Test Procedure for §170.314 (h)(1) Optional – applicability statement for secure health transport

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. 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)(1) 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 EDITION RELEASE 2 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 first transmission criterion at §170.314(h)(1) mirrors the capability expressed at §170.314(b)(1)(i)(A) and §170.314(b)(2)(ii)(A).

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 using the Applicability Statement for Secure Health Transport standard.

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, Certified EHR Technology (CEHRT) must maintain an association with a supported address (sender or recipient) and a collection of Trusted Anchors[1]. 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.

The test data for this test procedure is provided by ONC or the Vendor.

- Transmit – Evaluates the capability to electronically transmit health information.
    - The Tester identifies the payload (e.g., health information such as a 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 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

[1] 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."
[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 payload to be transmitted from the Transport Testing Tool to the EHR technology (HISP) using the Direct transport standard (ONC Applicability Statement for Secure Health Transport standard), based on ONC-supplied test information
  - The Tester verifies successful receipt of the transmitted payload 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 Transport Testing Tool

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).	

NORMATIVE TEST PROCEDURES

Derived Test Requirements

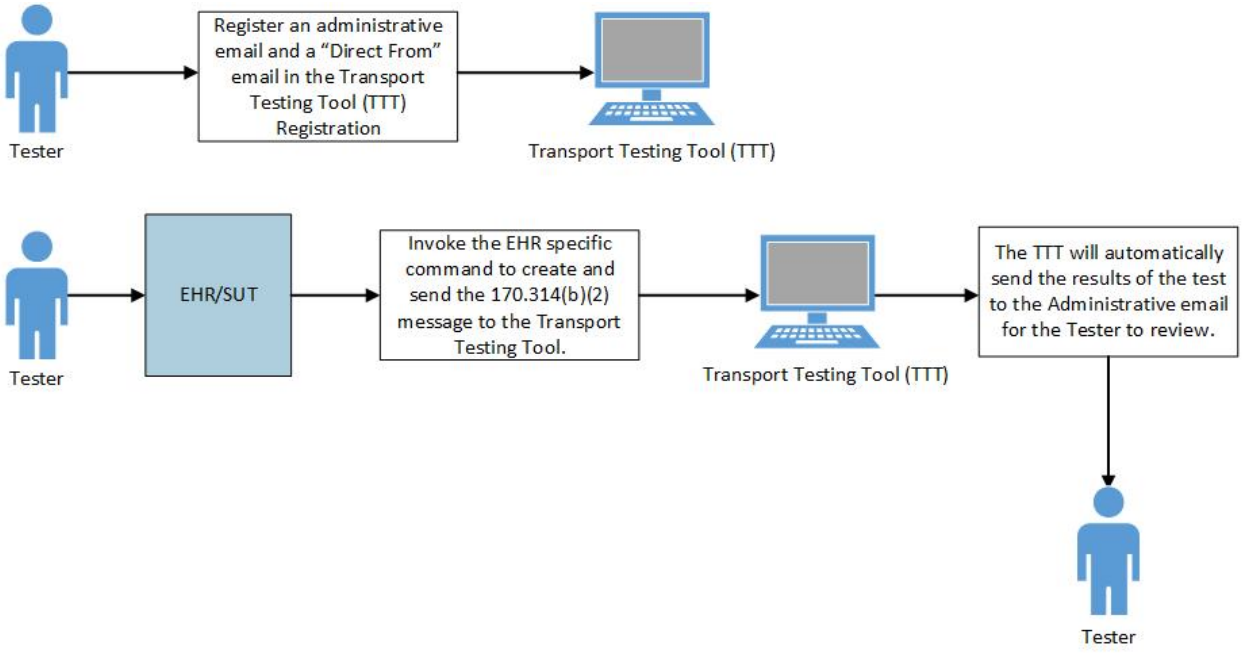
DTR170.314(h)(1) – 1: Transmit Health Information to a Third Party Using Direct

DTR170.314(h)(1) – 2: Receive Health Information from a Third Party Using Direct

[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"

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

Figure 1



Required Vendor Information

VE170.314(h)(1) – 1.01: 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(h)(1) – 1.02: The Vendor shall identify the Direct address for registering within the Transport Testing Tool

VE170.314(h)(1) – 1.03: The Vendor shall obtain the Transport Testing Tool's Public Key and Trust Anchor from the Transport 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)(1) – 1.04: 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

VE170.314(h)(1) – 1.05: The Vendor shall identify the Vendor-supplied payload for transmission to the Transport Testing Tool

Required Test Procedures

TE170.314(h)(1) – 1.01: The Tester shall download the Direct Certificate Discovery Tool's Trust Anchor and import it into the EHR technology's trust store

[4] When the test procedure refers to the Transport Testing Tool's trust anchor and certificates, this refers to the 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".

TE170.314(h)(1) – 1.02: The Tester shall use the Direct (From) address provided in VE170.314(h)(1) - 1.02 to execute the test using the Direct Certificate Discovery Tool

TE170.314(h)(1) – 1.03: The Tester shall use the non-Direct email address provided in VE170.314(h)(1) - 1.01 for receipt and validation of results of certificate discovery testing

TE170.314(h)(1) – 1.04: The Tester shall execute the following test cases within the Direct Certificate Discovery Tool:

- D1: Valid address-bound certificate discovery in DNS
- D2: Valid domain-bound certificate discovery in DNS
- D3: Valid address-bound certificate discovery in LDAP
- D4: Valid domain-bound certificate discovery in LDAP
- D5: Invalid address-bound certificate discovery in DNS
- D6: Invalid domain-bound certificate discovery in DNS
- D7: Invalid address-bound certificate discovery in LDAP
- D8: Invalid domain-bound certificate discovery in LDAP
- D9: Select valid address-bound certificate over invalid certificate in DNS
- D10: Certificate discovery in LDAP with one unavailable LDAP server
- D11: No certificates discovered in DNS CERT records and no SRV records
- D12: No certificates found in DNS CERT records and no available LDAP servers
- D13: No certificates discovered in DNS CERT records or LDAP servers
- D14: Discovery of certificate larger than 512 bytes in DNS
- D15: Certificate discovery in LDAP based on SRV priority value
- D16: Certificate discovery in LDAP based on SRV weight value

TE170.314(h)(1) – 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 and correctly fails to find the certificates for negative test cases)

TE170.314(h)(1) – 1.06: The Tester shall cause the EHR technology to register the Direct (To) address(es) specified in the Transport Testing Tool (to be available as a recipient for sending of Direct messages within the EHR technology)

TE170.314(h)(1) – 1.07: The Tester shall cause the EHR technology to transmit the Vendor-supplied payload indicated in VE170.314(h)(1) – 1.05 using ONC Applicability Statement for Secure Health Transport (Direct) standard to the Direct (To) address(es) specified in the Transport Testing Tool that are available within the EHR technology following TE170.314(h)(1) – 1.06. The Direct message shall be encrypted using the recipient's (Transport Testing Tool) Public Key obtained in VE170.314(h)(1) – 1.03 and signed using the sender's (Vendor) Private Key for the Referral Summary/Transition of Care document (C-CDA).

TE170.314(h)(1) – 1.08: Using the Inspection Test Guide, the Tester shall verify that the transmitted health information is sent according to the ONC Applicability Statement for Secure Health Transport (Direct) standard.

Inspection Test Guide

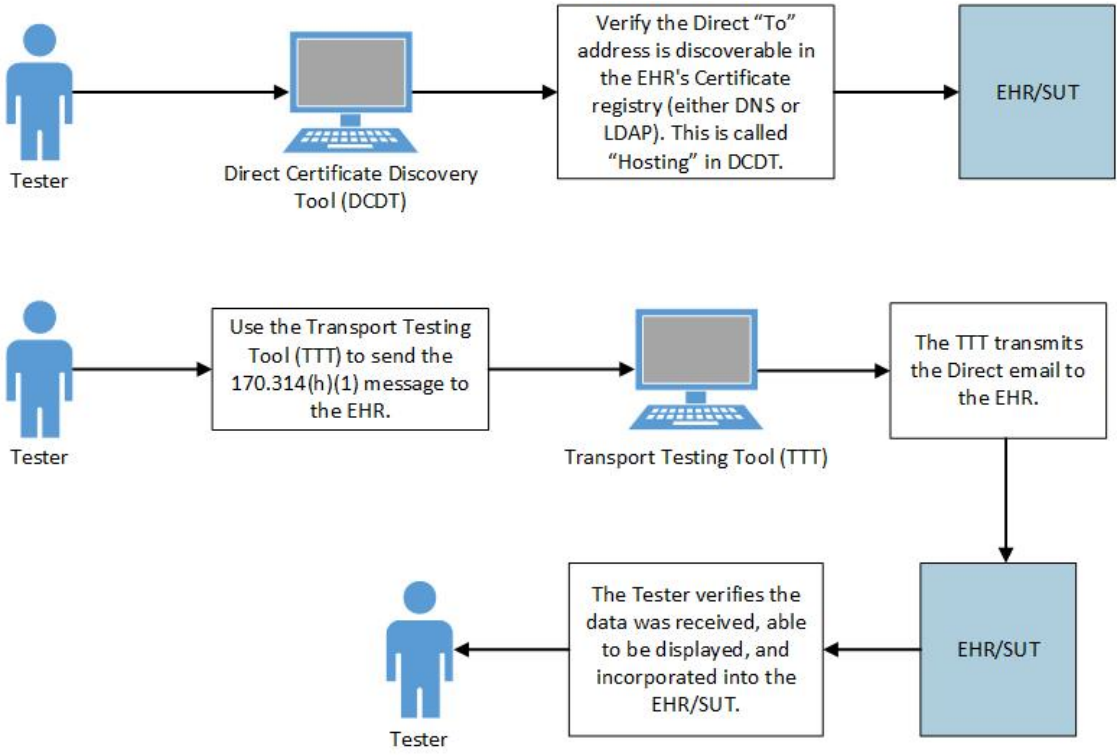
IN170.314(h)(1) – 1.01: Using the Direct Certificate Discovery Tool, the Tester shall inspect the results received via email to verify that all test cases for discovery of certificates hosted in DNS and LDAP were successful

IN170.314(h)(1) – 1.02: 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(h)(1) – 1.03: Using the Transport Testing Tool, the Tester shall verify that the transmitted health information has been sent and received successfully according to the ONC Applicability Statement for Secure Health Transport (Direct) standard, and the Transport Testing Tool validation report indicates successful decryption validation

DTR170.314(h)(1) – 2: Receive Summary Care Record Using Direct

Figure 2



Required Vendor Information

VE170.314(h)(1) – 2.01: The Vendor shall identify whether the EHR technology stores certificates as address-bound or domain-bound certificates and whether the EHR technology hosts certificates in DNS or LDAP servers

VE170.314(h)(1) – 2.02: The Vendor shall identify the Direct address for Test Cases within the Direct Certificate Discovery Tool

VE170.314(h)(1) – 2.03: 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(h)(1) – 2.04: The Vendor shall identify the Direct address for registering within the Transport Testing Tool that shall receive the Direct message

VE170.314(h)(1) – 2.05: The Vendor shall install the Valid Trust Anchor available from Transport Testing Tool homepage

VE170.314(h)(1) – 2.06: The Vendor shall identify the Transport Testing Tool's public certificate for use by the EHR to decrypt messages sent from the Transport Testing Tool

VE170.314(h)(1) – 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 Transport Testing Tool to the EHR technology

VE170.314(h)(1) – 2.08: The Vendor shall identify the EHR's Public Key (certificate) for encryption of the Direct message(s) to be uploaded to the Transport Testing Tool for sending of messages from the tool to the EHR technology

VE170.314(h)(1) – 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)(1) – 2.01: The Tester shall execute the applicable 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)(1) – 2.01 and the Direct address specified in VE170.314(h)(1) – 2.02

- Address-bound Certificate Test Cases
  - H1: Address-bound certificate search in DNS
  - H3: Address-bound certificate search in LDAP
- Domain-bound Certificate Test Cases
  - H2: Domain-bound certificate search in DNS
  - H4: Domain-bound certificate search in LDAP

TE170.314(h)(1) – 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)(1) – 2.03: The Tester shall enter a test session name for the sending of an unwrapped C-CDA document using the Direct standard. This name will be used later in the procedure to identify the corresponding MDN

TE170.314(h)(1) – 2.04: The Tester shall utilize the Transport Testing Tool to transmit an unwrapped Direct 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)(1) – 2.07 and VE170.314(h)(1) – 2.08) for a C-CDA document to the Vendor's Direct address specified in VE170.314(h)(1) – 2.04 and verify that

an MDN was received by the Transport Testing Tool using the Inspection Test Guide

TE170.314(h)(1) – 2.05: If the Vendor offers the capability to receive both Direct RFC-5751 wrapped and unwrapped messages as specified in VE170.314(h)(1) – 2.09,The Tester shall enter a test session name for the sending of a wrapped C-CDA document using the Direct standard. This name will be used later in the procedure to identify the corresponding MDN

TE170.314(h)(1) – 2.06: If the Vendor offers the capability to receive both Direct RFC-5751 wrapped and unwrapped messages as specified in VE170.314(h)(1) – 2.09, the Tester shall utilize the Transport Testing Tool to transmit a RFC-5751 wrapped Direct message digitally signed using a valid certificate and public key for the Vendor's EHR (provided in VE170.314(h)(1) – 2.07 and VE170.314(h)(1) – 2.08) for one C-CDA document (without an XDM label) to the Vendor's Direct address specified in VE170.314(h)(1) – 2.04 and verify that an MDN was received by the Transport Testing Tool using the Inspection Test Guide

TE170.314(h)(1) – 2.07: The Vendor shall download and install an invalid Trust Anchor available from the Transport Testing Tool

TE170.314(h)(1) – 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 standard. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(1) – 2.09: The Tester shall utilize the Transport Testing Tool to transmit an unwrapped C-CDA document (any C-CDA selection available in the Transport Testing Tool) to the EHR/HISP using the Direct transport standard

TE170.314(h)(1) – 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)(1) – 2.09 and no MDN was received by the Transport Testing Tool

TE170.314(h)(1) – 2.11: The Vendor shall remove the invalid Trust Anchor and reinstall the valid Trust Anchor as in VE170.314(h)(1) – 2.05

TE170.314(h)(1) – 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. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(1) – 2.13: The Tester shall utilize the Transport Testing Tool to transmit an unwrapped C-CDA document (either the ambulatory or inpatient C-CDA selection available in the Transport Testing Tool) using an invalid certificate (INVALID_CERT) to the EHR/HISP using the Direct transport standard

TE170.314(h)(1) – 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)(1) – 2.13 and no MDN was received by the Transport Testing Tool

TE170.314(h)(1) – 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. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(1) – 2.16: The Tester shall utilize the Transport Testing Tool to transmit an unwrapped C-CDA document (either the ambulatory or inpatient C-CDA selection available in the Transport Testing Tool) using an expired certificate (EXPIRED_CERT) to the EHR using the Direct transport standard

TE170.314(h)(1) – 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)(1) – 2.16 and no MDN was received by the Transport Testing Tool

TE170.314(h)(1) – 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. This name will be used later in the procedure to verify that no corresponding MDN was sent

TE170.314(h)(1) – 2.19: The Tester shall utilize the Transport Testing Tool to transmit an unwrapped C-CDA document (either the ambulatory or inpatient C-CDA selection available in the Transport Testing Tool) using a certificate with an invalid trust relationship (CERT_FROM_DIFFERENT_TRUST_ANCHOR) to the EHR/HISP using the Direct transport standard

TE170.314(h)(1) – 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)(1) – 2.19 and no MDN was received by the Transport Testing Tool

TE170.314(h)(1) – 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 NIST trust store stored in the EHR/HISP

Inspection Test Guide

IN170.314(h)(1) – 2.01: Using the Direct Certificate Discovery Tool, the Tester shall verify that the EHR's/HISP's hosted certificates are discoverable for the applicable test cases indicated in TE170.314(h)(1) – 2.01

IN170.314(h)(1) – 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)(1) – 2.03: Using the Transport Testing Tool, the Tester shall verify that Message Disposition Notifications were sent by the EHR to indicate successful receipt of messages sent in: TE170.314(h)(1) – 2.04, TE170.314(h)(1) – 2.06, through inspection of the Validation Reports sent to the email address registered in VE170.314(h)(1) – 2.03 or by clicking on the "View Direct Message Status" tab on the Transport Testing Tool and looking in the Table 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)(1) – 2.03. TE170.314(h)(1) – 2.05, above. Note: There should be a different Test Session name for each C-CDA sent.

IN170.314(h)(1) – 2.04: Using the Vendor system logs, the Tester shall verify that the messages transmitted in: TE170.314(h)(1) – 2.09 , TE170.314(h)(1) – 2.13, TE170.314(h)(1) – 2.16, and TE170.314(h)(1) – 2.19 were rejected and not received by the EHR/HISP (e.g. inspecting audit logs to verify rejections)

IN170.314(h)(1) – 2.05: Using the Transport Testing Tool, the Tester shall verify that no MDN was

received in response to the messages transmitted in TE170.314(h)(1) – 2.09 , TE170.314(h)(1) – 2.13, TE170.314(h)(1) – 2.16, and TE170.314(h)(1) – 2.19 by verifying that no Validation Report was sent to the email address registered in VE170.314(h)(1) – 2.03 or by clicking on the "View Direct Message Status" tab on the Transport 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)(1) – 2.08, TE170.314(h)(1) – 2.12, TE170.314(h)(1) – 2.15 and TE170.314(h)(1) – 2.18

TEST DATA

This test procedure utilizes both Vendor-supplied and ONC-supplied 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, 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)(1) Optional – Applicability Statement for Secure Health Transport 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. 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 the Direct Certificate Discovery Tool is available at the DCDT user group: https://groups.google.com/forum/#!forum/directtesttool or by contacting:

  Matthew Rahn (Matthew.Rahn@hhs.gov)
  Office of Standards and Technology
  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.

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