Test Procedure for §170.314 (h)(2) Optional – transmit – applicability statement for secure health transport and XDR/XDM for direct messaging

This document describes the test procedure for evaluating conformance of electronic health record (EHR) technology to the certification criteria defined in 45 CFR Part 170 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange, 2014 Edition, Release 2, Final Rule. http://www.healthit.gov/certification (navigation: 2014 Edition Release 2 Test Method). The test procedures may be updated to reflect on-going feedback received during the certification activities.

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

Certification Criteria

Refer to § 170.314(h)(2) for the certification criteria.
http://www.gpo.gov/fdsys/pkg/FR-2014-09-11

Per Section III.A.2 the Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange, 2014 Edition, Release 2, Final Rule issued September 11, 2014, this certification criterion is added to the 2014 Edition test method and is designated as “optional” in regulation.

2014 Release 2 Edition Preamble Language

Per Section III.A.2 of the preamble of the Electronic Health Record (EHR) Certification Criteria and the ONC Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange, 2014 Edition, Release 2, Final Rule where the Transmission certification criteria is discussed. As a result of the proposal to decouple content and transport capabilities from the Transitions of Care (ToC) certification criteria and the View, Download, Transmit (VDT) certification criterion, three separate transmission certification criteria were proposed. The second transmission criterion at §170.314(h)(2) is based on the standard expressed at § 170.314(b)(1)(i)(B) and 170.314(b)(2)(ii)(B).

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 evaluates the capability for EHR technology to electronically transmit and receive health information (e.g. the transition of care/referral summary document (summary care record) in conformance with the Consolidated Clinical Document Architecture (C-CDA) standard). The vendor may elect to be evaluated for the capability to transmit and receive the transition of care/referral summaries using the Applicability Statement for Secure Health Transport standard and the ONC XDR and XDM for Direct Messaging Specification standard. This option would permit EHR technology to be certified as being in compliance with the original proposal: certification to both the Applicability Statement for Secure Health Transport specification and the XDR and XDM for Direct Messaging specification.

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 Edge Testing Tool (ETT), 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, Certified EHR Technology (CEHRT) must maintain an association with a supported address (sender or recipient) and a collection of Trusted Anchors[1]. The ETT 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 ETT 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. ONC provides the test data for this test procedure.

- Transmit - Evaluates the capability to electronically transmit health information.
  - The Tester identifies the health information (C-CDA summary care record) to be electronically transmitted to a recipient
  - The Tester verifies that the EHR can discover certificates from other parties in DNS CERT records and LDAP servers[2]
  - Using the Vendor-identified function(s), the Tester verifies that the EHR technology (e.g. Health Information Service Provider (HISP) is able to create and store a listing of Direct recipients
  - Using the Vendor-identified function(s), the Tester causes the health information in C-CDA format to be transmitted to a third party using Direct and the Cross-Enterprise Document Reliable Interchange (XDR) and Cross-Enterprise Document Media Interchange (XDM) for Direct Messaging Specification, 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
  - Using the provided test data, the Tester verifies that the data rendered in the transmitted C-CDA are complete and accurate (This may be accomplished by inspection of the C-CDA.xml).

[1] Section 4.2.3 of the ONC Applicability Statement for Secure Health Transport: "Each implementation MUSTmaintain 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."

[2] 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."

- Receive – Evaluates the capability of EHR technology to electronically receive health information.
  - The Tester verifies that the EHR technology can correctly host address-bound or domain-bound certificates in either DNS CERT records or LDAP servers that are discoverable by other parties[3]
  - Using the Vendor-identified function(s), the Tester causes the health information in C-CDA format to be transmitted from the Edge Testing Tool to the EHR technology using Direct and the Cross-Enterprise Document Reliable Interchange (XDR) and Cross-Enterprise Document Media Interchange (XDM) for Direct Messaging Specification, based on ONCsupplied test information
  - The Tester verifies successful receipt of C-CDA documents using the Direct transport standard for unwrapped messages; If the vendor offers the capability to accept both unwrapped and wrapped messages (according to RFC-5751), the tester will verify successful receipt of a Direct message using both capabilities
  - The Tester verifies that the EHR rejects receipt of Direct messages when sent with an invalid trust anchor
  - The Tester verifies that the EHR rejects receipt of Direct messages when sent using an invalid, or expired certificate or sent using an invalid trust store
  - The Tester verifies successful receipt of the health information by the EHR, and that the health information can be successfully decrypted and that a Message Disposition Notification (MDN) is sent by the EHR to the Edge Testing Tool

REFERENCED STANDARDS

§170.202 Transport standards	Regulatory Referenced Standard
The Secretary adopts the following transport standards:	
(b) Standard. ONC XDR and XDM for Direct Messaging Specification (incorporated by reference in § 170.299).	

[3] Section 5.0 of the ONC Applicability Statement for Secure Health Transport v1.1: "STAs MUST be able to discover certificates using both the DNS as specified in this section and LDAP as described by the S&I Framework Certificate Discovery for Direct Project Implementation Guide. To achieve universal certificate discovery, STAs MAY elect to publish certificates in the DNS or using LDAP through the capabilities detailed in this section and in the S&I Framework Certificate Discovery for Direct Project Implementation Guide respectively"

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.314(h)(2) – 1: Transmit Health Information to a Third Party Using Direct and XDR/XDM for Direct Messaging

DTR170.314(h)(2) – 1: Receive Health Information from a Third Party Using Direct and XDM Validation DTR170.314(h)(2) – 1: Transmit Health Information to a Third Party Using Direct and XDR/XDM for Direct Messaging

Required Vendor Information

VE170.314(h)(2) – 1.01: 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 2014 Direct Certificate Discovery Tool

VE170.314(h)(2) – 1.02: 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 2014 Direct Certificate Discovery Tool

VE170.314(h)(2) – 1.03: The Vendor shall identify the Direct address for registering within the Edge Testing Tool

VE170.314(h)(2) – 1.04: The Vendor shall obtain the Edge Testing Tool's Public Key and Trust Anchor from the Edge Testing Tool and store it within the EHR technology function/location for encrypting Direct message(s) to be sent to another setting of care or provider of care[4] or HISP

VE170.314(h)(2) – 1.05: 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 Edge Testing Tool

VE170.314(h)(2) – 1.06: The Vendor shall identify the ONC-supplied test C-CDA document(s) available for transmission

VE170.314(h)(2) – 1.07: The Vendor shall identify a Contact Email address to be used for receipt of the validation report generated by the Edge Testing Tool if the Contact email address for XDM Validation

Required Test Procedures

TE170.314(h)(2) – 1.01: The Tester shall download the Direct Certificate Discovery Tool's Trust Anchor and import it into the EHR technology's trust store

TE170.314(h)(2) – 1.02: The Tester shall use the Direct (From) address provided in VE170.314(h)(2) – 1.01 to execute the test using the 2014 Direct Certificate Discovery Tool

TE170.314(h)(2) – 1.03: The Tester shall use the non-Direct email address provided in VE170.314(h)(2) -1.02 for receipt and validation of results of certificate discovery testing

[4] When the test procedure refers to the Edge Testing Tool's trust anchor and certificates, this refers to ONC hosted version on www.healthit.gov/ETT. If your organization is hosting its own version of Edge Testing Tool (ETT), then you will need to create your own trust anchor certificates and use these instead. For example, the trustanchor for hit-testing@ttpedge.sitenv.org,may change to"ett.yourdomain.com

TE170.314(h)(2) – 1.04: The Tester shall execute all test cases available within the Direct Certificate Discovery Tool

TE170.314(h)(2) – 1.05: 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 (this step does not need to be repeated if passed the first time)

TE170.314(h)(2) – 1.06: The Tester shall cause the EHR technology to register the Direct (To) addresses specified in the Edge Testing Tool to be available for Direct messaging with XDM Validation within the EHR technology

TE170.314(h)(2) – 1.07: The Tester shall cause the EHR technology to transmit Consolidated CDA conformant document(s) identified in VE170.314(h)(2) – 1.06 using ONC Applicability Statement for Secure Health Transport (Direct) standard with XDM Validation to the Direct (To) address(es) specified in the Edge Testing Tool Direct that are available within the EHR following TE170.314(h)(2) – 1.02. The Direct message shall be encrypted using the recipient's (Edge Testing Tool) Public Key obtained in VE170.314(h)(2)– 1.04 and signed using the sender's (Vendor) Private Key for the Referral Summary/Transition of Care document (C- CDA).

TE170.314 (h)(2) – 1.08: Using the Inspection Test Guide, the Tester shall verify that the Transition of Care/Referral Summary is transmitted according to the ONC Applicability Statement for Secure Health Transport (Direct) standard with XDM Validation

Inspection Test Guide

IN170.314(h)(2) – 1.01: Using the 2014 Direct Certificate Discovery Tool, the Tester shall inspect the results received via email to verify that all test cases for discovery of certificates hosted in DNS and LDAP were successful

IN170.314(h)(2) – 1.02: The Tester shall verify the appropriate Direct (To) address(es) (provided within the Edge Testing Tool Direct) have been registered within the EHR technology and are visible Direct addresses for transmitting of health information to the Edge Testing Tool according to the ONC Applicability Statement for Secure Health Transport (Direct) standard with XDM Validation

IN170.314(h)(2) – 1.03: Using the Edge Testing Tool Direct Message Status, the Tester shall verify that the transmitted C- CDA document has been transmitted and received successfully according to the ONC Applicability Statement for Secure Health Transport (Direct) standard with XDM Validation, and the Edge Testing Tool validation report indicates successful decryption validation and trust anchor validation

DTR170.314(h)(2)–2: Receive Summary of Care Record Using Direct and XDM Validation

Required Vendor Information

VE170.314(h)(2) – 2.01: The Vendor shall identify whether the EHR technology stores certificates as address-bound or domain-bound certificates and whether the EHR hosts certificates in DNS or LDAP servers

VE170.314(h)(2) – 2.02: The Vendor shall identify the Direct address for Test Cases within the 2014 Direct Certificate Discovery Tool

VE170.314(h)(2) – 2.03: The Vendor shall identify a Contact Email address to be used for receipt of the validation report generated by the Edge Testing Tool for XDM Validation

VE170.314(h)(2) – 2.04: The Vendor shall identify the Direct address for registering within the Edge Testing Tool that shall receive the Direct message with XDM Validation

VE170.314(h)(2) – 2.05: The Vendor shall install the Valid Trust Anchor available from Edge Testing Tool Direct Testing homepage

VE170.314(h)(2) – 2.06: The Vendor shall identify the Edge Testing Tool's public certificate for use by the EHR to decrypt messages sent from the Edge Testing Tool

VE170.314(h)(2) – 2.07: The Vendor shall create and identify certificate(s) for Direct receive address(es) to be used for digital signing of the Direct message(s) to be sent by the Edge Testing Tool to the EHR

VE170.314(h)(2) – 2.08: The Vendor shall identify the EHR's Public Key (certificate) for encryption of the Direct message(s) to be uploaded to the Edge Testing Tool for sending of messages from the tool to the EHR

VE170.314(h)(2) – 2.09: The Vendor shall identify whether the EHR technology offers the capability to accept only unwrapped messages or both unwrapped messages and wrapped (according to RFC-5751) messages

Required Test Procedures

TE170.314(h)(2) – 2.01: The Tester shall execute all test cases using the Direct Certificate Discovery Tool for address or domain-bound certificates hosted in DNS or LDAP servers based upon the Vendor's certificate hosting methods identified in VE170.314(h)(2) – 2.01 and the Direct address specified in VE170.314(h)(2) – 2.02

TE170.314(h)(2) – 2.02: Using the Inspection Test Guide, the Tester shall verify that the EHR technology is able to correctly host either address-bound or domain-bound certificate(s) hosted in either DNS or LDAP servers that is discoverable by others

TE170.314(h)(2) – 2.03: The Tester shall enter a test session name for the sending of an unwrapped C- CDA document using Direct with XDM validation. This name will be used later in the procedure to identify the corresponding MDN

TE170.314(h)(2) – 2.04: The Tester shall utilize the Edge Testing Tool Direct to transmit an unwrapped message (that does not use the Direct RFC-5751 wrapper) digitally signed using a valid certificate and public key for the Vendor's EHR/HISP (provided in VE170.314(h)(2) – 2.07 and VE170.314(h)(2) – 2.08 for a C-CDA document (with an

XDM label) to the Vendor’s Direct address specified in VE170.314(h)(2) –2.04 using ONC Applicability Statement for Secure Health Transport (Direct) standard with XDM Validation and verify that an MDN was received by the Edge Testing Tool using the Inspection Test Guide

TE170.314(h)(2) – 2.05: If the Vendor offers the capability to receive both Direct RFC-5751 wrapped and unwrapped messages as specified in VE170.314(h)(2) – 2.09, The Tester shall enter a test session name for the sending of a wrapped C-CDA document using Direct with XDM validation standard. This name will be used later in the procedure to identify the corresponding MDN

TE170.314(h)(2) – 2.06: If the Vendor offers the capability to receive Direct RFC-5751 wrapped messages as specified in VE170.314(h)(2) – 2.09, The Tester shall utilize the Edge Testing Tool Direct to transmit a Direct RFC-5751 wrapped message digitally signed using a valid certificate and public key for the Vendor’s EHR (provided in VE170.314(h)(2) – 2.07 and VE170.314(h)(2) – 2.08) for a C-CDA document (with an XDM label) to the Vendor’s Direct address specified in VE170.314(h)(2)– 2.04 using ONC Applicability Statement for Secure Health Transport (Direct) standard with XDM Validation and verify that an MDN was received by theEdge Testing Tool using the Inspection Test Guide

TE170.314(h)(2) – 2.07: The Vendor shall download and install an invalid Trust Anchor available from the Edge Testing Tool

TE170.314(h)(2) – 2.08: The Tester shall enter a test session name for the sending of an unwrapped C- CDA document with an invalid Trust Anchor using the Direct with XDM Validation. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(2) – 2.09: The Tester shall utilize the Edge Testing Tool Direct to transmit an unwrapped C-CDA document (any C-CDA selection available in the Edge Testing Tool) to the EHR/HISP using the Direct transport standard with XDM Validation

TE170.314(h)(2) – 2.10: Using the Inspection Test Guide, the Tester shall verify that the EHR/HISP rejects receipt of the Direct message transmitted in TE170.314(h)(2) – 2.09 and no MDN was received by the Edge Testing Tool

TE170.314(h)(2) – 2.11: The Vendor shall remove the invalid Trust Anchor and reinstall the valid Trust Anchor as in VE170.314(h)(2) – 2.05

TE170.314(h)(2) – 2.12: The Tester shall enter a test session name for the sending of an unwrapped C- CDA document with an invalid certificate using the Direct standard with XDM Validation. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(2) – 2.13: The Tester shall utilize the Edge Testing Tool Direct to transmit an unwrapped C-CDA document (either the ambulatory or inpatient C-CDA selection available in the Edge Testing Tool) using an invalid certificate (INVALID_CERT) to the EHR/HISP using the Direct transport standard with XDM Validation

TE170.314(h)(2) – 2.14: Using the Inspection Test Guide, the Tester shall verify that the EHR/HISP rejects receipt of the Direct message transmitted in TE170.314(h)(2) – 2.13 and no MDN was received by the Edge Testing Tool

TE170.314(h)(2) – 2.15: The Tester shall enter a test session name for the sending of an unwrapped C- CDA conformant document with an expired certificate using the Direct standard with XDM Validation. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(2) – 2.16: The Tester shall utilize the Edge Testing Tool Direct to transmit an unwrapped C-CDA document (either the ambulatory or inpatient C-CDA selection available in the Edge Testing Tool) using an expired certificate (EXPIRED_CERT) to the EHR using the Direct transport standard with XDM Validation

TE170.314(h)(2) – 2.17: Using the Inspection Test Guide, the Tester shall verify that the EHR rejects receipt of the Direct message transmitted in TE170.314(h)(2) – 2.16 and no MDN was received by the Edge Testing Tool

TE170.314(h)(2) – 2.18: The Tester shall enter a test session name for the sending of an unwrapped C- CDA document with a certificate with an invalid trust relationship using the Direct standard with XDM Validation. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(2) – 2.19: The Tester shall utilize the Edge Testing Tool Direct to transmit an unwrapped C-CDA document (either the ambulatory or inpatient C-CDA selection available in the Edge Testing Tool) using a certificate with an invalid trust relationship (CERT_FROM_DIFFERENT_TRUST_ANCHOR) to the EHR/HISP using the Direct transport standard with XDM Validation

TE170.314(h)(2) – 2.20: Using the Inspection Test Guide, the Tester shall verify that the EHR/HISP rejects receipt of the Direct message transmitted in TE170.314(h)(2) – 2.19 and no MDN was received by the Edge Testing Tool

TE170.314(h)(2) – 2.21: Using the Inspection Test Guide, the Tester shall verify that the EHR/HISP rejects receipt of the Direct messages using certificates that are invalid or expired, or have an invalid trust relationship to the ONC trust store stored in the EHR/HISP

Inspection Test Guide

IN170.314(h)(2) – 2.01: Using the 2014 Direct Certificate Discovery Tool, the Tester shall verify that the EHR’s hosted certificates are discoverable for the selected test cases

IN170.314(h)(2) – 2.02: Tester shall verify that all messages wrapped, unwrapped, or both were received. This may be accomplished by reviewing log files (or other equivalent methods)

IN170.314(h)(2) – 2.03: Using the Edge Testing Tool HISP Testing & Delivery Notification Message Tracking, the Tester shall verify that Message Disposition

Notifications were sent by the EHR to indicate successful receipt of messages sent in: TE170.314(h)(2) – 2.04, TE170.314(h)(2) – 2.06, through inspection of the Validation Reports sent to the email address registered in VE170.314(h)(2) –2.03 or by clicking on ” Direct Message Status” on the Edge Testing Tool and looking in the

Table for the time stamp corresponding to when the message was sent or for the Msg ID that matches the "Test Session" name entered in steps TE170.314(h)(2) – 2.03. TE170.314(h)(2) – 2.05, TE170.314(h)(2) – 1.06, TE170.314(h)(2) – 1.08. Note: There should be a different Test Session name for each C-CDA sent

IN170.314(h)(2) – 2.04: Using the SUT system logs, the Tester shall verify that the Messages transmitted in: TE170.314(h)(2) – 2.09 , TE170.314(h)(2) – 2.13, TE170.314(h)(2) – 2.16, and TE170.314(h)(2) – 2.19 were rejected and not received by the EHR/HISP (e.g. inspecting audit logs to verify rejections)

IN170.314(h)(2) – 2.05: Using the Edge Testing Tool HISP Testing & Delivery Notification Message Tracking, the Tester shall verify that no MDN was received in response to the messages transmitted in TE170.314(h)(2) – 2.09 , TE170.314(h)(2) – 2.13, TE170.314(h)(2) – 2.16, and TE170.314(h)(2) – 2.19 by verifying that no Validation Report was sent to the email address registered inVE170.314(h)(2) – 2.03 or by clicking on" Direct Message Status" on the Edge Testing Tool and looking in the Table to verify that no MDN was received for the time stamp corresponding to when the message was sent or the Msg ID that matches the "Test Session" name entered in steps TE170.314(h)(2) – 2.08, TE170.314(h)(2) – 2.12, TE170.314(h)(2) – 2.15 and TE170.314(h)(2) – 2.18

TEST DATA

ONC-supplied test data are 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-(NVLAP) Accredited Testing Labs (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 are 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 applicable 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(h)(2) Optional – Applicability Statement for Secure Health Transport and XDR/XDM for Direct Messaging 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 applicable 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 (2014 DCDT) – ONC provides a web application, which may be accessed through the Edge Testing Tool/Cert Discovery 2014 DCDT, 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 can be accessed from the Direct menu in the Edge Testing Tool.

- Edge Testing Tool (ETT) - The Edge Testing Tool is designed to support this test procedure.
    - The Edge Testing Tool Direct Testing (Sections: Register Direct, Send Direct Message and Message Validator) includes the capability to verify the ability to exchange Consolidated CDA (C-CDA) conformant documents using Direct transport standards (e.g., Direct and Direct + XDM).
    - The Edge Testing Tool Message Validators (Section: XDR Validator) includes the capability to verify the ability to exchange Consolidated CDA (C-CDA) conformant documents using ONC XDR and XDM for Direct Messaging.
    - The Edge Testing Tool Message Validators (Section: CCDA R1.1 Validator) includes the capability to verify the conformance of the CDA (C-CDA R1.1) documents.
    - The Edge Testing Tool Edge Testing (Sections: Homepage, SMTP Test Cases, IMAP Test Cases, POP3 Test Cases, XDR Test Cases) includes the capability to verify the ability to exchange Consolidated CDA (C-CDA) conformant documents using transport standards (e.g. SOAP).

- The Edge Testing Tool HISP Testing and Delivery Notification (Section: Message Tracking) includes the capability to verify the receipt of messages.
    - This application can be installed and deployed locally.
    - The Edge Testing Tool (ETT) is available at: http://www.healthit.gov/ett

Multiple browsers may be used to access this tool. As the tool has been testing using both Chrome and Firefox browsers, these are the recommended browsers. The Edge 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 Edge Testing Tool (ETT):

The Edge Testing Tool (ETT), via MDHT, evaluates individual conformance statements which have been derived from the standards and the "HL7 Implementation Guide for CDA® Release 2: IHE HealthStory 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	October 8, 2014
1.1	Delivered for National Coordinator Approval	December 23, 2014
1.1	Posted Approved Test Procedure	December 24, 2014
1.2	Changed all references of Transport Testing Tool (TTT) to Edge Testing Tool (ETT). The TTT tool has been retired. Sections impacted include: • Informative Test Description • DTR170.314(h)(2) – 1: Transmit Health Information to a Third Party Using Direct and XDR/XDM for Direct Messaging: VE170.314(h)(2) – 1.03, VE170.314(h)(2) – 1.04, VE170.314(h)(2) – 1.05, VE170.314(h)(2) – 1.07, TE170.314(h)(2) – 1.06, TE170.314(h)(2) – 1.07, IN170.314(h)(2) – 1.02, IN170.314(h)(2) – 1.03 • DTR170.314(h)(2)–2: Receive Summary of Care Record Using Direct and XDM Validation: VE170.314(h)(2) – 2.03, VE170.314(h)(2) – 2.04, VE170.314(h)(2) – 2.05, VE170.314(h)(2) – 2.06, VE170.314(h)(2) – 2.07, VE170.314(h)(2) – 2.08, TE170.314(h)(2) – 2.04, TE170.314(h)(2) – 2.06, TE170.314(h)(2) – 2.07, TE170.314(h)(2) – 2.09, TE170.314(h)(2) – 2.10, TE170.314(h)(2) – 2.13, TE170.314(h)(2) – 2.14, TE170.314(h)(2) – 2.16, TE170.314(h)(2) – 2.17, TE170.314(h)(2) – 2.19, TE170.314(h)(2) – 2.20, IN170.314(h)(2) – 2.03, IN170.314(h)(2) – 2.05 • Conformance Testing Tool updated the description of the validation tools used within the Test Procedure; removed the tool support information (this is available within the tools). • Addition of the version to Direct Certificate Discovery Tool (DCDT) references, as the Edge Testing Tool contains both 2014 and 2015 versions.	January 27, 2017
1.3	Removed DCDT link and provided information to access the DCDT information from the Edge Testing Tool	May 26, 2017