the non-Direct email address provided in VE170.314(e)(1)-3.02 for receipt and validation of results of certificate discovery testing

TE170.314(e)(1) – 3.04: The Tester shall execute all test cases within the Direct Certificate Discovery Tool

TE170.314(e)(1) – 3.05: Using the Inspection Test Guide, the Tester shall verify that the EHR technology is able to correctly discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP

TE170.314(e)(1) – 3.06: The Tester shall cause the EHR to register the Direct (To) addresses specified in the Transport Testing Tool (to be available as a recipient for sending of Direct messages within the EHR)

TE170.314(e)(1) – 3.07: The Tester shall cause the EHR to transmit human readable document(s) using ONC Applicability Statement for Secure Health Transport (Direct) standard (and record the user, date, time. and action performed) to the Direct (To) address(es) specified in the Transport Testing Tool that are available within the EHR following TE170.e.1 – 3.07. The Direct message shall be encrypted using the recipient's (Transport Testing Tool) Public Key obtained in VE170.314(e)(1) – 3.05 and signed using the sender's (Vendor) Private Key:

- Ambulatory: Ambulatory Summary available for download or downloaded in TE170.314(e)(1) – 2.02
- Inpatient: Inpatient Summary and Referral Summary/Transition of Care document available for download or downloaded in TE170.314(e)(1) – 2.02

TE170.314(e)(1) – 3.08: The Tester shall cause the EHR to transmit Consolidated CDA document(s) using ONC Applicability Statement for Secure Health Transport (Direct) standard to the Direct (To) address(es) specified in the Transport Testing Tool (and record the user, date, time. and action performed). The Direct message shall be encrypted using the recipient's (Transport Testing Tool) Public Key

[5] When the test procedure refers to the Transport Testing Tool's trust anchor and certificates, this refers to NIST hosted version on transport-testing.nist.gov. If your organization is hosting its own version of Transport Testing Tool (TTT), then you will need to create your own trust anchor certificates and use these instead. For example, the trust anchor for "hit-testing.nist.gov", may change to "ttt.yourdomain.com".

obtained in VE170.314(e)(1) – 3.07 and signed using the sender's (Vendor) Private Key:

- Ambulatory: Ambulatory Summary available for download or downloaded in TE170.314(e)(1) – 2.03
- Inpatient: Inpatient Summary and Referral Summary/Transition of Care document available for download or downloaded in TE170.314(e)(1) – 2.03

TE170.314(e)(1) – 3.09: Using the Inspection Test Guide, the Tester shall verify that the (Ambulatory or Inpatient) summary and Referral Summary/Transition of Care (Inpatient Only) is transmitted in human readable format, and is complete and accurate

TE170.314(e)(1) – 3.10: Using the Inspection Test Guide, the Tester shall verify that the (Ambulatory or Inpatient) summary and Referral Summary/Transition of Care (Inpatient Only) is transmitted according to the Consolidated CDA standard tested and the named vocabulary standards, and is complete and accurate

Inspection Test Guide

IN170.314(e)(1) – 3.01: Using the Direct Certificate Discovery Tool, the Tester shall inspect the results received via email to verify that all test cases were successful

IN170.314(e)(1) – 3.02: The Tester shall verify the appropriate Direct (To) address(es) (provided within the Transport Testing Tool) have been registered within the EHR technology and are visible Direct addresses for transmitting of health information to the Transport Testing Tool according to the ONC Applicability Statement for Secure Health Transport (Direct) standard

IN170.314(e)(1) – 3.03: Using the Transport Testing Tool, the Tester shall verify that the transmitted human readable document(s) and C-CDA document(s) have been transmitted and received successfully according to the ONC Applicability Statement for Secure Health Transport (Direct) standard, including successful decryption validation (Note: the human readable and C-CDA documents may be transmitted using the Direct standard in a single transmission or separate transmissions. If multiple documents are required for human readable format, all documents must be sent as separate attachments within a single transmission).

IN170.314(e)(1) – 3.04: Using the ONC-provided test data, the Tester shall verify that the patient's ambulatory summary is transmitted in human readable format, including, at a minimum, the following data elements (Ambulatory Only):

1) Provider's name
2) Provider's office contact information
3) Common MU Data Set (in their English representation (description) if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language

7) Smoking status
8) Problems
9) Medications
10) Medication Allergies
11) Laboratory test(s)
12) Laboratory value(s)/result(s)
13) Vital signs – height, weight, blood pressure, BMI
14) Care plan field(s), including goals and instructions
15) Procedures
16) Care team member(s)

Note: The tester may need to place the C-CDA XML and style sheet XML, acquired from the validation report, in separate files and save them in the same directory on the test computer in order to view the human readable document

IN170.314(e)(1) – 3.05: Using the ONC-provided test data, the Tester shall verify that the patient's inpatient summary is transmitted in human readable format, including, at a minimum, the following data elements (Inpatient Only):

1) Patient admission date
2) Patient discharge date
3) Admission/discharge location
4) Discharge instructions
5) Reason(s) for hospitalization
6) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language
    7) Smoking status
    8) Problems
    9) Medications
    10) Medication Allergies
    11) Laboratory test(s)
    12) Laboratory value(s)/result(s)
    13) Vital signs – height, weight, blood pressure, BMI
    14) Care plan field(s), including goals and instructions
    15) Procedures
    16) Care team member(s)

Note: The tester may need to place the C-CDA XML and style sheet XML, acquired from the validation report, in separate files and save them in the same directory on the test computer in order to view the human readable document

IN170.314(e)(1) – 3.06: Using the ONC-provided test data, the Tester shall verify that the patient's Referral Summary/Transition of Care is transmitted in human readable format, including, at a minimum, the following data elements (Inpatient Only):

1) Encounter diagnoses
2) Immunizations
3) Cognitive status
4) Functional status
5) Discharge instructions
6) Common MU Data Set (in their English representation if they associate with a vocabulary/code set)
    1) Patient name
    2) Sex
    3) Date of birth
    4) Race
    5) Ethnicity
    6) Preferred language
    7) Smoking status
    8) Problems
    9) Medications
    10) Medication Allergies
    11) Laboratory test(s)
    12) Laboratory value(s)/result(s)
    13) Vital signs – height, weight, blood pressure, BMI
    14) Care plan field(s), including goals and instructions
    15) Procedures
    16) Care team member(s)

IN170.314(e)(1) – 3.07: The Tester shall identify the C-CDA .xml files within the transmitted documents (This may involve reviewing EHR logs to access the transmitted documents, parsing files and inspecting the header to identify the C-CDA document .xml (vs. style sheet, human readable document, etc.))

IN170.314(e)(1) – 3.08: Using the provided test data, and the Validation Report produced by the Transport Testing Tool identified in the Conformance Test Tools section of this test procedure**,** the Tester shall verify that

- The C-CDA Implementation Guide conformance requirements tested are met by the electronically generated (Ambulatory/Inpatient) summary and Transition of Care/Referral Summary (Inpatient Only)
- The standards for the named vocabularies for the Common MU Data Set are met by the electronically generated summary (Ambulatory/Inpatient) and Transition of Care/Referral Summary (Inpatient Only)

IN170.314(e)(1) – 3.09: Using the ONC-provided test data, the Tester shall visually inspect the content of the C-CDA documents available within the .xml output available within the Validation Report produced by the Transport Testing Tool by inspecting .xml is complete and accurate.

DTR170.314(e)(1)-4: Record and Display Actions

Required Vendor Information

VE170.314(e)(1) – 4.01: Vendor shall identify if capabilities certified in § 170.314(d)(2) is accessible to the patient or whether a separate action log capability is utilized for the activity history log

Required Test Procedures

TE170.314(e)(1) – 4.01: The Tester shall execute DTR170.314(e)(1) – 1, DTR170.314(e)(1) – 2, and DTR170.314(e)(1) – 3.

TE170.314(e)(1) – 4.02: The Tester logs into the online system as the patient

TE170.314(e)(1) – 4.03: The Tester causes the online system to display user, date, and time for information viewed in TE170.314(e)(1) – 1.02 and TE170.314(e)(1) – 1.04 and verifies that the action log information is accurate and complete

TE170.314(e)(1) – 4.04: The Tester causes the online system to display user, date, and time information for information downloaded in TE170.314(e)(1) – 2.02 and verifies that the action log information is accurate and complete

TE170.314(e)(1) – 4.05: The Tester causes the online system to display user, date, and time information for information downloaded in TE170.314(e)(1) – 2.03 and verifies that the action log information is accurate and complete

TE170.314(e)(1) – 4.06: The Tester causes the online system to display user, date, and time information for information transmitted in TE170.314(e)(1) – 3.07 and verifies that the action log information is accurate and complete

TE170.314(e)(1) – 4.07: The Tester causes the online system to display user, date, and time information for information transmitted in TE170.314(e)(1) – 3.08 and verifies that the action log information is accurate and complete

Inspection Test Guide

IN170.314(e)(1) – 4.01: Using the Vendor-identified patient ID and the dates, times, and users noted in TE170.314(e)(1) – 1.02 and TE170.314(e)(1) – 1.04, and viewing the test patient's health information, the Tester shall

- Verify that the actions of viewing health information by both the patient and patient's authorized representative in DTR170.314(e)(1) – 1: View Health Information test is accurate compared to the correct patient's record
- Verify that, for those actions, the correct date and time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4), and user are stored accurately and without omission in the correct patient's record

IN170.314(e)(1) – 4.02: Using the Vendor-identified patient and the dates, times, and users noted in TE170.314(e)(1) – 2.02 and TE170.324.e.1 – 2.03, downloading the test patient's health information, the Tester shall

- Verify that the actions of downloading health information in DTR170.314(e)(1) – 2: Download Health Information test is accurate compared to the correct patient's record
- Verify that, for those actions, the correct date and time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4), and user identification are stored accurately and without omission in the correct patient's record

IN170.314(e)(1) – 4.03: Using the Vendor-identified patient and the dates, times, and users noted in TE170.314(e)(1) – 3.07 and TE170.324(e)(1) – 3.08, transmitting the test patient's health information, the Tester shall

- Verify that the action of transmitting health information to a third party in DTR170.314(e)(1) – 3: Transmit Health Information Using Direct test is accurate compared to the correct patient's record
- Verify that, for those actions, the correct date and time (utilizing a system clock that has been synchronized following the (RFC 1305) Network Time Protocol, or (RFC 5905) Network Time Protocol Version 4), and user identification are stored accurately and without omission in the correct patient's record

DTR170.314(e)(1)-5: Submit and Verify Summative Testing Results for WCAG Conformance

Required Vendor Information

VE170.314(e)(1) – 5.01: The Vendor shall identify each web page associated with an "accessible version" of view, download, and transmit functions (and accessing them)

VE170.314(e)(1) – 5.02: The Vendor shall identify "pure decoration" and third-party content on accessible web pages associated with view, download, and transmit functions (and accessing them)

VE170.314(e)(1) – 5.03: The Vendor shall identify supported browsers associated with view, download, and transmit functions (and accessing them) (For supplemental guidance, reference: http://www.w3.org/TR/UNDERSTANDING-WCAG20/conformance.html#uc-accessibility-support-head)

VE170.314(e)(1) – 5.04: The Vendor shall provide documentation describing the techniques and methods used in development to support WCAG2.0

VE170.314(e)(1) – 5.05: The Vendor shall provide documentation of the applicable success criteria for level A conformance (see "How to Meet WCAG 2.0" (customized for only Level A success criteria and excluding advisory techniques) for supplemental guidance) and document any success criteria that are not applicable (and rationale for non-applicability) (see http://www.w3.org/WAI/WCAG20/quickref/ for supplemental guidance)

VE170.314(e)(1) – 5.06: The Vendor shall provide documentation of testing tools applied to each web page identified in VE170.314(e)(1) – 5.01

VE170.314(e)(1) – 5.07: The Vendor shall provide documentation of aspects of conformance not verified by testing tools from Items 1-5 of WCAG2.0 Conformance - http://www.w3.org/TR/2008/REC-WCAG20-20081211/#conformance-reqs

VE170.314(e)(1) – 5.08: The Vendor shall provide documentation of explanation of any conformance failures or rationale for over-ruling of tool output

VE170.314(e)(1) – 5.09: The Vendor shall record and report all WCAG2.0 conformance results (e.g. as indicated in http://www.w3.org/WAI/ER/conformance/ED-methodology-20120915#step5)

Required Test Procedures

TE170.314(e)(1) – 5.01: Using the Inspection Test Guide, the Tester shall examine the Vendor-provided documentation identified in VE170314(e)1 – 5.01 through VE170314(e)1 – 5.08

TE170.314(e)(1) – 5.02: Using the Inspection Test Guide, the Tester shall examine the Vendor-provided conformance testing results submitted in VE170314(e)1 – 5.09

Inspection Test Guide

IN170.314(e)(1) – 5.01: The Tester shall evaluate that the Vendor-provided documentation for WCAG2.0 conformance testing and use of conformance tools for each web page submitted for testing are complete, and meet the conformance requirements for WCAG 2.0 Level A (Vendors may choose to report these results with the content and completion requirement guidance listed athttp://www.w3.org/WAI/ER/conformance/ED-methodology-20120915#step5)

IN170.314(e)(1) – 5.02: The Tester shall evaluate the Vendor-provided documentation of tool failures or over-ruling of tool outputs (Accessibility evaluation guidance available at: http://www.w3.org/WAI/eval/Overview.html)

IN170.314(e)(1) – 5.03: The Tester shall evaluate the Vendor-provided documentation of conformance not verified by testing tools (For supplemental guidance, reference http://www.w3.org/WAI/eval/selectingtools.html)

IN170.314(e)(1) – 5.04: The Tester shall evaluate that the results in conformance testing of web page(s) selected by the tester is comparable to Vendor-provided documentation and Vendor-provided conformance testing results

TEST DATA

ONC supplied test data is provided with the test procedure to ensure that the applicable requirements identified in the criteria can be adequately evaluated for conformance, as well as, to provide consistency in the testing process across multiple National Voluntary Laboratory Accreditation Program-Accredited Testing Laboratories (ATLs). The provided test data focus on evaluating the basic capabilities of required EHR technology, rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support. The test data is formatted for readability of use within the testing process. The format is not prescribing a particular end-user view or rendering. No additional requirements should be drawn from the format.

The Tester shall use and apply the provided test data during the test, without exception, unless one of the following conditions exists:

- The Tester determines that the Vendor product is sufficiently specialized that the provided test data needs to be modified in order to conduct an adequate test. Having made the determination that some modification to the provided test data is necessary, the Tester shall record the modifications made as part of the test documentation.
- The Tester determines that changes to the test data will improve the efficiency of the testing process; primarily through using consistent demographic data throughout the testing workflow. The Tester shall ensure that the functional and interoperable requirements identified in the criterion can be adequately evaluated for conformance and that the test data provides a comparable level of robustness. Having made the determination that some modification to the provided test data is necessary, the Tester shall record the modifications made as part of the test documentation.

Test Data for §170.314(e)(1) VDT is available at http://www.healthit.gov/certification (navigation: 2014 Edition Test Method)

Any departure from the provided test data shall strictly focus on meeting the basic capabilities required of EHR technology relative to the certification criterion rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support.

The test procedures require that the Tester enter the test data into the EHR technology being evaluated for conformance. The intent is that the Tester fully controls the process of entering the test data in order to ensure that the data are correctly entered as specified in the test procedure. If a situation arises where it is impractical for a Tester to directly enter the test data, the Tester, at the Tester's discretion, may instruct the Vendor to enter the test data, so long as the Tester remains in full control of the testing process, directly observes the test data being entered by the Vendor, and validates that the test data are entered correctly as specified in the test procedure.

CONFORMANCE TEST TOOLS

The following testing tools are available to evaluate conformance to the standards referenced in this test procedure:

- Direct Certificate Discovery Tool (DCDT) – ONC provides a web application certificate discovery testing tool to support this test procedure. This tool was created to support automated testing of systems that plan to enact the Certificate Discovery and Provider Directory Implementation Guide, approved as normative specification by the Direct community, as of July 9, 2012. It is based on the written test package and requirement traceability matrix created by the Modular Specifications project.
    - This application can be installed and deployed locally.

- The Direct Certificate Discovery Tool, User's Guide, configuration instructions, and other documentation are available at: http://code.google.com/p/direct-certificate-discovery-tool/

Support for this tool is available by contacting:
Avinash Shanbhag (Avinash.Shanbhag@hhs.gov)
Director, Nationwide Health Information Network Division
Office of Standards and Interoperability
Office of the National Coordinator for Health IT, HHS

- Transport Testing Tool (TTT) -- the Transport Testing Tool is designed to support this test procedure. The Transport Testing Tool includes the capability to verify the ability to exchange Consolidated CDA (C-CDA) conformant documents using transport standards (e.g., Direct, Direct + XDM, SOAP). C-CDA conformance testing within the Transport Testing Tool relies on Model Driven Health Tools (MDHT) for Consolidated CDA validation developed by ONC.
  - The Transport Testing Tool (TTT) is available at: http://transport-testing.nist.gov

  Support for the Transport Testing Tool is available by submitting questions to the Transport Testing Tool user group at: https://groups.google.com/d/forum/transport-testing-tool. Inquiries may also be sent to this user group via email: transport-testing-tool@googlegroups.com

Multiple browsers may be used to access this tool; if the tool does not load completely using Internet Explorer 8 or Internet Explorer 9, alternative browsers such as Firefox, Google Chrome, or Safari are recommended. The Transport Testing Tool uses non-standard ports. If your firewall blocks HTTP traffic on non-standard ports, this tool may not be accessible. Please retry access from a location without a firewall that blocks non-standard ports. Alternatively users may download and run a local version of the tool.

The following information is provided to assist the Tester in interpreting the conformance reports generated by the Transport Testing Tool (TTT:

The Transport Testing Tool (TTT), via MDHT, evaluates individual conformance statements which have been derived from the standards and the "HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, DSTU Release 1.1 (US Realm) Draft Standard for Trial Use July 2012" identified in the Final Rule and the test data provided in this test procedure. The validation tools evaluate the submitted HL7 message instance for each conformance statement, and then produce a conformance report. The Tester should consider that a report containing only Affirmative and Warning messages indicates general conformance to the standard and test data expectations. If reported, errors should be considered as significant departures from the standard or test data requirements which need to be corrected in order to claim conformance. ATLs will need to further analyze each error to determine if, in the context of meeting the criterion and overall meaningful use objective, the error results in a failure of the test procedure by the EHR technology. The tester may need to inspection test data values derived from required vocabularies and code sets.

Document History

Version Number	Description of Change	Date Published
1.0	Released for public comment	November 19, 2012
1.1	Delivered for National Coordinator Approval	December 3, 2012
1.2	Posted Approved Test Procedure	December 14, 2012
1.3	Posted Updated Approved Test Procedure Updates: • Removed Normative Test Procedure steps to upload trust anchor to TTT and validate the trust anchor, and removed references to these steps in the Informative Test Description • Inserted references to visually inspect .xml to verify content/values are acceptable • Added footnote in Normative Test Procedure clarifying Transport Testing Tool Trust Anchor and Certificates for local installation • Inserted new VE – 3.06 • Updated step numbers in Normative Test Procedure to be consecutive • Modified Record and Display Normative Test Procedure references to correctly reference steps in previous sections of the Normative Test Procedure	February 1, 2013
1.4	Posted Updated Approved Test Procedure Updates: • In Informative Test Description, added statement “The transmission of the C-CDA and human readable document formats may occur as separate transactions or both documents may be transmitted within a single transmission.” • In Normative Test Procedure, added step TE170.314(e)(1) – 2.04 for the Tester to validate C-CDA conformance using the C-CDA Document Validator within the Transport Testing Tool • In Inspection Test Guide, modified IN170.314(e)(1) – 2.05 to replace “Validation Report” with “results of the C-CDA Document Validator” • In Inspection Test Guide, modified IN170.314(e)(1) – 2.06 to clarify instructions for a visual inspection of the C-CDA.xml • In Inspection Test Guide, added “Note: the human readable and C-CDA documents may be transmitted using the Direct standard in a single transmission or separate transmissions” in IN170.314(e)(1) – 3.03 • In Inspection Test Guide, added strikethrough to IN170.314(e)(1) – 3.07 • In Inspection Test Guide, modified IN170.314(e)(1) – 3.09 to clarify instructions for a visual inspection of the C-CDA documents available within the .xml output, and add strikethrough to “(by inspecting .xml)”	February 22, 2013

1.5	Posted Updated Approved Test Procedure Updates: • In VE170.314(e)(1) – 1.04 changed “and authorized ” to “an authorized” • In DTR170.314(e)(1) – 4 inspection test guide changed “patient ID” to “patient” and “user ID” to “user” • Clarification provided in informative test description outlining the requirement for EHR technology to make available two documents for download and transmission in the inpatient setting (page 5) • Added clarification in informative test description that information in human readable format must be human readable in a single download and transmission (for example C-CDA conformant document and associated style sheet must be available in a single download and a single transmission) (page 5)	May 8, 2013

1.6	Updated Approved Test Procedure Updates: • Removed v1.4 note explaining strikethrough text in informative test description • Added clarification in the informative test description that EHR vendors must make a minimum of two "types" of documents available rather than two individual documents (page 5) • Specified in the informative test description that the inpatient summary must contain the elements listed in the 170.314(e)(1) certification criterion (page 5) • Replaced "a transition of care/referral summary that may be created" with "transition of care/referral summaries that were created" in the informative test description to better align with the certification criterion language (page 5) • Added clarification to the informative test description: "If multiple documents are required for human readable format, these documents must be sent as separate attachments in any order within a single transmission. Vendors may provide additional attachments (e.g. XDM package) in the transmission if desired." (page 5) • Added note to informative test description clarifying that resources provided that are not normative parts of the WCAG 2.0 level "A" standard are provided as supplemental guidance only (page 9) • Removed strikethrough of text in normative test procedure • Added note to IN170.314(e)(1) – 3.03 "If multiple documents are required for human readable format, all documents must be sent as separate attachments within a single transmission)." • Added note to IN170.314(e)(1) – 3.04 and IN170.314(e)(1) – 3.05 "Note: The tester may need to place the C-CDA XML and style sheet XML, acquired from the validation report, in separate files and save them in the same directory on the test computer in order to view the human readable document" • Removed "IN170.314(e)(1) – 5.04: The Tester shall evaluate that the Vendor-provided conformance testing results conform(s) to the content and completion requirements specified at http://www.w3.org/WAI/ER/conformance/ED-methodology-20120915#step5" • Updated VE170.314(e)(1) – 5.03, VE170.314(e)(1) – 5.05, and IN170.314(e)(1) – 5.03 to indicate that links provided are supplemental guidance • Added note to IN170.314(e)(1) – 5.01 "(Vendors may choose to report these results with the content and completion requirement guidance listed athttp://www.w3.org/WAI/ER/conformance/ED-methodology-20120915#step5)" • Updated Test Procedure steps to maintain correct numerical order	June 10, 2013

1.7	Updated Approved Test Procedure Updates: • Updated the NTP protocol to allow for synching to occur within 5 seconds • Updated the Document History of Version 1.6 to clarify which step was removed when referring to IN170.314(e)(1) – 5.04 • Updated the Document History of Version 1.6 to indicate that test procedure steps were renumbered to maintain numerical order after modifications	July 11, 2013

[i] **ANNEX A: APPROVED SECURITY FUNCTIONS**

Annex A provides a list of the Approved security functions applicable to FIPS PUB 140-2. The categories include transitions, symmetric key, asymmetric key, message authentication and hashing. An excerpt is provided below.

Transitions

National Institute of Standards and Technology, *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Special Publication 800-131A, January 2011. Sections relevant to this Annex: 1, 2, 3, 9 and 10.

Symmetric Key (AES, TDEA and EES)

1. **Advanced Encryption Standard (AES)**

National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, Addendum to Special Publication 800-38A, October 2010.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May 2004.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, Special Publication 800-38E, January 2010.

2. **Triple-DES Encryption Algorithm (TDEA)**

National Institute of Standards and Technology, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Special Publication 800-67, May 2004.

National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Special Publication 800-38A, December 2001. Appendix E references Modes of Triple-DES.

American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation,* ANSI X9.52-1998. Copies of X9.52-1998 may be obtained from X9, a standards committee for the financial services industry.

3. **Escrowed Encryption Standard (EES)**

National Institute of Standards and Technology, *Escrowed Encryption Standard (EES)*, Federal Information Processing Standards Publication 185, February 9, 1984.

Asymmetric Key (DSS – DSA, RSA and ECDSA)

1. **Digital Signature Standard (DSS)**
    a. National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-3, June, 2009. (DSA2, RSA2 and ECDSA2)
    b. National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA)
    c. RSA Laboratories, *PKCS#1 v2.1: RSA Cryptography Standard*, June 14, 2002. Only the versions of the algorithms RSASSA-PKCS1-v1_5 and RSASSA-PSS contained within this document shall be used.

Secure Hash Standard (SHS)

1. **Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)**

    National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-4, March, 2012.

Random Number Generators (RNG and DRBG)

1. **Annex C: *Approved Random Number Generators*** National Institute of Standards and Technology, *Annex C: Approved Random Number Generators for FIPS 140-2, Security Requirements for Cryptographic Modules*.

Message Authentication (Triple-DES, AES and SHS)

1. **Triple-DES**
   National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985.
2. **AES**
   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, Special Publication 800-38B, May 2005.
   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, Special Publication 800-38C, May 2004.
   National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, November 2007.

3. **SHS**

National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198-1, July, 2008.