

2015 Edition §170.315(h)(1) Direct Project					
Testing Components:					
				Data	
Test Procedure Version 1.1 – Last Updated 12/4/15					

Please consult the Final Rule entitled: *2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications* for a detailed description of the certification criterion with which these testing steps are associated. We also encourage developers to consult the Certification Companion Guide in tandem with the test procedure as they provide clarifications that may be useful for product development and testing.

Note: The order in which the test steps are listed reflects the sequence of the certification criterion and does not necessarily prescribe the order in which the test should take place

Required Tests

(h)(1)(i) Applicability Statement for Secure Health Transport

Able to send and receive health information in accordance with the standards specified in § 170.202(a)(2).

Standards: § 170.202 (a)(2)- [ONC Applicability Statement for Secure Health Transport v1.2](#) (incorporated by reference in § 170.299).

Tools: [Direct Certificate Discovery Tool \(DCDT\)](#)

(i) – Send

Criteria ¶	System Under Test	Test Lab Verification
(i)	<ol style="list-style-type: none"> Discover Certificates: The user performs setup tasks to discover Direct Certificate Discovery Tool (DCDT) certificates by downloading the DCDT Trust Anchor, uploading it into the Health IT module’s Direct instance, and mapping the Direct address to a non-Direct email address for receiving results Discover Certificates: The user can discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP in DCDT using identified Health IT function(s). The user selects “2014 Direct” within the Edge Testing Tool (ETT) to access the Transport Testing Tool (TTT). The user registers a Direct address within the TTT and corresponding Contact Email address for receipt of the TTT validation report within the “Register Direct” tab. The user identifies the payload for sending to the TTT. ONC-supplied payloads are available for download from the Home page of the TTT. 	<ol style="list-style-type: none"> Discover Certificates: The tester verifies the Health IT module can discover and use address-bound and domainbound certificates hosted in both DNS and LDAP in order to create and store a listing of Direct recipients using the Direct Certificate Discovery Tool. All listed certificates listed in both DNS and LDAP must be tested corresponding to the ONC Applicability Statement for Secure Health Transport v1.2. The tester verifies the Health IT module can register a Direct email address using the TTT and has supplied a corresponding Contact Email address for receipt of the TTT validation report. Using the TTT validation report, the tester verifies the payload sent to the TTT is encrypted using the TTT’s Public Key and signed using the Health IT module’s Private Key.

Criteria ¶	System Under Test	Test Lab Verification
	<p>6. The user sends encrypted and signed health information to a third party (TTT) using Direct in accordance with the standard specified at §170.202(a)(2): ONC Applicability Statement for Secure Health Transport using identified Health IT function(s).</p> <p>7. Based upon the types of Direct messages the Health IT Module supports for sending of information (“wrapped” RFC-5751 messages required), the user sends health information to a third party using Direct in accordance with the standard specified at §170.202(a)(2) ONC Applicability Statement for Secure Health Transport.</p> <p>8. The user provides evidence and demonstrates of successful send of encrypted and signed health information from the Health IT module to 3 partners (e.g., Other vendor Health IT modules (HISPs) that have implemented (h)(1) or (h)(2) capabilities) using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport, which includes:</p> <ul style="list-style-type: none"> • Documentation of the Health IT module sending “Wrapped” RFC-5751 messages to 3 partner HISPs • Demonstration of the Health IT module receiving processed Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT module. 	<p>4. Using the TTT validation report, the tester verifies the identified health information is successfully transmitted to a third party using Direct in accordance with the standard specified at §170.202(a)(2), using the RFC-5751 “wrapped” message format.</p> <p>5. Using the validation report, the tester verifies that the payload was successfully received by the TTT, and that the TTT was able to successfully decrypt the message.</p> <p>6. The tester verifies that the Health IT module has successfully sent encrypted and signed health information to 3 partner HISPs using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport. The verification includes:</p> <ul style="list-style-type: none"> • Indication through documentation that the Health IT module sent “Wrapped” RFC-5751 messages • Evidence through demonstration of the Health IT module receiving processed Message Disposition Notifications (MDNs) from each of the 3 partner HISPs generated upon receiving the Direct message from the Health IT module.

(i) – Receive

Criteria ¶	System Under Test	Test Lab Verification
(i)	<ol style="list-style-type: none"> 1. Hosting Certificates: The user performs setup tasks to test hosting of certificates by entering the Health IT module’s Direct address within DCDT. 2. Hosting Certificates: The user executes test cases based upon whether the Health IT module is able to host either address-bound or domain-bound certificates in either DNS or LDAP servers using the DCDT. 3. The user selects “2014 Direct” within the ETT to access the Transport Testing Tool (TTT). 4. The user selects the “Send Direct Message” tab and completes the required information, identifying the Direct Address for testing receipt and digital sign of health information in accordance with the standard specified at §170.202(a)(2): ONC Applicability Statement for Secure Health Transport. 5. The user installs the TTT’s Valid Trust Anchor within the Health IT module. 6. The user identifies the Health IT module’s Public Key for encryption of messages to be sent by TTT to the Health IT module. 7. The user receives RFC-5751 “wrapped” health information sent from TTT using Direct in accordance with the standard specified at §170.202(a)(2) ONC Applicability Statement for Secure Health Transport and sends corresponding MDNs. 8. The user rejects health information sent from TTT that is not in accordance with the standard specified at §170.202(a)(2) ONC Applicability Statement for Secure Health Transport. 9. The user provides evidence of successful receipt of encrypted and signed health information from 3 partners (e.g., Other vendor Health IT modules (HISPs) that have implemented (h)(2) capabilities) using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport. The evidence includes documentation of: 	<ol style="list-style-type: none"> 1. Hosting Certificates: The tester verifies that the Health IT module’s hosted certificates are discoverable as displayed on screen for the DCDT test cases executed. 2. The tester verifies that health information can be successfully received by the Health IT module from the TTT accordance with the standard specified at §170.202(a)(2), using “wrapped” RFC-5751 messages. 3. The tester verifies that an MDN from the Health IT module was received from the TTT for all messages in Step 2. 4. Negative Test: The tester verifies that the Health IT module rejects Direct messages received with an invalid Trust Anchor and no corresponding MDN was received by the TTT 5. Negative Test: The tester verifies that the Health IT module rejects Direct messages received with an invalid Trust Anchor and invalid certificate. The tester verifies that no corresponding MDN was received by the TTT. 6. Negative Test: The tester verifies that the Health IT module rejects Direct messages received with an expired certificate. The tester verifies that no corresponding MDN was received by the TTT. 7. Negative Test: The tester verifies that the Health IT module rejects Direct messages received with an invalid Trust Relationship. The tester verifies that no corresponding MDN was received by the TTT. 8. Negative Test: The tester verifies that the Health IT module rejects Direct messages received without an Authority Information Access (AIA) extension. The tester verifies that no corresponding MDN was received by the TTT.

Criteria ¶	System Under Test	Test Lab Verification
	<ul style="list-style-type: none"> The Health IT module receiving “Wrapped” RFC-5751 messages from 3 partner HISPs The Health IT module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the 3 partner HISPs generated upon successfully receiving a Direct message from the Health IT module. 	<p>9. Negative Test: The tester verifies that the Health IT module rejects Direct messages received with an invalid message digest. The tester verifies that no corresponding MDN was received by the TTT.</p> <p>10. The tester verifies that the Health IT module has received encrypted and signed health information from 3 partner HISPs using Direct v1.2 in accordance with the standard specified at §170.202(a)(2): Applicability Statement for Secure Health Transport. The documentation includes:</p> <ul style="list-style-type: none"> Indication that the Health IT module successfully received “Wrapped” RFC-5751 messages Evidence of the Health IT module generating and transmitting processed Message Disposition Notifications (MDNs) to each of the 3 partner HISPs generated upon receiving the Direct message from the partner HISP.

(ii) Applicability Statement for Secure Health Transport and Delivery Notification in Direct

Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

Standards: § 170.202 (e)(1)Delivery Notification - [ONC Implementation Guide for Delivery Notification in Direct v1.0](#).

Tools: [Edge Testing Tool \(ETT\)](#)

(ii) – Send

Criteria ¶	System Under Test	Test Lab Verification
(ii)	<ol style="list-style-type: none"> 1. Enter the Health IT module's profile information into the Edge Testing Tool (ETT) with HISP as Sender. 2. Execute ETT Test Cases for HISP as Sender. 	<ol style="list-style-type: none"> 1. (Successful Flow 1): The tester verifies the Health IT module sends both a successful hand-off message and success notification to the ETT (as Sending Edge) if no security and trust processing is necessary. 2. (Successful Flow 2): The tester verifies the Health IT module returns a successful hand-off status to the ETT (as Sending Edge) upon receipt of the message. 3. (Successful Flow 2): The tester verifies a processed MDN is received by the Health IT module and is decrypted with trust verified. 4. (Successful Flow 2): The tester verifies a dispatched MDN is received by the Health IT module and is decrypted with trust verified. 5. (Successful Flow 2): The tester verifies the Health IT module sends a success notification to the Sending Edge Client. 6. Negative Test (Delivery Failure Flow 1): The tester verifies the Health IT module returns an Error Condition to the Sending Edge Client when it cannot encrypt and/or sign the message or does not trust a recipient due to trust validation issues. This can be due to: <ul style="list-style-type: none"> • Sending Edge Client is not authenticated or authorized; • Message is invalid; or • For internal Health IT Module communication, a failure may indicate a message delivery failure if the Health IT module implements synchronous delivery. 7. Negative Test (Delivery Failure Flow 2): The tester verifies the Health IT module returns a successful hand-off status message to the ETT (as Sending Edge Client) followed by a Failure Notification to the Sending Edge Client when the security and trust process fails. This can be due to: <ul style="list-style-type: none"> • Trust relationship not established with the ETT (as Receiving HISP); • Sending Edge Client's certificate and/or private key could not be resolved; • Sending Edge Client's certificate is expired or revoked; • The ETT (as Receiving HISP)'s certificate could not be resolved; • The ETT (as Receiving HISP)'s certificate is expired or revoked; or • The ETT (as Receiving HISP)'s certificate does not meet Health IT module's certificate policies 8. Negative Test (Delivery Failure Flow 3): The tester verifies the Health IT module returns a Failure Notification to the Sending Edge Client when the ETT (as Receiving HISP) returns an SMTP error. This can be due to: <ul style="list-style-type: none"> • The Health IT module has been blacklisted by the ETT (as Receiving HISP) SMTP server; • Message exceeds size limit; • Invalid SMTP header format (invalid address format); or • Invalid message format.

Criteria ¶	System Under Test	Test Lab Verification
(ii)		<p>9. Negative Test (Delivery Failure Flow 4): The tester verifies the Health IT module returns a successful hand-off status message followed by a Failure Notification to the Sending Edge Client when the wait time between successfully sending the message to the ETT (as Receiving HISP) wait time for the Health IT module to receive a processed MDN from the ETT (as Receiving HISP) been exceeded.</p> <p>10. Negative Test (Delivery Failure Flow 5): The tester verifies the Health IT module returns a successful hand-off status message followed by a Failure Notification to the ETT (as Sending Edge Client) when the Health IT module cannot deliver a message to its destination when no security and trust processing is necessary. This can be due to:</p> <ul style="list-style-type: none"> • Delivery components are malfunctioning or unavailable; • The final destination does not exist (invalid address); or • The final destination is full (mail box over quota). <p>11. Negative Test (Delivery Failure Flow 6): The tester verifies that Health IT module returns a successful hand-off message, receives, decrypts, and verifies trust of a processed MDN message received from the ETT (as Receiving HISP), and then generates a Failure Notification to the Sending Edge Client. The Health IT module receives, decrypts, and verifies trust of a MDN failed message from the ETT (as Receiving HISP).</p> <p>12. Negative Test (Notification Failure Flow 1): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful hand-off status message upon message receipt; successfully encrypts and signs the message for sending to the ETT (as Receiving HISP); receives, decrypts, and verifies trust of a processed MDN from the ETT (as Receiving HISP); generates and sends a Failure Notification to the ETT (as Sending Edge) when the wait time for receiving a dispatched MDN message from the ETT (as Receiving HISP) has been exceeded.</p> <p>13. Negative Test (Notification Failure Flow 2): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful hand-off status message. The tester verifies a Failure Notification is sent by the Health IT module to the ETT (as Sending Edge) when the wait time for receiving a processed MDN from the ETT (as Receiving HISP) has been exceeded. The tester verifies that if a subsequent dispatched MDN message is received by the Health IT module from the ETT (as Receiving HISP) indicating the message has reached its final destination, no success message is sent to the ETT (as Sending Edge).</p> <p>14. Negative Test (Notification Failure Flow 3): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful hand-off status message and receives a dispatched MDN message from the ETT (as Receiving HISP) before receiving a processed MDN message from the ETT (as Receiving HISP). The wait time for receipt of a processed MDN has not been exceeded. The tester verifies the Health IT module sends a success notification of delivery of the message to the ETT (as Sending Edge).</p>

Criteria ¶	System Under Test	Test Lab Verification
(ii)		<p>15. Negative Test (Notification Failure Flow 4): The tester verifies the Health IT module sends the ETT (as Sending Edge) a successful hand-off status message. The tester verifies a Failure Notification is sent by the Health IT module to the ETT (as Sending Edge) when the wait time for receiving a processed MDN from the ETT (as Receiving HISP) has been exceeded. The tester verifies that if a subsequent failed MDN message is received by the Health IT module from the ETT (as Receiving HISP), no further messages are sent to the ETT (as Sending Edge).</p> <p>16. Negative Test (Notification Failure Flow 5): The tester verifies that the Health IT module sends the ETT (as Sending Edge) a successful hand-off status message, followed by a Failure Notification if the Health IT module receives a MDN failed message from the ETT (as Receiving HISP) prior to the wait time for receiving a processed MDN from the ETT (as Receiving HISP) message has been exceeded.</p>

(ii) – Receive

Criteria ¶	System Under Test	Test Lab Verification
(ii)	<ol style="list-style-type: none"> 1. Enter the Health IT module's profile information into the ETT with HISP as Receiver. 2. Enter the Health IT module's profile information into the ETT with HISP as Receiver. 	<ol style="list-style-type: none"> 1. (Successful Flow 2): The tester verifies the Health IT module can successfully receive a message from the ETT (as Sending HISP). 2. (Successful Flow 2): The tester verifies the Health IT module generates, encrypts, and signs a processed MDN message to the ETT (as Sending HISP) upon successfully receiving decrypting, and validating trust. 3. (Successful Flow 2): The tester verifies the Health IT module generates, encrypts, and signs a dispatched MDN message to the ETT (as Sending HISP) upon receiving a success notification of delivery of the message from the ETT (as Receiving Edge Client). 4. Negative Test (Delivery Failure Flow 3): The tester verifies the Health IT module sends an SMTP error code to the ETT (as Sending HISP) when rejecting a message due to: <ul style="list-style-type: none"> • ETT (as Sending HISP) has been blacklisted by the Health IT module's SMTP server; • Message exceeds size limit; • Invalid SMTP header format (invalid address format); or • Invalid message format. 5. Negative Test (Delivery Failure Flow 4): The tester verifies the Health IT module successfully receives the message, but does not send a processed MDN to the ETT (as Sending HISP), but does not pass security and trust validation due to: <ul style="list-style-type: none"> • Trust relationship not established with ETT (as Sending HISP); • ETT (as Sending HISP)'s certificate could not be resolved; • ETT (as Sending HISP)'s certificate is expired or revoked; • ETT (as Sending HISP)'s certificate does not meet Health IT module's certificate policies; or • Message is not encrypted or signed. 6. Negative Test (Delivery Failure Flow 6): The tester verifies the Health IT module successfully receives the message, generates, encrypts, and signs a processed MDN, but then is unable to deliver the message to its destination. The tester verifies the Health IT module generates, encrypts, and signs a failed MDN message to the ETT (as Sending HISP).

Document History

Version Number	Description of Change	Date
1.0	Released for Comment - NPRM	March 31, 2015
1.1	Released for Comment - FR	October 30, 2015
1.2	Updated and Released for Comment	December 4, 2015

Dependencies: For all related and required criteria, please refer to the [Master Table of Related and Required Criteria](#).