Direct Project, Edge Protocol, and XDR/XDM

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 03-21-2025

Regulation Text

Regulation Text

§ 170.315 (h)(2) *Direct Project, Edge Protocol, and XDR/XDM—*

1. Able to send and receive health information in accordance with:
    1. The standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message;
    2. The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and
    3. Both edge protocol methods specified by the standard in § 170.202(d).
2. *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

Standard(s) Referenced

Paragraph (h)(2)(i)(A)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.2, August 2015

Paragraph (h)(2)(i)(B)

§ 170.202(b) ONC XDR and XDM for Direct Messaging Specification

Paragraph (h)(2)(i)(C)

§ 170.202(d) ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014

Paragraph (h)(2)(ii)

§ 170.202(e)(1) Delivery Notification - Implementation Guide for Delivery Notification in Direct v1.0

Standard Version Advancement Process (SVAP) Version(s) Approved

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing: Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.

Privacy & Security Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(h)(2). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(h) criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (h) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "View, download, and transmit to 3rd party (VDT)" and (e)(2) "Secure messaging," which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

If choosing Approach 2:

For each applicable privacy and security certification criterion not certified using Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with new SITE UI language	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (h)(2) *Direct Project, Edge Protocol, and XDR/XDM—*

1. Able to send and receive health information in accordance with:
    1. The standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message;
    2. The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and
    3. Both edge protocol methods specified by the standard in § 170.202(d).
2. *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

Standard(s) Referenced

Paragraph (h)(2)(i)(A)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.2, August 2015

Paragraph (h)(2)(i)(B)

§ 170.202(b) ONC XDR and XDM for Direct Messaging Specification

Paragraph (h)(2)(i)(C)

§ 170.202(d) ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014

Paragraph (h)(2)(ii)

§ 170.202(e)(1) Delivery Notification - Implementation Guide for Delivery Notification in Direct v1.0

Standard Version Advancement Process (SVAP) Version(s) Approved

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies
Conditions and Maintenance of Certification

Real World Testing: Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.

Privacy & Security Requirements
Privacy and Security: This certification criterion was adopted at § 170.315(h)(2). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(h) criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (h) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

If choosing Approach 2:

For each applicable privacy and security certification criterion not certified using Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Testing
Testing Tool

Standards Implementation & Testing Environment (SITE): Direct Tooling, Send Direct Message

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(h)(2)	Refer to the Standards Implementation & Testing Environment (SITE)

Revision History

Version #	Description of Change	Version Date

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with new SITE UI language	03-21-2025

This Test Procedure illustrates the test steps required to certify a Health IT Module to this criterion. Please consult the most recent Final Rules on the Certification Regulations page for a detailed description of the certification criterion with which these testing steps are associated. ASTP/ONC also encourages developers to consult the Certification Companion Guide in tandem with the test procedure as it provides clarifications that may be useful for product development and testing.

Note: The test step order does not necessarily prescribe the order in which the tests should take place.

Testing components

ONC
Supplied
Test
Data

SVAP

Paragraph (h)(2)(i)(A) – Send

System Under Test

Discover Certificates

1. The user performs setup tasks to discover Direct Certificate Discovery Tool (DCDT) certificates (by downloading the DCDT Trust Anchor from ASTP's Standards Implementation & Testing Environment (SITE): Direct Tooling for H2, "Discovery Test Tool," uploading it into the Health IT Module's Direct instance, and mapping the Direct address to a non-Direct email address for receiving results) so that 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).

Register Direct Address

2. The user selects "Register Direct" within SITE: Direct Tooling for H2 selecting the category Send and sub-category Paragraph (i) Register Direct and registers a Direct address within SITE and corresponding Contact Email address for receipt of SITE validation report.

Send Health Information Using Direct

3. Using the Send Direct tool under Direct Tooling for H2, the user identifies the payload for sending to SITE via Direct. ASTP/ONC-supplied payloads are available for download from the SITE Resources-Documentation page.
4. The user sends encrypted and signed health information to a third party (SITE) using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015 using identified health IT function(s).
5. 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) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015.

Approved SVAP Version(s)

Complete steps 2-5 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

Discover Certificates

1. The tester verifies the Health IT Module can discover and use address-bound and domain-bound 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 certificates listed in both DNS and LDAP must be tested corresponding to the standard specified at § 170.202(a)(2).

Register Direct Address

2. The tester verifies the Health IT Module can register a Direct email address using SITE and has supplied a corresponding Contact Email address for receipt of SITE validation report.

Send Health Information Using Direct

3. Using SITE validation report, the tester verifies the payload sent to SITE is encrypted using the SITE's Public Key and signed using the Health IT Module's Private Key.
4. Using SITE 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.
5. Using the validation report, the tester verifies the payload was successfully received by SITE and that SITE was able to successfully decrypt the message.

Approved SVAP Version(s)

Complete verification for step 3-5 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

System Under Test

Discover Certificates

1. The user performs setup tasks to discover Direct Certificate Discovery Tool (DCDT) certificates (by downloading the DCDT Trust Anchor from ASTP's Standards Implementation & Testing Environment (SITE): Direct Tooling for H2, "Discovery Test Tool," uploading it into the Health IT Module's Direct instance, and mapping the Direct address to a non-Direct email address for receiving results) so that 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).

Register Direct Address

2. The user selects "Register Direct" within SITE: Direct Tooling for H2 selecting the category Send and sub-category Paragraph (i) Register Direct and registers a Direct address within SITE and corresponding Contact Email address for receipt of SITE validation report.

Send Health Information Using Direct

Test Lab Verification

Discover Certificates

1. The tester verifies the Health IT Module can discover and use address-bound and domain-bound 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 certificates listed in both DNS and LDAP must be tested corresponding to the standard specified at § 170.202(a)(2).

Register Direct Address

System Under Test

3. Using the Send Direct tool under Direct Tooling for H2, the user identifies the payload for sending to SITE via Direct. ASTP/ONC-supplied payloads are available for download from the SITE Resources-Documentation page.
4. The user sends encrypted and signed health information to a third party (SITE) using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015 using identified health IT function(s).
5. 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) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015.

Approved SVAP Version(s)

Complete steps 2-5 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

2. The tester verifies the Health IT Module can register a Direct email address using SITE and has supplied a corresponding Contact Email address for receipt of SITE validation report.

Send Health Information Using Direct

3. Using SITE validation report, the tester verifies the payload sent to SITE is encrypted using the SITE's Public Key and signed using the Health IT Module's Private Key.
4. Using SITE 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.
5. Using the validation report, the tester verifies the payload was successfully received by SITE and that SITE was able to successfully decrypt the message.

Approved SVAP Version(s)

Complete verification for step 3-5 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(A) – Receive

System Under Test

Hosting Certificates

1. The user performs setup tasks to test hosting of certificates by entering the Health IT Module's Direct address within SITE: Direct Tooling for H2, selecting "Receive," then subcategory Paragraph (i) Certificate Discovery / Hosting – DCDT and executing 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.

SUT Connection

2. The user selects the "Send Direct Message" within SITE: Direct Tooling for H2 and performs setup tasks to enable the receipt of Direct Messages including:
    - Completion of the required information, identifying the Direct Address for testing receipt and digital signing of health information in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015.
    - Installation of the SITE's Valid Trust Anchor within the Health IT Module.
    - Identification and upload of the Health IT Module's Public Key for encryption of messages to be sent by SITE to the Health IT Module.

Receive Direct Message

3. The user receives RFC-5751, "wrapped" health information sent from SITE using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015 and sends corresponding MDNs.

Reject Receipt of Direct Message (Negative Testing)

4. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Invalid Certificate.
5. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Expired Certificate.
6. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).

7. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
8. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Invalid Message Digest.

Approved SVAP Version(s)

Complete steps 2-8 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

Hosting Certificates

1. The tester verifies the Health IT Module's hosted certificates are discoverable as displayed on screen for the DCDT test cases executed.

SUT Connection

2. No action required.

Receive Direct Message

3. The tester verifies that:
    - The health information can be successfully received by the Health IT Module from SITE in accordance with the standard specified at § 170.202(a)(2) using "wrapped" RFC-575,1 messages.
    - An MDN from the Health IT Module was received from SITE for all messages in Step 3 of the SUT.

Reject Receipt of Direct Message (Negative Testing)

4. Invalid Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Certificate and no corresponding MDN was received by SITE from the Health IT Module.
5. Expired Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Expired Certificate and no corresponding MDN was received by SITE from the Health IT Module.

6. Invalid Trust Relationship (Different Trust Anchor): The tester verifies the Health IT Module rejects Direct messages received with an Invalid Trust Relationship (Different Trust Anchor) and no corresponding MDN was received by SITE from the Health IT Module.
7. No Authority Information Access (AIA) extension: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Certificate and no corresponding MDN was received by SITE from the Health IT Module.
8. Invalid Message Digest: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Message Digest and no corresponding MDN was received by SITE from the Health IT Module.

Approved SVAP Version(s)

Complete steps 3-8 verification against the testing outcomes in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

System Under Test

Hosting Certificates

1. The user performs setup tasks to test hosting of certificates by entering the Health IT Module's Direct address within SITE: Direct Tooling for H2, selecting "Receive," then subcategory Paragraph (i) Certificate Discovery / Hosting – DCDT and executing 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.

SUT Connection

Test Lab Verification

Hosting Certificates

1. The tester verifies the Health IT Module's hosted certificates are discoverable as displayed on screen for the DCDT test cases executed.

SUT Connection

2. No action required.

Receive Direct Message

System Under Test

2. The user selects the “Send Direct Message” within SITE: Direct Tooling for H2 and performs setup tasks to enable the receipt of Direct Messages including:
    - Completion of the required information, identifying the Direct Address for testing receipt and digital signing of health information in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015.
    - Installation of the SITE’s Valid Trust Anchor within the Health IT Module.
    - Identification and upload of the Health IT Module’s Public Key for encryption of messages to be sent by SITE to the Health IT Module.

Receive Direct Message

3. The user receives RFC-5751, “wrapped” health information sent from SITE using Direct in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015 and sends corresponding MDNs.

Reject Receipt of Direct Message (Negative Testing)

4. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Invalid Certificate.
5. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Expired Certificate.
6. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).

Test Lab Verification

3. The tester verifies that:
    - The health information can be successfully received by the Health IT Module from SITE in accordance with the standard specified at § 170.202(a)(2) using “wrapped” RFC-575,1 messages.
    - An MDN from the Health IT Module was received from SITE for all messages in Step 3 of the SUT.

Reject Receipt of Direct Message (Negative Testing)

4. Invalid Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Certificate and no corresponding MDN was received by SITE from the Health IT Module.
5. Expired Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Expired Certificate and no corresponding MDN was received by SITE from the Health IT Module.
6. Invalid Trust Relationship (Different Trust Anchor): The tester verifies the Health IT Module rejects Direct messages received with an Invalid Trust Relationship (Different Trust Anchor) and no corresponding MDN was received by SITE from the Health IT Module.

System Under Test

7. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
8. The user rejects health information that is not in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 sent from SITE to the Health IT Module using the following tool option: Invalid Message Digest.

Approved SVAP Version(s)

Complete steps 2-8 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

7. No Authority Information Access (AIA) extension: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Certificate and no corresponding MDN was received by SITE from the Health IT Module.
8. Invalid Message Digest: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Message Digest and no corresponding MDN was received by SITE from the Health IT Module.

Approved SVAP Version(s)

Complete steps 3-8 verification against the testing outcomes in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(B) – Send using Direct + XDM

System Under Test

Discover Certificates

1. The user performs setup tasks to discover Direct Certificate Discovery Tool (DCDT) certificates (by downloading the DCDT Trust Anchor from the SITE: Direct Tooling for H2, choosing "Send using Direct+XDM", then subcategory Paragraph (i) Certificate Discovery/Hosting - DCDT, uploading it into the Health IT Module's Direct instance and mapping the Direct address to a non-Direct email address for receiving results) so that the user can discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP in DCDT using developer-identified health IT function(s).

Register Direct Address

2. The user selects “Register Direct” within SITE: Direct Tooling for H2 and registers a Direct address within SITE and optionally a corresponding Contact Email address for receipt of the SITE validation report.

Send Health Information Using Direct with XDR/XDM

3. The user identifies the payload for sending to SITE via Direct with XDM Validation. ASTP/ONC-supplied payloads are available for download from SITE: Documentation, C-CDA USCDI Certification Test Data.
4. The user sends encrypted and signed health information to a third party in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification using limited metadata, using RFC-5751, “wrapped” messages.
5. The user sends encrypted and signed health information to a third party, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification using full metadata, using RFC-5751, “wrapped” messages.
6. The XDM package sent by the Health IT Module is able to be successfully validated using SITE: Direct Tooling for H2, "XDM Validator."

Approved SVAP Version(s)

Complete steps 2 – 6 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

Discover Certificates

1. The tester verifies the Health IT Module can discover and use address-bound and domain-bound 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 certificates listed in both DNS and LDAP must be tested corresponding to the § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015.

Register Direct Address

2. The tester verifies the Health IT Module can register a Direct email address using SITE and if supplied a corresponding Contact Email address for receipt of SITE validation report.

Send Health Information Using Direct with XDR/XDM

3. Using the SITE validation report, the tester verifies the payload sent to SITE is encrypted using the SITE's Public Key and signed using the Health IT Module's Private Key.
4. Using SITE validation report, the tester verifies the identified health information is successfully transmitted to a third party using Direct with XDR/XDM, in accordance with the standard specified at § 170.202(b), using RFC-5751, "wrapped" messages.
5. Using the validation report, the tester verifies the payload using limited XDS metadata was successfully received by SITE and that SITE was able to successfully decrypt the message.
6. Using the XDM payload available for download within the validation report, the tester uploads the XDM payloads (sent using both limited and full metadata) to SITE's XDM Message Validator. The tester reviews SITE validation report to verify the XDM package is valid.

Approved SVAP Version(s)

Complete step 2 – 6 verifications in accordance with the ONC Applicability Statement for Secure Health Transport v1.3, May 2021 (Direct v1.3)

System Under Test

Discover Certificates

1. The user performs setup tasks to discover Direct Certificate Discovery Tool (DCDT) certificates (by downloading the DCDT Trust Anchor from the SITE: Direct Tooling for H2, choosing "Send using Direct+XDM", then subcategory Paragraph (i) Certificate Discovery/Hosting - DCDT, uploading it into the Health IT Module's Direct instance and mapping the Direct address to a non-Direct email address for receiving results) so that the user can discover and use address-bound and domain-bound certificates hosted in both DNS and LDAP in DCDT using developer-identified health IT function(s).

Register Direct Address

2. The user selects "Register Direct" within SITE: Direct Tooling for H2 and registers a Direct address within SITE and optionally a corresponding Contact Email address for receipt of the SITE validation report.

Send Health Information Using Direct with XDR/XDM

Test Lab Verification

Discover Certificates

1. The tester verifies the Health IT Module can discover and use address-bound and domain-bound 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 certificates listed in both DNS and LDAP must be tested corresponding to the § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015.

Register Direct Address

2. The tester verifies the Health IT Module can register a Direct email address using SITE and if supplied a corresponding Contact Email address for receipt of SITE validation report.

System Under Test

3. The user identifies the payload for sending to SITE via Direct with XDM Validation. ASTP/ONC-supplied payloads are available for download from SITE: Documentation, C-CDA USCDI Certification Test Data.
4. The user sends encrypted and signed health information to a third party in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification using limited metadata, using RFC-5751, “wrapped” messages.
5. The user sends encrypted and signed health information to a third party, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification using full metadata, using RFC-5751, “wrapped” messages.
6. The XDM package sent by the Health IT Module is able to be successfully validated using SITE: Direct Tooling for H2, "XDM Validator."

Approved SVAP Version(s)

Complete steps 2 – 6 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

Send Health Information Using Direct with XDR/XDM

3. Using the SITE validation report, the tester verifies the payload sent to SITE is encrypted using the SITE’s Public Key and signed using the Health IT Module’s Private Key.
4. Using SITE validation report, the tester verifies the identified health information is successfully transmitted to a third party using Direct with XDR/XDM, in accordance with the standard specified at § 170.202(b), using RFC-5751, ”wrapped” messages.
5. Using the validation report, the tester verifies the payload using limited XDS metadata was successfully received by SITE and that SITE was able to successfully decrypt the message.
6. Using the XDM payload available for download within the validation report, the tester uploads the XDM payloads (sent using both limited and full metadata) to SITE’s XDM Message Validator. The tester reviews SITE validation report to verify the XDM package is valid.

Approved SVAP Version(s)

Complete step 2 – 6 verifications in accordance with the ONC Applicability Statement for Secure Health Transport v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(B) – Send conversion using XDR

System Under Test

1. Using the SITE: Direct Tooling for H2, HISP Testing Portal, "Sender," the Health IT Module receives a Direct message from SITE (as Sending HISP), translates it to an XDR message, and sends it to SITE (as Edge) (XDR Test 10).
2. The Health IT Module receives a Direct + XDM message from SITE (as Sending HISP), translates it to an XDR message with Limited Metadata, and sends it to SITE (as Edge) (XDR Test 11).
3. The Health IT Module receives a Direct + XDM message from SITE (as Sending HISP), translates it to an XDR message with Full Metadata sent to SITE (as Edge) (XDR Test 12).

Approved SVAP Version(s)

Complete steps 1, 2, and 3 for XDR Tests 10, 11, and 12 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

1. Using the visual inspection, the tester verifies the Direct Message was received, translated, and transmitted as an XDR to SITE (as Edge) (XDR Test 10).
2. Using the visual inspection, the tester verifies the Direct + XDM message was received, translated, and transmitted as an XDR to SITE (as Edge) using Limited Metadata (XDR Test 11).
3. Using the visual inspection, the tester verifies the Direct + XDM message received, translated, and transmitted as an XDR to SITE (as Edge) using Full Metadata (XDR Test 12).

Approved SVAP Version(s)

Complete steps 1-3 verifications using visual inspection for XDR tests 10, 11, and 12 in accordance with the ONC Applicability Statement for Secure Health Transport v1.3, May 2021 (Direct 1.3)

System Under Test	Test Lab Verification

System Under Test

1. Using the SITE: Direct Tooling for H2, HISP Testing Portal, "Sender," the Health IT Module receives a Direct message from SITE (as Sending HISP), translates it to an XDR message, and sends it to SITE (as Edge) (XDR Test 10).
2. The Health IT Module receives a Direct + XDM message from SITE (as Sending HISP), translates it to an XDR message with Limited Metadata, and sends it to SITE (as Edge) (XDR Test 11).
3. The Health IT Module receives a Direct + XDM message from SITE (as Sending HISP), translates it to an XDR message with Full Metadata sent to SITE (as Edge) (XDR Test 12).

Approved SVAP Version(s)

Complete steps 1, 2, and 3 for XDR Tests 10, 11, and 12 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

1. Using the visual inspection, the tester verifies the Direct Message was received, translated, and transmitted as an XDR to SITE (as Edge) (XDR Test 10).
2. Using the visual inspection, the tester verifies the Direct + XDM message was received, translated, and transmitted as an XDR to SITE (as Edge) using Limited Metadata (XDR Test 11).
3. Using the visual inspection, the tester verifies the Direct + XDM message received, translated, and transmitted as an XDR to SITE (as Edge) using Full Metadata (XDR Test 12).

Approved SVAP Version(s)

Complete steps 1-3 verifications using visual inspection for XDR tests 10, 11, and 12 in accordance with the ONC Applicability Statement for Secure Health Transport v1.3, May 2021 (Direct 1.3)

Paragraph (h)(2)(i)(B) – Receive using Direct + XDM

System Under Test

Hosting Certificates

1. The user performs setup tasks to test hosting of certificates (by entering the Health IT Module's Direct address within SITE: Direct Tooling, "Discovery Test Tool") and 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.

SUT Connection

2. The user selects “Send Direct Email” within SITE: Direct Tooling for H2 and performs setup tasks to enable the receipt of Direct with XDR/XDM Messages including:
    - Completion of the required information, identifying the Direct Address for testing receipt and digital signing of health information in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification.
    - Installation of the SITE's Valid Trust Anchor within the Health IT Module.
    - Identification and upload of the Health IT Module’s Public Key for encryption of messages to be sent by SITE to the Health IT Module.

Receive Direct + XDR/XDM Message

3. The user receives health information sent from SITE using Direct in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification with limited metadata and sends corresponding MDNs, using RFC-5751 “wrapped” messages.
4. The user receives health information sent from SITE using Direct in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification with full metadata and sends corresponding MDNs.

Validate XDM Package

5. The user uploads the XDM payload received from SITE to SITE: “XDM Validator” to perform validation of the XDM package.

Reject Receive of Direct Message (Negative Testing)

6. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Invalid Certificate.
7. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Expired Certificate.
8. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).
9. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
10. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Invalid Message Digest.

Approved SVAP Version(s)

Complete steps 2-4 in accordance with the ONC Applicability Statement for Secure Health Transport v1.3, May 2021 (Direct v1.3)

Test Lab Verification

Hosting Certificates

1. The tester verifies the Health IT Module's hosted certificates are discoverable as displayed on screen for the DCDT test cases executed.

SUT Connection

2. No Action Required.

Receive Direct + XDR/XDM Message

3. The tester verifies health information can be successfully received by the Health IT Module from SITE in accordance with the standard specified at § 170.202(b) using the limited XDS metadata profile, using RFC-5751, "wrapped" messages and that an MDN from the Health IT Module was received by SITE for all messages.
4. The tester verifies health information can be successfully received by the Health IT Module from SITE in accordance with the standard specified at § 170.202(b), using the full XDS metadata profile and using RFC-5751, "wrapped" messages and that an MDN from the Health IT Module was received by SITE for all messages.

Validate XDM Package

5. Using the SITE validation report, the tester verifies the XDM payload received by the Health IT Module and uploaded to SITE Validator successfully passes XDM validation.

Reject Receive of Direct Message (Negative Testing)

6. Invalid Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Certificate and that no corresponding MDN was received by SITE from the Health IT Module.
7. Expired Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Expired Certificate and that no corresponding MDN was received by SITE from the Health IT Module.
8. Invalid Trust Relationship (Different Trust Anchor): The tester verifies the Health IT Module rejects Direct messages received with an Invalid Trust Relationship (Different Trust Anchor) and that no corresponding MDN was received by SITE from the Health IT Module.

9. No Authority Information Access (AIA) extension: The tester verifies the Health IT Module rejects Direct messages received with No Authority Information Access (AIA) extension and that no corresponding MDN was received by SITE from the Health IT Module.
10. Invalid Message Digest: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Message Digest and that no corresponding MDN was received by SITE from the Health IT Module.

Approved SVAP Version(s)

Complete steps 3-4 verifications in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

System Under Test

Hosting Certificates

1. The user performs setup tasks to test hosting of certificates (by entering the Health IT Module's Direct address within SITE: Direct Tooling, "Discovery Test Tool") and 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.

SUT Connection

Test Lab Verification

Hosting Certificates

1. The tester verifies the Health IT Module's hosted certificates are discoverable as displayed on screen for the DCDT test cases executed.

SUT Connection

2. No Action Required.

Receive Direct + XDR/XDM Message

3. The tester verifies health information can be successfully received by the Health IT Module from SITE in accordance with the standard specified at § 170.202(b) using the limited XDS metadata profile, using RFC-5751, "wrapped" messages and that an MDN from the Health IT Module was received by SITE for all messages.
4. The tester verifies health information can be successfully received by the Health IT Module from SITE in accordance with the standard specified at § 170.202(b), using the full XDS metadata profile and using RFC-5751, "wrapped" messages and that an MDN from the Health IT Module was received by SITE for all messages.

Validate XDM Package

System Under Test

2. The user selects “Send Direct Email” within SITE: Direct Tooling for H2 and performs setup tasks to enable the receipt of Direct with XDR/XDM Messages including:
    - Completion of the required information, identifying the Direct Address for testing receipt and digital signing of health information in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification.
    - Installation of the SITE's Valid Trust Anchor within the Health IT Module.
    - Identification and upload of the Health IT Module’s Public Key for encryption of messages to be sent by SITE to the Health IT Module.

Receive Direct + XDR/XDM Message

3. The user receives health information sent from SITE using Direct in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification with limited metadata and sends corresponding MDNs, using RFC-5751 “wrapped” messages.
4. The user receives health information sent from SITE using Direct in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification with full metadata and sends corresponding MDNs.

Validate XDM Package

5. The user uploads the XDM payload received from SITE to SITE: “XDM Validator” to perform validation of the XDM package.

Reject Receive of Direct Message (Negative Testing)

Test Lab Verification

5. Using the SITE validation report, the tester verifies the XDM payload received by the Health IT Module and uploaded to SITE Validator successfully passes XDM validation.

Reject Receive of Direct Message (Negative Testing)

6. Invalid Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Certificate and that no corresponding MDN was received by SITE from the Health IT Module.
7. Expired Certificate: The tester verifies the Health IT Module rejects Direct messages received with an Expired Certificate and that no corresponding MDN was received by SITE from the Health IT Module.
8. Invalid Trust Relationship (Different Trust Anchor): The tester verifies the Health IT Module rejects Direct messages received with an Invalid Trust Relationship (Different Trust Anchor) and that no corresponding MDN was received by SITE from the Health IT Module.
9. No Authority Information Access (AIA) extension: The tester verifies the Health IT Module rejects Direct messages received with No Authority Information Access (AIA) extension and that no corresponding MDN was received by SITE from the Health IT Module.
10. Invalid Message Digest: The tester verifies the Health IT Module rejects Direct messages received with an Invalid Message Digest and that no corresponding MDN was received by SITE from the Health IT Module.

Approved SVAP Version(s)

System Under Test

6. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Invalid Certificate.
7. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Expired Certificate.
8. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).
9. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
10. The user rejects health information not in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification sent from SITE to the Health IT Module using the following tool option: Invalid Message Digest.

Test Lab Verification

Complete steps 3-4 verifications in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Approved SVAP Version(s)

Complete steps 2-4 in accordance with the ONC Applicability Statement for Secure Health Transport v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(B) – Receive conversion using XDR

System Under Test

1. Using SITE: Direct Tooling, HISP Testing Portal, select the XDR tab and using “Your System as: Receiver” the Health IT Module receives a properly formatted XDR message with limited metadata from SITE (as Edge), and translates it to a Direct message, and sends it to SITE (as Destination HISP) (XDR Test 13).
2. The Health IT Module receives a properly formatted XDR message with full metadata from SITE (as Edge), translates it to a Direct message, and sends it to SITE (as Destination HISP) (XDR Test 14).

Test Lab Verification

1. The tester verifies the message received by the Health IT Module was converted to a Direct Message, with Limited Metadata, and returned to SITE, in accordance with the standard § 170.202(b) ONC XDR and XDM for Direct Messaging Specification, using the SITE validation report, sent to the contact’s registered email address, and the SITE logs (XDR Test 13).
2. The tester verifies the message received by the Health IT Module was converted to a Direct Message with Full Metadata, and returned to SITE, in accordance with the standard § 170.202(b), using the SITE validation report, sent to the contact’s registered email address, and the SITE logs (XDR Test 14).

System Under Test	Test Lab Verification
1. Using SITE: Direct Tooling, HISP Testing Portal, select the XDR tab and using “Your System as: Receiver” the Health IT Module receives a properly formatted XDR message with limited metadata from SITE (as Edge), and translates it to a Direct message, and sends it to SITE (as Destination HISP) (XDR Test 13). 2. The Health IT Module receives a properly formatted XDR message with full metadata from SITE (as Edge), translates it to a Direct message, and sends it to SITE (as Destination HISP) (XDR Test 14).	1. The tester verifies the message received by the Health IT Module was converted to a Direct Message, with Limited Metadata, and returned to SITE, in accordance with the standard § 170.202(b) ONC XDR and XDM for Direct Messaging Specification, using the SITE validation report, sent to the contact’s registered email address, and the SITE logs (XDR Test 13). 2. The tester verifies the message received by the Health IT Module was converted to a Direct Message with Full Metadata, and returned to SITE, in accordance with the standard § 170.202(b), using the SITE validation report, sent to the contact’s registered email address, and the SITE logs (XDR Test 14).

Paragraph (h)(2)(i)(C) – Send Using Edge Protocol for IHE XDR profile for Limited Metadata Document Sources

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the XDR tab with “System as Sender,” the user establishes a Mutual TLS session for the Health IT Module to authenticate to SITE (XDR Test 16).
2. The Health IT Module provides documentation of the Health IT Module’s ability to reject the connection for a TLS session initiated with an Edge due to an invalid certificate.

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Send Payload

4. The user configures the SITE’s endpoints within the Health IT Module and provides the Health IT Module’s Direct “To” address to generate endpoints. Acting as a HISP, the Health IT Module receives and translates a Direct message to an XDR message, and sends the translated message to SITE (acting as an Edge) for the following types of messages:
    - Direct to send to Edge as an XDR message (XDR Test 10);
    - Direct + XDM to send to Edge as an XDR message with Limited Metadata (XDR Test 11); and
    - Direct + XDM to send to Edge as an XDR message with Full Metadata (XDR Test 12).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using SITE: HISP Testing Portal, select the XDR tab with “System as Receiver”, SITE (as Edge) sends a message to the Health IT Module using a bad address (non-existent), such that the Health IT Module is unable to deliver the message. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile due to a bad address (non-existent) (XDR MT Test 13).
6. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) is not trusted. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile due to an untrusted HISP (SITE as Destination HISP) (XDR MT Test 14).
7. SITE (as Edge) sends a message to the Health IT Module using a valid address, but the SITE’s (as Destination HISP) certificates are not published. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile due to an unpublished HISP certificate (SITE as Destination HISP) (XDR MT Test 15).

8. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) does not respond with a processed MDN. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile, due to exceeded wait period for receiving a processed MDN from SITE (as Destination HISP) (XDR MT Test 16).

Test Lab Verification

SUT Connection– Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module initiates a Mutual TLS session with SITE (XDR Test 16).
2. The tester verifies evidence of the Health IT Module's capability to initiate a TLS session but reject the connection with an Edge due to an invalid certificate.

SUT Connection– Secure Network If Not Using TLS

3. The tester verifies through evidence that the system provides a "secure network" as described at § 170.202(d).

Send Payload

4. Using SITE validation report, the tester verifies the Health IT Module can translate the following using § 170.202(d):
    - Direct Message to Health IT Module to XDR message (XDR Test 10);
    - Direct + XDM Message to Health IT Module to XDR message with Limited Metadata (XDR Test 11); and
    - Direct + XDM Message to Health IT Module to XDR message with Full Metadata (XDR Test 12).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using visual inspection of SITE logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to bad address (non-existent) (XDR MT Test 13).
6. Using visual inspection of the logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to Untrusted Destination HISP (XDR MT Test 14).
7. Using visual inspection of SITE logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to Unpublished Certificate for Destination HISP (XDR MT Test 15).
8. Using visual inspection of SITE logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to Delivery Failure Timeout (XDR MT Test 16).

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the XDR tab with “System as Sender,” the user establishes a Mutual TLS session for the Health IT Module to authenticate to SITE (XDR Test 16).
2. The Health IT Module provides documentation of the Health IT Module’s ability to reject the connection for a TLS session initiated with an Edge due to an invalid certificate.

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Send Payload

4. The user configures the SITE’s endpoints within the Health IT Module and provides the Health IT Module’s Direct “To” address to generate endpoints. Acting as a HISP, the Health IT Module receives and translates a Direct message to an XDR message, and sends the translated message to SITE (acting as an Edge) for the following types of messages:
    - Direct to send to Edge as an XDR message (XDR Test 10);
    - Direct + XDM to send to Edge as an XDR message with Limited Metadata (XDR Test 11); and
    - Direct + XDM to send to Edge as an XDR message with Full Metadata (XDR Test 12).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using SITE: HISP Testing Portal, select the XDR tab with “System as Receiver”, SITE (as Edge) sends a message to the Health IT Module using a bad address (non-existent), such that the Health IT Module is unable to deliver the message. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile due to a bad address (non-existent) (XDR MT Test 13).

Test Lab Verification

SUT Connection– Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module initiates a Mutual TLS session with SITE (XDR Test 16).
2. The tester verifies evidence of the Health IT Module’s capability to initiate a TLS session but reject the connection with an Edge due to an invalid certificate.

SUT Connection– Secure Network If Not Using TLS

3. The tester verifies through evidence that the system provides a “secure network” as described at § 170.202(d).

Send Payload

4. Using SITE validation report, the tester verifies the Health IT Module can translate the following using § 170.202(d):
    - Direct Message to Health IT Module to XDR message (XDR Test 10);
    - Direct + XDM Message to Health IT Module to XDR message with Limited Metadata (XDR Test 11); and
    - Direct + XDM Message to Health IT Module to XDR message with Full Metadata (XDR Test 12).

System Under Test

6. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) is not trusted. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile due to an untrusted HISP (SITE as Destination HISP) (XDR MT Test 14).
7. SITE (as Edge) sends a message to the Health IT Module using a valid address, but the SITE's (as Destination HISP) certificates are not published. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile due to an unpublished HISP certificate (SITE as Destination HISP) (XDR MT Test 15).
8. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) does not respond with a processed MDN. The Health IT Module delivers a failure message to SITE (as Edge) using the XDR profile, due to exceeded wait period for receiving a processed MDN from SITE (as Destination HISP) (XDR MT Test 16).

Test Lab Verification

Message Tracking Using Processed MDNs (Negative Tests)

5. Using visual inspection of SITE logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to bad address (non-existent) (XDR MT Test 13).
6. Using visual inspection of the logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to Untrusted Destination HISP (XDR MT Test 14).
7. Using visual inspection of SITE logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to Unpublished Certificate for Destination HISP (XDR MT Test 15).
8. Using visual inspection of SITE logs, the tester verifies the Health IT Module has sent failure messages to SITE (as Edge) using the XDR profile due to Delivery Failure Timeout (XDR MT Test 16).

Paragraph (h)(2)(i)(C) – Send Using Edge Protocol for SMTP

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the SMTP tab with “System as Sender,” the user initiates a TLS session for the Health IT Module with SITE (SMTP Test 8).
2. The Health IT Module provides documentation of the Heath IT Module’s ability to reject the connection for a TLS session initiated with an Edge due to an invalid certificate.

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Send Payload

4. The user sends a document to SITE (SMTP Test 14).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using SITE: HISP Testing Portal, “Message Tracking” with “System as Sender,” SITE (as Edge) sends a message to the Health IT Module using a bad address (non-existent), such that the Health IT Module is unable to deliver the message. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to a bad address (non-existent):
    - SMTP MT Test 1 or alternatively;
    - SMTP/IMAP MT Test 5 (Alternative);
    - SMTP/POP MT Test 9 (Alternative).
6. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) is not trusted. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to an untrusted HISP (SITE as Destination HISP):
    - SMTP MT Test 2 or alternatively;
    - SMTP/IMAP MT Test 6 (Alternative);
    - SMTP/POP MT Test 10 (Alternative).
7. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE’s (as Destination HISP) certificates are not published. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to an unpublished HISP certificate (SITE as Destination HISP):
    - SMTP MT Test 3 or alternatively;
    - SMTP/IMAP MT Test 7 (Alternative);
    - SMTP/POP MT Test 11 (Alternative).

8. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) does not respond with a processed MDN. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to exceeded wait period for receiving a processed MDN from SITE (as Destination HISP), delivery time-out:
    - SMTP MT Test 4 or alternatively;
    - SMTP/IMAP MT Test 8 (Alternative);
    - SMTP/POP MT Test 12 (Alternative).

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module initiates a TLS session (SMTP Test 8).
2. The tester verifies evidence of the Health IT Module's capability to initiate a TLS session, but reject the connection with an Edge due to an invalid certificate.

SUT Connection – Secure Network If Not Using TLS

3. The tester verifies through evidence that the system provides a "secure network" as described at § 170.202(d).

Send Payload

4. The tester verifies the Health IT Module can send an SMTP Message using the SMTP Edge Protocol (SMTP Test 14).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using visual inspection of SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure message due to a bad address (non-existent) to SITE (as Edge) for the following tests:
    - SMTP MT Test 1 or alternatively;
    - SMTP/IMAP MT Test 5 (Alternative);
    - SMTP/POP MT Test 9 (Alternative).

6. Using SITE, the tester verifies the Health IT Module successfully performs message tracking using processed MDNs. Using visual inspection of SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure messages due to an untrusted HISP to SITE (as Edge) for the following tests:
    - SMTP MT Test 2 or alternatively;
    - SMTP/IMAP MT Test 6 (Alternative);
    - SMTP/POP MT Test 10 (Alternative).
7. Using visual inspection of SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure messages due to an unpublished HISP certificate to SITE (as Edge) for the following tests:
    - SMTP MT Test 3 or alternatively;
    - SMTP/IMAP MT Test 7 (Alternative);
    - SMTP/POP MT Test 11 (Alternative).
8. Using visual inspection of the SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure messages due to exceeded wait period for receiving a processed MDN to the SITE (as Edge) for the following tests:
    - SMTP MT Test 4 or alternatively;
    - SMTP/IMAP MT Test 8 (Alternative);
    - SMTP/POP MT Test 12 (Alternative).

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the SMTP tab with “System as Sender,” the user initiates a TLS session for the Health IT Module with SITE (SMTP Test 8).
2. The Health IT Module provides documentation of the Heath IT Module’s ability to reject the connection for a TLS session initiated with an Edge due to an invalid certificate.

SUT Connection – Secure Network If Not Using TLS

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module initiates a TLS session (SMTP Test 8).
2. The tester verifies evidence of the Health IT Module’s capability to initiate a TLS session, but reject the connection with an Edge due to an invalid certificate.

SUT Connection – Secure Network If Not Using TLS

3. The tester verifies through evidence that the system provides a “secure network” as described at § 170.202(d).

Send Payload

System Under Test

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a "secure network" as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Send Payload

4. The user sends a document to SITE (SMTP Test 14).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using SITE: HISP Testing Portal, "Message Tracking" with "System as Sender," SITE (as Edge) sends a message to the Health IT Module using a bad address (non-existent), such that the Health IT Module is unable to deliver the message. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to a bad address (non-existent):
    - SMTP MT Test 1 or alternatively;
    - SMTP/IMAP MT Test 5 (Alternative);
    - SMTP/POP MT Test 9 (Alternative).
6. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) is not trusted. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to an untrusted HISP (SITE as Destination HISP):
    - SMTP MT Test 2 or alternatively;
    - SMTP/IMAP MT Test 6 (Alternative);
    - SMTP/POP MT Test 10 (Alternative).

Test Lab Verification

4. The tester verifies the Health IT Module can send an SMTP Message using the SMTP Edge Protocol (SMTP Test 14).

Message Tracking Using Processed MDNs (Negative Tests)

5. Using visual inspection of SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure message due to a bad address (non-existent) to SITE (as Edge) for the following tests:
    - SMTP MT Test 1 or alternatively;
    - SMTP/IMAP MT Test 5 (Alternative);
    - SMTP/POP MT Test 9 (Alternative).
6. Using SITE, the tester verifies the Health IT Module successfully performs message tracking using processed MDNs. Using visual inspection of SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure messages due to an untrusted HISP to SITE (as Edge) for the following tests:
    - SMTP MT Test 2 or alternatively;
    - SMTP/IMAP MT Test 6 (Alternative);
    - SMTP/POP MT Test 10 (Alternative).

System Under Test	Test Lab Verification
7. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE's (as Destination HISP) certificates are not published. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to an unpublished HISP certificate (SITE as Destination HISP): ◦ SMTP MT Test 3 or alternatively; ◦ SMTP/IMAP MT Test 7 (Alternative); ◦ SMTP/POP MT Test 11 (Alternative). 8. SITE (as Edge) sends a message to the Health IT Module using a valid address, but SITE (as Destination HISP) does not respond with a processed MDN. The Health IT Module delivers a failure message to SITE (as Edge) using the following edge protocol due to exceeded wait period for receiving a processed MDN from SITE (as Destination HISP), delivery time-out: ◦ SMTP MT Test 4 or alternatively; ◦ SMTP/IMAP MT Test 8 (Alternative); ◦ SMTP/POP MT Test 12 (Alternative).	7. Using visual inspection of SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure messages due to an unpublished HISP certificate to SITE (as Edge) for the following tests: ◦ SMTP MT Test 3 or alternatively; ◦ SMTP/IMAP MT Test 7 (Alternative); ◦ SMTP/POP MT Test 11 (Alternative). 8. Using visual inspection of the SITE logs to confirm the receipt of the negative delivery status notification message, the tester verifies the Health IT Module has sent a delivery failure messages due to exceeded wait period for receiving a processed MDN to the SITE (as Edge) for the following tests: ◦ SMTP MT Test 4 or alternatively; ◦ SMTP/IMAP MT Test 8 (Alternative); ◦ SMTP/POP MT Test 12 (Alternative).

Paragraph (h)(2)(i)(C) – Send Using Edge Protocol for IMAP (SMTP Alternative)

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the IMAP tab with "System as Sender", the user initiates an IMAP session to the Health IT Module with STARTTLS (STARTTLS command) and PLAIN SSL authentication (AUTHENTICATE command) (IMAP Test 8, 11, 15).

2. The Health IT Module provides documentation of the Heath IT Module's ability to processes connection requests initiated using STARTTLS with valid cipher suite(s) in accordance with RFC 3501 and the subsequently updated standards: RFC 2246, NIST Special Publication 800-52 Revision 1, RFC 7465, and is in accordance with the security standards specified in the § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 (IMAP Test 8, 11, 15).
3. The Health IT Module provides documentation of the ability to accept a valid authentication mechanism and authenticates the Edge.
4. Negative Test: The Health IT Module provides documentation of the ability to reject an authentication request from an Edge.

SUT Connection – Secure Network If Not Using TLS

5. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a "secure network" as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Execute IMAP4 Commands

6. Using SITE: HISP Testing Portal, select the IMAP tab with "System as Sender", the user initiates an IMAP session to the Health IT Module using the IMAP4 CAPABILITIES command, NOOP command, and LOGOUT command (or equivalent for a secure network) (IMAP Tests 1, 2, 3).
7. Using SITE, the user initiates an IMAP session to the Health IT Module using the STARTTLS and AUTHENTICATE commands (or equivalent for a secure network), LOGIN command, SELECT command, and FETCH command (IMAP Tests 8, 11, 15).

Reject IMAP4 Connection (Negative Tests)

8. Negative Test: The user demonstrates the Health IT Module rejects an IMAP4 connection with a bad command syntax by terminating the connection from SITE (IMAP Test 9).
9. Negative Test: The user demonstrates the Health IT Module rejects an IMAP4 connections with bad commands using the right syntax based upon the specific state of the connection by terminating the connection from SITE (IMAP Test 10).

Message Processing

10. SITE (as Edge) is able to fetch attachments from the Health IT Module using an IMAP4 connection (IMAP Test 32).
11. Negative Test: The Health IT Module rejects authentication requests from SITE due to an invalid username/password (IMAP Test 17).

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module is able to successfully initiate an IMAP4 session with the Health IT Module (IMAP Test 8, 11, 15).
2. The tester verifies evidence of the Health IT Module's capability to process connection requests initiated using STARTTLS with one or more valid cipher suite (IMAP Test 8, 11, 15).
3. The tester verifies evidence of the Health IT Module's capability to accept authentication requests.
4. Negative Test: The tester verifies evidence of the Health IT Module's capability to reject authentication requests.

SUT Connection – Secure Network If Not Using TLS

5. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a "secure network" as described at § 170.202(d).

Execute IMAP4 Commands

6. Using SITE logs, the tester verifies the Health IT Module is has successfully implemented the following commands IMAP4 CAPABILITY, NOOP, and LOGOUT (or equivalent for a secure network) (IMAP Test 1, 2, 3).
7. Using SITE logs, the tester verifies the Health IT Module is has successfully implemented the following commands IMAP4 STARTTLS and AUTHENTICATE (or equivalent for a secure network), LOGIN, SELECT, and FETCH (IMAP Test 8, 11, 15).

Reject IMAP4 Connection (Negative Tests)

8. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects a bad command syntax with the appropriate response and terminates connection with SITE (IMAP Tests 9).
9. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects a bad command with correct syntax with the appropriate response and terminates connection with SITE (IMAP Tests 10).

Message Processing

10. Using SITE logs, the tester verifies the Health IT Module is able to host attachments and make them available for fetching using IMAP (IMAP Test 32).
11. Negative Test: Using SITE logs, the tester verifies the Health IT Module rejects authentication requests due to invalid username/password (IMAP Test 17).

System Under Test	Test Lab Verification

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the IMAP tab with “System as Sender”, the user initiates an IMAP session to the Health IT Module with STARTTLS (STARTTLS command) and PLAIN SSL authentication (AUTHENTICATE command) (IMAP Test 8, 11, 15).
2. The Health IT Module provides documentation of the Heath IT Module’s ability to processes connection requests initiated using STARTTLS with valid cipher suite(s) in accordance with RFC 3501 and the subsequently updated standards: RFC 2246, NIST Special Publication 800-52 Revision 1, RFC 7465, and is in accordance with the security standards specified in the § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 (IMAP Test 8, 11, 15).
3. The Health IT Module provides documentation of the ability to accept a valid authentication mechanism and authenticates the Edge.
4. Negative Test: The Health IT Module provides documentation of the ability to reject an authentication request from an Edge.

SUT Connection – Secure Network If Not Using TLS

5. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Execute IMAP4 Commands

6. Using SITE: HISP Testing Portal, select the IMAP tab with “System as Sender”, the user initiates an IMAP session to the Health IT Module using the IMAP4 CAPABILITIES command, NOOP command, and LOGOUT command (or equivalent for a secure network) (IMAP Tests 1, 2, 3).
7. Using SITE, the user initiates an IMAP session to the Health IT Module using the STARTTLS and AUTHENTICATE commands (or equivalent for a secure network), LOGIN command, SELECT command, and FETCH command (IMAP Tests 8, 11, 15).

Reject IMAP4 Connection (Negative Tests)

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module is able to successfully initiate an IMAP4 session with the Health IT Module (IMAP Test 8, 11, 15).
2. The tester verifies evidence of the Health IT Module’s capability to process connection requests initiated using STARTTLS with one or more valid cipher suite (IMAP Test 8, 11, 15).
3. The tester verifies evidence of the Health IT Module’s capability to accept authentication requests.
4. Negative Test: The tester verifies evidence of the Health IT Module’s capability to reject authentication requests.

SUT Connection – Secure Network If Not Using TLS

5. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d).

Execute IMAP4 Commands

System Under Test

8. Negative Test: The user demonstrates the Health IT Module rejects an IMAP4 connection with a bad command syntax by terminating the connection from SITE (IMAP Test 9).
9. Negative Test: The user demonstrates the Health IT Module rejects an IMAP4 connections with bad commands using the right syntax based upon the specific state of the connection by terminating the connection from SITE (IMAP Test 10).

Message Processing

10. SITE (as Edge) is able to fetch attachments from the Health IT Module using an IMAP4 connection (IMAP Test 32).
11. Negative Test: The Health IT Module rejects authentication requests from SITE due to an invalid username/password (IMAP Test 17).

Test Lab Verification

6. Using SITE logs, the tester verifies the Health IT Module is has successfully implemented the following commands IMAP4 CAPABILITY, NOOP, and LOGOUT (or equivalent for a secure network) (IMAP Test 1, 2, 3).
7. Using SITE logs, the tester verifies the Health IT Module is has successfully implemented the following commands IMAP4 STARTTLS and AUTHENTICATE (or equivalent for a secure network), LOGIN, SELECT, and FETCH (IMAP Test 8, 11, 15).

Reject IMAP4 Connection (Negative Tests)

8. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects a bad command syntax with the appropriate response and terminates connection with SITE (IMAP Tests 9).
9. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects a bad command with correct syntax with the appropriate response and terminates connection with SITE (IMAP Tests 10).

Message Processing

System Under Test	Test Lab Verification
	10. Using SITE logs, the tester verifies the Health IT Module is able to host attachments and make them available for fetching using IMAP (IMAP Test 32). 11. Negative Test: Using SITE logs, the tester verifies the Health IT Module rejects authentication requests due to invalid username/password (IMAP Test 17).

Paragraph (h)(2)(i)(C) – Send Using Edge Protocol for POP3 (SMTP Alternative)

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the POP3 tab with “System as Sender,” and the user initiates a POP session to the Health IT Module with STARTTLS (STARTTLS command) (POP Test 5, 11, 15).
2. The Health IT Module provides documentation of the Heath IT Module’s ability to processes connection requests initiated using STARTTLS with a valid cipher suite(s) in accordance with RFC 3501, and the subsequently updated standards: RFC 2246, NIST Special Publication 800-52, Revision 1, RFC 7465, and is in accordance with the security standards specified in the § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 (POP Test 5, 11, 15).

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Execute POP3 Commands

4. Using SITE: HISP Testing Portal, with the POP3 tab and “System as Sender,” and the user initiates a POP session to the Health IT Module using the POP3 CAPA command, NOOP command, and QUIT command (or equivalent for a secure network) (POP Test 1, 2).
5. Using SITE, the user initiates a POP session to the Health IT Module using the POP3 STAT command, STARTTLS command (or equivalent for a secure network), RETR command, LIST command, and RSET command (POP Test 5, 11, 15).

Reject POP3 Connection (Negative Tests)

6. Negative Test: The user demonstrates the Health IT Module rejects a POP3 connection with a bad command syntax by terminating the connection from SITE (POP Test 9).
7. Negative Test: The user demonstrates the Health IT Module rejects a POP3 connection with bad commands using the right syntax based upon the specific state of the connection by terminating the connection from SITE (POP Test 10).

Message Processing

8. SITE (as Edge) is able to fetch attachments from the Health IT Module using an IMAP4 connection (POP Test 32).
9. Negative Test: The Health IT Module rejects authentication requests from SITE due to an invalid username/password (POP Test 17).

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module is able to successfully initiate a POP session with the Health IT Module (POP Test 5, 11, 15).
2. The tester verifies evidence of the Health IT Module’s capability to process connection requests initiated using STARTTLS with one or more valid cipher suite (POP Test 3-5, 11, 15).

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d).

Execute POP3 Commands

4. Using SITE logs, the tester verifies the Health IT Module has successfully implemented the following commands: POP3 CAPA, NOOP, and QUIT (or equivalent for a secure network) (POP Test 1, 2).

5. Using SITE logs, the tester verifies the Health IT Module has successfully implemented the following commands POP3 STAT, STARTTLS (or equivalent for a secure network), RETR, LIST, and RSET (POP Test 5, 11, 15).

Reject POP3 Connection (Negative Tests)

6. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects bad command syntax commands with the appropriate response and terminates connection with SITE (POP Test 9).
7. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects bad commands using the right syntax commands with the appropriate response and terminates connection with SITE (POP Test 10).

Message Processing

8. Using SITE logs, the tester verifies the Health IT Module is able to host attachments and make them available for fetching using POP (POP Test 32).
9. Negative Test: Using SITE logs, the tester verifies the Health IT Module rejects authentication requests due to invalid username/password (POP Test 17).

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Portal, select the POP3 tab with “System as Sender,” and the user initiates a POP session to the Health IT Module with STARTTLS (STARTTLS command) (POP Test 5, 11, 15).
2. The Health IT Module provides documentation of the Heath IT Module’s ability to processes connection requests initiated using STARTTLS with a valid cipher suite(s) in accordance with RFC 3501, and the subsequently updated standards: RFC 2246, NIST Special Publication 800-52, Revision 1, RFC 7465, and is in accordance with the security standards specified in the § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2 (POP Test 5, 11, 15).

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Execute POP3 Commands

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module is able to successfully initiate a POP session with the Health IT Module (POP Test 5, 11, 15).
2. The tester verifies evidence of the Health IT Module’s capability to process connection requests initiated using STARTTLS with one or more valid cipher suite (POP Test 3-5, 11, 15).

SUT Connection – Secure Network If Not Using TLS

System Under Test

4. Using SITE: HISP Testing Portal, with the POP3 tab and “System as Sender,” and the user initiates a POP session to the Health IT Module using the POP3 CAPA command, NOOP command, and QUIT command (or equivalent for a secure network) (POP Test 1, 2).
5. Using SITE, the user initiates a POP session to the Health IT Module using the POP3 STAT command, STARTTLS command (or equivalent for a secure network), RETR command, LIST command, and RSET command (POP Test 5, 11, 15).

Reject POP3 Connection (Negative Tests)

6. Negative Test: The user demonstrates the Health IT Module rejects a POP3 connection with a bad command syntax by terminating the connection from SITE (POP Test 9).
7. Negative Test: The user demonstrates the Health IT Module rejects a POP3 connection with bad commands using the right syntax based upon the specific state of the connection by terminating the connection from SITE (POP Test 10).

Message Processing

8. SITE (as Edge) is able to fetch attachments from the Health IT Module using an IMAP4 connection (POP Test 32).
9. Negative Test: The Health IT Module rejects authentication requests from SITE due to an invalid username/password (POP Test 17).

Test Lab Verification

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d).

Execute POP3 Commands

4. Using SITE logs, the tester verifies the Health IT Module has successfully implemented the following commands: POP3 CAPA, NOOP, and QUIT (or equivalent for a secure network) (POP Test 1, 2).
5. Using SITE logs, the tester verifies the Health IT Module has successfully implemented the following commands POP3 STAT, STARTTLS (or equivalent for a secure network), RETR, LIST, and RSET (POP Test 5, 11, 15).

Reject POP3 Connection (Negative Tests)

System Under Test

Test Lab Verification

6. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects bad command syntax commands with the appropriate response and terminates connection with SITE (POP Test 9).
7. Negative Tests: Using SITE logs, the tester verifies the Health IT Module rejects bad commands using the right syntax commands with the appropriate response and terminates connection with SITE (POP Test 10).

Message Processing

8. Using SITE logs, the tester verifies the Health IT Module is able to host attachments and make them available for fetching using POP (POP Test 32).
9. Negative Test: Using SITE logs, the tester verifies the Health IT Module rejects authentication requests due to invalid username/password (POP Test 17).

Paragraph (h)(2)(i)(C) – Receive Using Edge Protocol for IHE XDR profile for Limited Metadata Document Sources

System Under Test

SUT Connection– Using TLS and SASL

1. Using SITE: HISP Testing Portal, with the XDR tab and “System as Receiver,” the user establishes authentication from SITE to the Health IT Module using Mutual TLS correctly (XDR Test 18).
2. Using SITE, the user establishes authentication from SITE to the Health IT Module using bad certificates (incorrect Mutual TLS configuration) (XDR Test 19).

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a “secure network” as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Receive Payload

4. The user enters the Health IT Module’s endpoints for receiving an XDR message from SITE (as Edge) for Limited Metadata (XDR Test 13) and the Health IT Module receives a properly formatted XDR message with limited metadata from SITE (as Edge) and translates it to a Direct message sent to SITE (as Destination HISP) (XDR Test 13).
5. The user enters the Health IT Module’s endpoints for receiving an XDR message from SITE (as Edge) for Full Metadata (XDR Test 14) and the Health IT Module receives a properly formatted XDR message with full metadata from SITE (as Edge) and translates it to a Direct message sent to SITE (as Destination HISP) (XDR Test 14).

Incorrect XDR Message Receive

6. The Health IT Module returns errors when the following incorrect messages are received from SITE with Invalid SOAP envelope details (XDR Test 15a).
7. The Health IT Module returns errors when the following incorrect messages are received from SITE with Invalid SOAP body details (XDR Test 15b), including:
    - Missing metadata elements;
    - Missing associations between ebRIM constructs;
    - Missing Direct Address block.

Test Lab Verification

SUT Connection– Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module is capable of accepting and validating a Mutual TLS session when authenticating to SITE. Using visual inspection of the logs, the tester verifies the Health IT Module does not accept connections due to incorrect Mutual TLS configuration (XDR Test 18).

2. Using visual inspection of the logs, the tester verifies the Health IT Module does not accept connections due to an invalid certificate published by SITE (XDR Test 19).

SUT Connection – Secure Network If Not Using TLS

3. The tester verifies through evidence that the system provides a "secure network" as described at § 170.202(d).

Receive Payload

4. Using visual inspection of the logs, the tester verifies the Health IT Module is capable of receiving and processing a valid XDR message with limited metadata and the Health IT Module does not accept invalid messages sent from SITE (XDR Test 13).
5. Using visual inspection of the logs, the tester verifies the Health IT Module is capable of receiving and processing a valid XDR message with full metadata and the Health IT Module does not accept invalid messages sent from SITE (XDR Test 14).

Incorrect XDR Message Receive

6. Using logs, the tester verifies the Health IT Module recognizes that the messages sent from SITE are Invalid messages (XDR Test 15a).
7. Using logs, the tester verifies the Health IT Module rejects the bad messages (XDR Test 15b).

System Under Test

SUT Connection– Using TLS and SASL

1. Using SITE: HISP Testing Portal, with the XDR tab and "System as Receiver," the user establishes authentication from SITE to the Health IT Module using Mutual TLS correctly (XDR Test 18).
2. Using SITE, the user establishes authentication from SITE to the Health IT Module using bad certificates (incorrect Mutual TLS configuration) (XDR Test 19).

SUT Connection – Secure Network If Not Using TLS

3. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a "secure network" as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Test Lab Verification

SUT Connection– Using TLS and SASL

1. Using SITE, the tester verifies the Health IT Module is capable of accepting and validating a Mutual TLS session when authenticating to SITE. Using visual inspection of the logs, the tester verifies the Health IT Module does not accept connections due to incorrect Mutual TLS configuration (XDR Test 18).
2. Using visual inspection of the logs, the tester verifies the Health IT Module does not accept connections due to an invalid certificate published by SITE (XDR Test 19).

SUT Connection – Secure Network If Not Using TLS

System Under Test

Receive Payload

4. The user enters the Health IT Module's endpoints for receiving an XDR message from SITE (as Edge) for Limited Metadata (XDR Test 13) and the Health IT Module receives a properly formatted XDR message with limited metadata from SITE (as Edge) and translates it to a Direct message sent to SITE (as Destination HISP) (XDR Test 13).
5. The user enters the Health IT Module's endpoints for receiving an XDR message from SITE (as Edge) for Full Metadata (XDR Test 14) and the Health IT Module receives a properly formatted XDR message with full metadata from SITE (as Edge) and translates it to a Direct message sent to SITE (as Destination HISP) (XDR Test 14).

Incorrect XDR Message Receive

6. The Health IT Module returns errors when the following incorrect messages are received from SITE with Invalid SOAP envelope details (XDR Test 15a).
7. The Health IT Module returns errors when the following incorrect messages are received from SITE with Invalid SOAP body details (XDR Test 15b), including:
    - Missing metadata elements;
    - Missing associations between ebRIM constructs;
    - Missing Direct Address block.

Test Lab Verification

3. The tester verifies through evidence that the system provides a "secure network" as described at § 170.202(d).

Receive Payload

4. Using visual inspection of the logs, the tester verifies the Health IT Module is capable of receiving and processing a valid XDR message with limited metadata and the Health IT Module does not accept invalid messages sent from SITE (XDR Test 13).
5. Using visual inspection of the logs, the tester verifies the Health IT Module is capable of receiving and processing a valid XDR message with full metadata and the Health IT Module does not accept invalid messages sent from SITE (XDR Test 14).

Incorrect XDR Message Receive

6. Using logs, the tester verifies the Health IT Module recognizes that the messages sent from SITE are Invalid messages (XDR Test 15a).
7. Using logs, the tester verifies the Health IT Module rejects the bad messages (XDR Test 15b).

Paragraph (h)(2)(i)(C) – Receive Using Edge Protocol for SMTP

System Under Test

SUT Connection – Using TLS and SASL

1. Using SITE: HISP Testing Tool with the SMTP tab using SITE “System as Receiver,” the user initiates a valid TLS session for the Health IT Module with SITE sent from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 9).
2. The user authenticates SITE with the Health IT Module using PLAIN SASL as an SMTP server from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 16).
3. The Health IT Module provides documentation of the ability to authenticate to an Edge using SASL as an SMTP server.
4. The Health IT Module receives an authentication from SITE using an Invalid SASL username/password as an SMTP server from the username supplied by the Health IT Module email account being authenticated (SMTP Test 22).

SUT Connection – Secure Network If Not Using TLS

5. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a "secure network" as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Receive Payload

6. The user receives a document from SITE using valid SMTP commands from the username supplied by the Health IT Module email account being authenticated and establishes a connection with SITE (SMTP Test 20).
7. The user receives a document from SITE using invalid data as part of the DATA command from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 10).
8. The user receives a document from SITE using invalid SMTP commands as part of the DATA command from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 11).
9. The user receives a document from SITE from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address beyond the allowable time period (SMTP Test 13).

Test Lab Verification

SUT Connection – Using TLS and SASL

1. Using SITE, the tester verifies a secure session was established with the Health IT Module based upon TLS initiation using correct syntax (SMTP Test 9).
2. Using SITE with a predetermined username and password, the tester verifies a secure session was established with the Health IT Module with PLAIN SASL authentication (SMTP Test 16).

3. The tester verifies evidence of the capability to establish a secure session with the Health IT Module based upon successful authentication (SMTP Test 16).
4. The tester verifies evidence of the capability to reject an authentication (SMTP Test 22).

SUT Connection – Secure Network If Not Using TLS

5. The tester verifies through evidence that the system provides a "secure network" as described at § 170.202(d).

Receive Payload

6. Using SITE, the tester verifies the Health IT Module can receive an SMTP Message using § 170.202(d) and the Validation Report indicates the successful sequence of commands for SMTP protocols (SMTP Test 20).
7. Using SITE logs, the tester verifies a secure connection cannot be established based upon invalid data provided and does not accept the data by using appropriate responses to an invalid DATA command (SMTP Test 10).
8. Using SITE logs, the tester verifies a secure connection cannot be established based upon invalid data provided and does not accept the data by using appropriate responses to invalid SMTP commands or invalid size limits of SMTP commands (SMTP Test 11).
9. Using SITE, the tester verifies the Health IT Module has kept the transaction open for beyond the specified time constraints found with RFC 2821, Section 4.5.3.2, and therefore cannot accept the incoming message (SMTP Test 13).

System Under Test	Test Lab Verification
SUT Connection – Using TLS and SASL 1. Using SITE: HISP Testing Tool with the SMTP tab using SITE "System as Receiver," the user initiates a valid TLS session for the Health IT Module with SITE sent from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 9). 2. The user authenticates SITE with the Health IT Module using PLAIN SASL as an SMTP server from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 16).	**SUT Connection – Using TLS and SASL** 1. Using SITE, the tester verifies a secure session was established with the Health IT Module based upon TLS initiation using correct syntax (SMTP Test 9). 2. Using SITE with a predetermined username and password, the tester verifies a secure session was established with the Health IT Module with PLAIN SASL authentication (SMTP Test 16). 3. The tester verifies evidence of the capability to establish a secure session with the Health IT Module based upon successful authentication (SMTP Test 16).

System Under Test

3. The Health IT Module provides documentation of the ability to authenticate to an Edge using SASL as an SMTP server.
4. The Health IT Module receives an authentication from SITE using an Invalid SASL username/password as an SMTP server from the username supplied by the Health IT Module email account being authenticated (SMTP Test 22).

SUT Connection – Secure Network If Not Using TLS

5. The user demonstrates the ability to provide a secure connection to the SUT by providing evidence and demonstration that the system uses a "secure network" as described at § 170.202(d) ONC Implementation Guide for Direct Edge Protocols, v1.1.

Receive Payload

6. The user receives a document from SITE using valid SMTP commands from the username supplied by the Health IT Module email account being authenticated and establishes a connection with SITE (SMTP Test 20).
7. The user receives a document from SITE using invalid data as part of the DATA command from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 10).
8. The user receives a document from SITE using invalid SMTP commands as part of the DATA command from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address (SMTP Test 11).
9. The user receives a document from SITE from the username supplied by the Health IT Module email account being authenticated to the Health IT Module SMTP email address beyond the allowable time period (SMTP Test 13).

Test Lab Verification

4. The tester verifies evidence of the capability to reject an authentication (SMTP Test 22).

SUT Connection – Secure Network If Not Using TLS

5. The tester verifies through evidence that the system provides a “secure network” as described at § 170.202(d).

Receive Payload

6. Using SITE, the tester verifies the Health IT Module can receive an SMTP Message using § 170.202(d) and the Validation Report indicates the successful sequence of commands for SMTP protocols (SMTP Test 20).
7. Using SITE logs, the tester verifies a secure connection cannot be established based upon invalid data provided and does not accept the data by using appropriate responses to an invalid DATA command (SMTP Test 10).
8. Using SITE logs, the tester verifies a secure connection cannot be established based upon invalid data provided and does not accept the data by using appropriate responses to invalid SMTP commands or invalid size limits of SMTP commands (SMTP Test 11).
9. Using SITE, the tester verifies the Health IT Module has kept the transaction open for beyond the specified time constraints found with RFC 2821, Section 4.5.3.2, and therefore cannot accept the incoming message (SMTP Test 13).

Paragraph (h)(2)(ii) – Send

System Under Test

Disposition-Notification-Options Header

1. Using SITE: HISP Testing Portal, with the Message Tracking tab and “Your System as Sender,” the Health IT Module is able to successfully process the Disposition-Notifications-Options-Header received from SITE (as Sending Edge) and include it in the message to the destination (SITE as Destination HISP):
    - SMTP MT Test 21(a) or alternatively;
    - IMAP: SMTP/IMAP MT Test 21(b) (Alternative);
    - POP3: SMTP/POP MT Test 21(c) (Alternative).

Delivery Failure Due to Bad Destination Address

2. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a bad address (non-existent) for the destination, send the message to SITE (as Destination HISP), which will return an error as it will be unable to deliver the message to the address. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 23(a) or alternatively;
    - SMTP/IMAP MT Test 23(b) (Alternative);
    - SMTP/POP MT Test 23(c) (Alternative).

Delivery Failure Due to Untrusted Destination HISP

3. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as an untrusted Destination HISP). The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 24(a) or alternatively;
    - SMTP/IMAP MT Test 24(b) (Alternative);
    - SMTP/POP MT Test 24(c) (Alternative).

Delivery Failure Due to Unpublished Certificate for Destination HISP

4. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP). Due to the unpublished certificate, security and trust processing fails. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 25(a) or alternatively;
    - SMTP/IMAP MT Test 25(b) (Alternative);
    - SMTP/POP MT Test 25(c) (Alternative).

Delivery Failure Timeout for Processed MDN

5. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP). The wait time for the Health IT Module to receive a Processed MDN from the Destination HISP is exceeded. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 26(a) or alternatively;
    - SMTP/IMAP MT Test 26(b) (Alternative);
    - SMTP/POP MT Test 26(c) (Alternative).

Delivery Failure for Dispatched MDN

6. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP) which provides a Processed MDN but does not provide a Dispatched MDN to the Health IT Module. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 27(a) or alternatively;
    - SMTP/IMAP MT Test 27(b) (Alternative);
    - SMTP/POP MT Test 27(c) (Alternative).

Delivery Failure Timeout for Dispatched MDN

7. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP) which provides a Processed MDN to the Health IT Module. The Health IT Module receives a Dispatched MDN after the expected wait time is exceeded. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification and does not forward the dispatched MDN to SITE (as Sending Edge) message via:
    - SMTP MT Test 28(a) or alternatively;
    - SMTP/IMAP MT Test 28(b) (Alternative);
    - SMTP/POP MT Test 28(c) (Alternative).

Positive Delivery Notification

8. The Health IT Module is able to successfully process a message fromSITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP) which provides a Processed MDN and Dispatched MDN to the Health IT Module. The Health IT Module only sends SITE (as Sending Edge) a positive delivery status notification (dispatched MDN) message via:
    - SMTP MT Test 29(a) or alternatively;
    - SMTP/IMAP MT Test 29(b) (Alternative),
    - SMTP/POP MT Test 29(c) (Alternative).

Requesting Delivery Notification for XDR Edge HISP

9. The Health IT Module is able to successfully process a message from SITE (as Sending Edge), using SITE: HISP Testing Portal, with the XDR tab and “System as Receiver,” that includes a valid Direct address block header and valid destination. The Health IT Module includes the header in the message to SITE (as Destination HISP) within SMTP headers (XDR MT Test 30).
10. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) that includes a valid Direct address block, header, and invalid destination. The Health IT Module is able to process the header handle an invalid delivery notification request (XDR MT Test 31).

XDR Delivery Failure: Bad Address

11. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) that includes an invalid (non-existent) address. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 32).

XDR Delivery Failure: Untrusted Destination HISP

12. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) is not trusted and the Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 33).

XDR Delivery Failure: Unpublished Destination HISP Certificate

13. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) does not have published certificates, and security and trust processing fails. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 34).

XDR Delivery Failure: No Processed MDN

14. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) does not respond with a Processed MDN. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 35).

XDR Delivery Failure: No Dispatched MDN

15. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) responds with a Processed MDN, but no Dispatched MDN. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 36).

XDR Delivery Failure: Timeout for Dispatched MDN

16. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) responds with a Processed MDN, but the Dispatched MDN is received after the expected wait time has exceeded. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 37).

XDR Positive Delivery Notification

17. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) responds with a Processed MDN and Dispatched MDN within the expected time period. The Health IT Module sends only one positive delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 38).

Test Lab Verification

Disposition-Notification-Options Header

1. SITE test results for the following tests are successful:
    - SMTP MT Test 21(a) or alternatively;
    - SMTP/IMAP MT Test 21(b) (Alternative);
    - SMTP/POP MT Test 21(c) (Alternative).

Delivery Failure Due to Bad Destination Address

2. SITE test results for the following tests are successful:
    - SMTP MT Test 23(a) or alternatively;
    - SMTP/IMAP MT Test 23(b) (Alternative);
    - SMTP/POP MT Test 23(c) (Alternative).

Delivery Failure Due to Untrusted Destination HISP

3. SITE test results for the following tests are successful:
    - SMTP MT Test 24(a) or alternatively;
    - SMTP/IMAP MT Test 24(b) (Alternative);
    - SMTP/POP MT Test 24(c) (Alternative).

Delivery Failure Due to Unpublished Certificate for Destination HISP

4. SITE test results for the following tests are successful:
    - SMTP MT Test 25(a) or alternatively;
    - SMTP/IMAP MT Test 25(b) (Alternative);
    - SMTP/POP MT Test 25(c) (Alternative).

Delivery Failure Timeout for Processed MDN

5. SITE test results for the following tests are successful:
    - SMTP MT Test 26(a) or alternatively;
    - SMTP/IMAP MT Test 26(b) (Alternative);
    - SMTP/POP MT Test 26(c) (Alternative).

Delivery Failure for Dispatched MDN

6. SITE test results for the following tests are successful:
    - SMTP MT Test 27(a) or alternatively;
    - SMTP/IMAP MT Test 27(b) (Alternative);
    - SMTP/POP MT Test 27(c) (Alternative).

Delivery Failure Timeout for Dispatched MDN

7. The SITE test results for the following tests are successful:
    - SMTP MT Test 28(a) or alternatively;
    - SMTP/IMAP MT Test 28(b) (Alternative);
    - SMTP/POP MT Test 28(c) (Alternative).

Positive Delivery Notification

8. SITE test results for the following tests are successful:
    - SMTP MT Test 29(a) or alternatively;
    - SMTP/IMAP MT Test 29(b) (Alternative);
    - SMTP/POP MT Test 29(c) (Alternative).

Requesting Delivery Notification for XDR Edge HISP

9. SITE test results for XDR MT Test 30 are successful.
10. SITE test results for XDR MT Test 31 are successful.

XDR Delivery Failure: Bad Address

11. SITE test results for XDR MT Test 32 are successful.

XDR Delivery Failure: Untrusted Destination HISP

12. SITE test results for XDR MT Test 33 are successful.

XDR Delivery Failure: Unpublished Destination HISP Certificate

13. SITE test results for XDR MT Test 34 are successful.

XDR Delivery Failure: No Processed MDN

14. SITE test results for XDR MT Test 35 are successful.

XDR Delivery Failure: No Dispatched MDN

15. SITE test results for XDR MT Test 36 are successful.

XDR Delivery Failure: Timeout for Dispatched MDN

16. SITE test results for XDR MT Test 37 are successful.

XDR Positive Delivery Notification

17. SITE test results for XDR MT Test 38 are successful.

System Under Test	Test Lab Verification
Disposition-Notification-Options Header	**Disposition-Notification-Options Header**

System Under Test

1. Using SITE: HISP Testing Portal, with the Message Tracking tab and “Your System as Sender,” the Health IT Module is able to successfully process the Disposition-Notifications-Options-Header received from SITE (as Sending Edge) and include it in the message to the destination (SITE as Destination HISP):
    - SMTP MT Test 21(a) or alternatively;
    - IMAP: SMTP/IMAP MT Test 21(b) (Alternative);
    - POP3: SMTP/POP MT Test 21(c) (Alternative).

Delivery Failure Due to Bad Destination Address

2. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a bad address (non-existent) for the destination, send the message to SITE (as Destination HISP), which will return an error as it will be unable to deliver the message to the address. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 23(a) or alternatively;
    - SMTP/IMAP MT Test 23(b) (Alternative);
    - SMTP/POP MT Test 23(c) (Alternative).

Delivery Failure Due to Untrusted Destination HISP

3. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as an untrusted Destination HISP). The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 24(a) or alternatively;
    - SMTP/IMAP MT Test 24(b) (Alternative);
    - SMTP/POP MT Test 24(c) (Alternative).

Delivery Failure Due to Unpublished Certificate for Destination HISP

4. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP). Due to the unpublished certificate, security and trust processing fails. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 25(a) or alternatively;
    - SMTP/IMAP MT Test 25(b) (Alternative);
    - SMTP/POP MT Test 25(c) (Alternative).

Delivery Failure Timeout for Processed MDN

Test Lab Verification

1. SITE test results for the following tests are successful:
    - SMTP MT Test 21(a) or alternatively;
    - SMTP/IMAP MT Test 21(b) (Alternative);
    - SMTP/POP MT Test 21(c) (Alternative).

Delivery Failure Due to Bad Destination Address

2. SITE test results for the following tests are successful:
    - SMTP MT Test 23(a) or alternatively;
    - SMTP/IMAP MT Test 23(b) (Alternative);
    - SMTP/POP MT Test 23(c) (Alternative).

Delivery Failure Due to Untrusted Destination HISP

System Under Test

5. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP). The wait time for the Health IT Module to receive a Processed MDN from the Destination HISP is exceeded. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 26(a) or alternatively;
    - SMTP/IMAP MT Test 26(b) (Alternative);
    - SMTP/POP MT Test 26(c) (Alternative).

Delivery Failure for Dispatched MDN

6. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP) which provides a Processed MDN but does not provide a Dispatched MDN to the Health IT Module. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification message via:
    - SMTP MT Test 27(a) or alternatively;
    - SMTP/IMAP MT Test 27(b) (Alternative);
    - SMTP/POP MT Test 27(c) (Alternative).

Delivery Failure Timeout for Dispatched MDN

7. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP) which provides a Processed MDN to the Health IT Module. The Health IT Module receives a Dispatched MDN after the expected wait time is exceeded. The Health IT Module sends SITE (as Sending Edge) a negative delivery status notification and does not forward the dispatched MDN to SITE (as Sending Edge) message via:
    - SMTP MT Test 28(a) or alternatively;
    - SMTP/IMAP MT Test 28(b) (Alternative);
    - SMTP/POP MT Test 28(c) (Alternative).

Positive Delivery Notification

Test Lab Verification

3. SITE test results for the following tests are successful:
    - SMTP MT Test 24(a) or alternatively;
    - SMTP/IMAP MT Test 24(b) (Alternative);
    - SMTP/POP MT Test 24(c) (Alternative).

Delivery Failure Due to Unpublished Certificate for Destination HISP

4. SITE test results for the following tests are successful:
    - SMTP MT Test 25(a) or alternatively;
    - SMTP/IMAP MT Test 25(b) (Alternative);
    - SMTP/POP MT Test 25(c) (Alternative).

Delivery Failure Timeout for Processed MDN

System Under Test

8. The Health IT Module is able to successfully process a message fromSITE (as Sending Edge) with a valid address for the destination, send the message to SITE (as Destination HISP) which provides a Processed MDN and Dispatched MDN to the Health IT Module. The Health IT Module only sends SITE (as Sending Edge) a positive delivery status notification (dispatched MDN) message via:
    - SMTP MT Test 29(a) or alternatively;
    - SMTP/IMAP MT Test 29(b) (Alternative),
    - SMTP/POP MT Test 29(c) (Alternative).

Requesting Delivery Notification for XDR Edge HISP

9. The Health IT Module is able to successfully process a message from SITE (as Sending Edge), using SITE: HISP Testing Portal, with the XDR tab and "System as Receiver," that includes a valid Direct address block header and valid destination. The Health IT Module includes the header in the message to SITE (as Destination HISP) within SMTP headers (XDR MT Test 30).
10. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) that includes a valid Direct address block, header, and invalid destination. The Health IT Module is able to process the header handle an invalid delivery notification request (XDR MT Test 31).

XDR Delivery Failure: Bad Address

11. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) that includes an invalid (non-existent) address. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 32).

XDR Delivery Failure: Untrusted Destination HISP

12. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) is not trusted and the Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 33).

XDR Delivery Failure: Unpublished Destination HISP Certificate

Test Lab Verification

5. SITE test results for the following tests are successful:
    - SMTP MT Test 26(a) or alternatively;
    - SMTP/IMAP MT Test 26(b) (Alternative);
    - SMTP/POP MT Test 26(c) (Alternative).

Delivery Failure for Dispatched MDN

6. SITE test results for the following tests are successful:
    - SMTP MT Test 27(a) or alternatively;
    - SMTP/IMAP MT Test 27(b) (Alternative);
    - SMTP/POP MT Test 27(c) (Alternative).

Delivery Failure Timeout for Dispatched MDN

System Under Test

13. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) does not have published certificates, and security and trust processing fails. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 34).

XDR Delivery Failure: No Processed MDN

14. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) does not respond with a Processed MDN. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 35).

XDR Delivery Failure: No Dispatched MDN

15. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) responds with a Processed MDN, but no Dispatched MDN. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 36).

XDR Delivery Failure: Timeout for Dispatched MDN

16. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) responds with a Processed MDN, but the Dispatched MDN is received after the expected wait time has exceeded. The Health IT Module sends a negative delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 37).

XDR Positive Delivery Notification

17. The Health IT Module is able to successfully process a message from SITE (as Sending Edge) to a valid address. SITE (as Destination HISP) responds with a Processed MDN and Dispatched MDN within the expected time period. The Health IT Module sends only one positive delivery status notification message to SITE (as Sending Edge) using XDR profile (XDR MT Test 38).

Test Lab Verification

7. The SITE test results for the following tests are successful:
    - SMTP MT Test 28(a) or alternatively;
    - SMTP/IMAP MT Test 28(b) (Alternative);
    - SMTP/POP MT Test 28(c) (Alternative).

Positive Delivery Notification

8. SITE test results for the following tests are successful:
    - SMTP MT Test 29(a) or alternatively;
    - SMTP/IMAP MT Test 29(b) (Alternative);
    - SMTP/POP MT Test 29(c) (Alternative).

Requesting Delivery Notification for XDR Edge HISP

9. SITE test results for XDR MT Test 30 are successful.
10. SITE test results for XDR MT Test 31 are successful.

XDR Delivery Failure: Bad Address

System Under Test	Test Lab Verification
	11. SITE test results for XDR MT Test 32 are successful.
	XDR Delivery Failure: Untrusted Destination HISP
	12. SITE test results for XDR MT Test 33 are successful.
	XDR Delivery Failure: Unpublished Destination HISP Certificate
	13. SITE test results for XDR MT Test 34 are successful.
	XDR Delivery Failure: No Processed MDN
	14. SITE test results for XDR MT Test 35 are successful.
	XDR Delivery Failure: No Dispatched MDN
	15. SITE test results for XDR MT Test 36 are successful.
	XDR Delivery Failure: Timeout for Dispatched MDN
	16. SITE test results for XDR MT Test 37 are successful.
	XDR Positive Delivery Notification
	17. SITE test results for XDR MT Test 38 are successful.

Paragraph (h)(2)(ii) – Receive

System Under Test

SMTP: Disposition-Notification-Options Header

1. Using SITE: HISP Testing Portal, with the Message Tracking tab and “Your System as Receiver,” the Health IT Module is able to receive and successfully process a message from SITE (as Sending HISP) that contains a valid Disposition-Notification-Options Header and include it in the message to the destination (SMTP MT Test 39).
2. Negative Test: The Health IT Module is able to receive and successfully process a message from SITE (as Sending HISP) that contains an invalid Disposition-Notification-Options Header and include it in the message to the destination (SMTP MT Test 40).

XDR: Failure Notification (Configurable Wait Time Exceeded)

3. The Health IT Module receives a message from SITE (as Sending HISP), using SITE: HISP & Delivery Notification “XDR Cases” with “System as Receiver”, and is unable to deliver the message to its final destination (SITE as Destination Edge). The Health IT Module delivers a Processed MDN to SITE (as Sending HISP) followed by a delivery failure message to SITE (as Sending HISP) after the wait time has exceeded for delivering the message to its final destination (XDR MT Test 43).

XDR: Failure Notification

4. The Health IT Module receives a message from SITE (as Sending HISP), and is unable to deliver the message to its final destination (SITE as Destination Edge) due to a bad address (non-existent). The Health IT Module delivers a Processed MDN to SITE (as Sending HISP) followed by a delivery failure message to SITE (as Sending HISP) due to the bad address (non-existent) (XDR MT Test 44).

Test Lab Verification

SMTP: Disposition-Notification-Options Header

1. SITE test results for SMTP MT Test 39 are successful.
2. SITE test results for SMTP MT Test 40 are successful.

XDR: Failure Notification (Configurable Wait Time Exceeded)

3. SITE test results for XDR MT Test 43 are successful.

XDR: Failure Notification

4. SITE test results for XDR MT Test 44 are successful.

System Under Test	Test Lab Verification
SMTP: Disposition-Notification-Options Header 1. Using SITE: HISP Testing Portal, with the Message Tracking tab and “Your System as Receiver,” the Health IT Module is able to receive and successfully process a message from SITE (as Sending HISP) that contains a valid Disposition-Notification-Options Header and include it in the message to the destination (SMTP MT Test 39). 2. Negative Test: The Health IT Module is able to receive and successfully process a message from SITE (as Sending HISP) that contains an invalid Disposition-Notification-Options Header and include it in the message to the destination (SMTP MT Test 40). **XDR: Failure Notification (Configurable Wait Time Exceeded)** 3. The Health IT Module receives a message from SITE (as Sending HISP), using SITE: HISP & Delivery Notification “XDR Cases” with “System as Receiver”, and is unable to deliver the message to its final destination (SITE as Destination Edge). The Health IT Module delivers a Processed MDN to SITE (as Sending HISP) followed by a delivery failure message to SITE (as Sending HISP) after the wait time has exceeded for delivering the message to its final destination (XDR MT Test 43). **XDR: Failure Notification** 4. The Health IT Module receives a message from SITE (as Sending HISP), and is unable to deliver the message to its final destination (SITE as Destination Edge) due to a bad address (non-existent). The Health IT Module delivers a Processed MDN to SITE (as Sending HISP) followed by a delivery failure message to SITE (as Sending HISP) due to the bad address (non-existent) (XDR MT Test 44).	**SMTP: Disposition-Notification-Options Header** 1. SITE test results for SMTP MT Test 39 are successful. 2. SITE test results for SMTP MT Test 40 are successful. **XDR: Failure Notification (Configurable Wait Time Exceeded)** 3. SITE test results for XDR MT Test 43 are successful. **XDR: Failure Notification** 4. SITE test results for XDR MT Test 44 are successful.

Paragraph (h)(2)(i)(A) – Send

System Under Test

The Health IT Module provides evidence of and demonstrates successful send of encrypted and signed health information from the Health IT Module to three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(1) or (h)(2) capabilities) using SITE

Send Direct Message using Version 1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, which includes:

- Documentation of the Health IT Module sending “Wrapped” RFC-5751 messages to three partner HISPs.
- Documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies the Health IT Module has successfully sent encrypted and signed health information to three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015. The verification includes:

- Indication through documentation that the Health IT Module sent “Wrapped” RFC-5751, messages to three separate and unrelated HISP partners.
- Indication through documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Required Enhanced Testing: SITE Direct v1.2

The Health IT Module submits evidence of multi-partner testing with three different and unrelated partner HISPs using SITE Direct v1.2 (in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, August 2015), formatted only as a “wrapped” message.

Approved SVAP Version(s)

The Health IT Module submits evidence of multi-partner testing with three different and unrelated partner HISPs in accordance with the standard specified at ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3) formatted only as a

“wrapped” message.

System Under Test

The Health IT Module provides evidence of and demonstrates successful send of encrypted and signed health information from the Health IT Module to three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(1) or (h)(2) capabilities) using SITE Send Direct Message using Version 1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, which includes:

- Documentation of the Health IT Module sending “Wrapped” RFC-5751 messages to three partner HISPs.
- Documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies the Health IT Module has successfully sent encrypted and signed health information to three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015. The verification includes:

- Indication through documentation that the Health IT Module sent “Wrapped” RFC-5751, messages to three separate and unrelated HISP partners.
- Indication through documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(A) – Required Enhanced[1] Testing, Receive

[1] Partners with whom the Health IT Module chooses to test do not have to be certified at the time of testing as long as the testing uses SITE Direct v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015, formatted only as a “wrapped” message.

Approved SVAP Version(s)

[1] Partners with whom the Health IT Module chooses to test do not have to be certified at the time of testing as long as the testing uses SITE Direct v1.3, in accordance with the standard specified at ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct), formatted only as a “wrapped” message.

System Under Test

The user provides evidence of successful receipt of encrypted and signed health information from three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(2) capabilities) using SITE Send Direct Message v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015. The evidence includes:

- Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from three partner HISPs.
- Documentation of the Health IT Module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the three partner HISPs generated upon successfully receiving a Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies that the Health IT Module has received encrypted and signed health information from three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015. The documentation includes:

- Indication that the Health IT Module successfully received “Wrapped” RFC-5751, messages from three separate and unrelated HISP partners.
- Indication of the Health IT Module generating and transmitting processed Message Disposition Notification (MDNs) to each of the three partner HISPs generated upon receiving the Direct message from each partner HISP.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

System Under Test

The user provides evidence of successful receipt of encrypted and signed health information from three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(2) capabilities) using SITE Send Direct Message v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015. The evidence includes:

- Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from three partner HISPs.
- Documentation of the Health IT Module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the three partner HISPs generated upon successfully receiving a Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies that the Health IT Module has received encrypted and signed health information from three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015. The documentation includes:

- Indication that the Health IT Module successfully received “Wrapped” RFC-5751, messages from three separate and unrelated HISP partners.
- Indication of the Health IT Module generating and transmitting processed Message Disposition Notification (MDNs) to each of the three partner HISPs generated upon receiving the Direct message from each partner HISP.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(B) – Send

System Under Test

The Health IT Module provides evidence and demonstrates of successful send of encrypted and signed health information from the Health IT Module to three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(1) or (h)(2) capabilities) using SITE Send Direct Message v1.2, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification, which includes:

- Documentation of the Health IT Module sending “Wrapped” RFC-5751, messages to three partner HISPs.

- Documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies that the Health IT Module has successfully sent encrypted and signed health information to three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification. The verification includes:

- Indication through documentation that the Health IT Module sent “Wrapped” RFC-5751, messages to three separate and unrelated HISP partners.
- Indication through documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Required Enhanced Testing: ONC XDR and XDM for Direct

The Health IT Module submits evidence of multi-partner testing with three different and unrelated partner HISPs using SITE Direct v1.2, (in accordance with the standard specified at § 170.202(b): ONC XDR and XDM for Direct Messaging Specification (incorporated by reference in § 170.299)), including support for both limited and full XDS metadata profiles, formatted only as a “wrapped” message.

Approved SVAP Version(s)

The Health IT Module submits evidence of multi-partner testing with three different and unrelated partner HISPs in accordance with the standard specified at ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3) formatted only as a “wrapped” message.

System Under Test	Test Lab Verification

System Under Test

The Health IT Module provides evidence and demonstrates of successful send of encrypted and signed health information from the Health IT Module to three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(1) or (h)(2) capabilities) using SITE Send Direct Message v1.2, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification, which includes:

- Documentation of the Health IT Module sending "Wrapped" RFC-5751, messages to three partner HISPs.
- Documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated by the partner HISPs upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies that the Health IT Module has successfully sent encrypted and signed health information to three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification. The verification includes:

- Indication through documentation that the Health IT Module sent "Wrapped" RFC-5751, messages to three separate and unrelated HISP partners.
- Indication through documentation of the Health IT Module receiving processed Message Disposition Notifications (MDNs) from each of the three partner HISPs generated upon receiving the Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Paragraph (h)(2)(i)(B) – Required Enhanced[1] Testing, Receive

[1] Partners with whom the Health IT Module chooses to test do not have to be certified at the time of testing as long as the testing uses SITE Direct v1.2, in accordance with the standard specified at § 170.202(a)(2): Applicability Statement for Secure Health Transport v1.2, August 2015, formatted only as a "wrapped" message.

Approved SVAP Version(s)

[1] Partners with whom the Health IT Module chooses to test do not have to be certified at the time of testing as long as the testing uses SITE Direct v1.3, in accordance with the standard specified at ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct), formatted only as a “wrapped” message.

System Under Test

The user provides evidence of successful receipt of encrypted and signed health information from three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(2) capabilities) using SITE Direct v1.2, in accordance with the standard specified § 170.202(b) ONC XDR and XDM for Direct Messaging Specification. The evidence includes:

- Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from three partner HISPs.
- Documentation of the Health IT Module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the three partner HISPs generated upon successfully receiving a Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies that the Health IT Module has received encrypted and signed health information from three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification. The documentation includes:

- Indication that the Health IT Module successfully received “Wrapped” RFC-5751 messages from three separate and unrelated HISP partners.
- Indication of the Health IT Module generating and transmitting processed Message Disposition Notification (MDNs) to each of the three partner HISPs generated upon receiving the Direct message from each partner HISP.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

System Under Test	Test Lab Verification

System Under Test

The user provides evidence of successful receipt of encrypted and signed health information from three partners (e.g., other vendor Health IT Modules (HISPs) that have implemented (h)(2) capabilities) using SITE Direct v1.2, in accordance with the standard specified § 170.202(b) ONC XDR and XDM for Direct Messaging Specification. The evidence includes:

- Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from three partner HISPs.
- Documentation of the Health IT Module generates and sends processed Message Disposition Notifications (MDNs) that are transmitted to each of the three partner HISPs generated upon successfully receiving a Direct message from the Health IT Module.

Approved SVAP Version(s)

Complete this test in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Test Lab Verification

The tester verifies that the Health IT Module has received encrypted and signed health information from three partner HISPs using SITE Direct v1.2, in accordance with the standard specified at § 170.202(b) ONC XDR and XDM for Direct Messaging Specification. The documentation includes:

- Indication that the Health IT Module successfully received “Wrapped” RFC-5751 messages from three separate and unrelated HISP partners.
- Indication of the Health IT Module generating and transmitting processed Message Disposition Notification (MDNs) to each of the three partner HISPs generated upon receiving the Direct message from each partner HISP.

Approved SVAP Version(s)

Complete verifications of this test in accordance with ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3)

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (h)(2) *Direct Project, Edge Protocol, and XDR/XDM—*

1. Able to send and receive health information in accordance with:
    1. The standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message;
    2. The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and
    3. Both edge protocol methods specified by the standard in § 170.202(d).
2. *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

Standard(s) Referenced

Paragraph (h)(2)(i)(A)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.2, August 2015

Paragraph (h)(2)(i)(B)

§ 170.202(b) ONC XDR and XDM for Direct Messaging Specification

Paragraph (h)(2)(i)(C)

§ 170.202(d) ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014

Paragraph (h)(2)(ii)

§ 170.202(e)(1) Delivery Notification - Implementation Guide for Delivery Notification in Direct v1.0

Standard Version Advancement Process (SVAP) Version(s) Approved

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing: Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.

Privacy & Security Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(h)(2). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(h) criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (h) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "View, download, and transmit to 3rd party (VDT)" and (e)(2) "Secure messaging," which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

If choosing Approach 2:

For each applicable privacy and security certification criterion not certified using Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with new SITE UI language	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (h)(2) *Direct Project, Edge Protocol, and XDR/XDM—*

1. Able to send and receive health information in accordance with:
    1. The standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message;
    2. The standard specified in § 170.202(b), including support for both limited and full XDS metadata profiles; and
    3. Both edge protocol methods specified by the standard in § 170.202(d).
2. *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in § 170.202(e)(1).

Standard(s) Referenced

Paragraph (h)(2)(i)(A)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.2, August 2015

Paragraph (h)(2)(i)(B)

§ 170.202(b) ONC XDR and XDM for Direct Messaging Specification

Paragraph (h)(2)(i)(C)

§ 170.202(d) ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014

Paragraph (h)(2)(ii)

§ 170.202(e)(1) Delivery Notification - Implementation Guide for Delivery Notification in Direct v1.0

Standard Version Advancement Process (SVAP) Version(s) Approved

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct)

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

Certification Dependencies
Conditions and Maintenance of Certification

Real World Testing: Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.

Privacy & Security Requirements
Privacy and Security: This certification criterion was adopted at § 170.315(h)(2). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(h) criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (h) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "View, download, and transmit to 3rd party (VDT)" and (e)(2) "Secure messaging," which are explicitly stated.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

If choosing Approach 2:

For each applicable privacy and security certification criterion not certified using Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Testing

Testing Tool

Standards Implementation & Testing Environment (SITE): Direct Tooling, Send Direct Message

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(h)(2)	Refer to the Standards Implementation & Testing Environment (SITE)

Certification Companion Guide: Direct Project, Edge Protocol, and XDR/XDM

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product certification. The CCG is not a substitute for the requirements outlined in regulation and related ONC final rules. It extracts key portions of ONC final rules' preambles and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the Certification Regulations page for links to all ONC final rules or consult other regulatory references as noted. The CCG is for public use and should not be sold or redistributed.

The below table outlines whether this criterion has additional Maintenance of Certification dependencies, update requirements and/or eligibility for standards updates via SVAP. Review the Certification Dependencies and Required Update Deadline drop-downs above if this table indicates “yes” for any field.

Base EHR Definition	Real World Testing	Insights Condition	SVAP	Requires Updates
Included	Yes	No	Yes	No

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- In order to meet the Base EHR Definition, a provider would need to possess technology that has been certified to either this criterion at § 170.315(h)(2) or the “Direct Project” criterion at § 170.315(h)(1).
- Several training/demo videos of the Edge Testing Tool (ETT) used for the testing and certification of health IT are available on GitHub.

  Please address any ETT technical questions through the ETT Google Group.
- This certification criterion uses the Applicability Statement for Secure Health Transport, Version 1.2 standard. This new version of the specification includes updates that improve interoperability through the clarification of requirements that have been subject to varying interpretations, particularly requirements around message delivery notifications. This version also clarifies pertinent requirements in the standards underlying the Applicability Statement for Secure Health Transport. Refer to the standard for more details about the improvements it includes. [see also 80 FR 62679]
- Testing for this criterion will require the processing of invalid test cases that frequently occur in real-world situations so that Security/Trust Agents (STAs) can demonstrate error handling abilities, including handling XDM packages and message disposition.
- Direct, the Edge protocols (SMTP, XDR) and XDM processing are the required standards for health IT certifying to (h)(2). IMAP and POP3 are optional SMTP standards. [see also 80 FR 62680]
- Certification to this criterion is the only option for “transport-only” focused health information services providers (HISPs). However, HISP technology certified to this criterion would be able to electronically exchange with any health IT certified to § 170.315(b)(1) Transitions of care criterion. Further, HISP technology certified to this criterion may also be used to meet the Base EHR definition with any other health IT certified to § 170.315(b)(1) without the need for joint certification of the products.

- Consistent with the IG for Delivery Notification in Direct, ONC's policy intent is that the receiving HISP must provide delivery notification messages either when it is also the sending HISP, or when it is specifically requested to do so by the sending HISP. A HISP is not compelled to request delivery notifications, but a certified HISP is required to produce them if requested.
- A secure network is generally recognized as one where all of the nodes (endpoints) are known, uniquely identified, access controlled, with strong end-to-end encryption. For example, a virtual private network (VPN) or a network physically isolated from any other with specialized equipment using endpoint encryption.

Clarifications:

- In order to meet the Base EHR Definition, a provider would need to possess technology that has been certified to either this criterion at § 170.315(h)(2) or the "Direct Project" criterion at § 170.315(h)(1).
- Several training/demo videos of the Edge Testing Tool (ETT) used for the testing and certification of health IT are available on GitHub.
  Please address any ETT technical questions through the ETT Google Group.
- This certification criterion uses the Applicability Statement for Secure Health Transport, Version 1.2 standard. This new version of the specification includes updates that improve interoperability through the clarification of requirements that have been subject to varying interpretations, particularly requirements around message delivery notifications. This version also clarifies pertinent requirements in the standards underlying the Applicability Statement for Secure Health Transport. Refer to the standard for more details about the improvements it includes. [see also 80 FR 62679]
- Testing for this criterion will require the processing of invalid test cases that frequently occur in real-world situations so that Security/Trust Agents (STAs) can demonstrate error handling abilities, including handling XDM packages and message disposition.
- Direct, the Edge protocols (SMTP, XDR) and XDM processing are the required standards for health IT certifying to (h)(2). IMAP and POP3 are optional SMTP standards. [see also 80 FR 62680]
- Certification to this criterion is the only option for "transport-only" focused health information services providers (HISPs). However, HISP technology certified to this criterion would be able to electronically exchange with any health IT certified to § 170.315(b)(1) Transitions of care criterion. Further, HISP technology certified to this criterion may also be used to meet the Base EHR definition with any other health IT certified to § 170.315(b)(1) without the need for joint certification of the products.
- Consistent with the IG for Delivery Notification in Direct, ONC's policy intent is that the receiving HISP must provide delivery notification messages either when it is also the sending HISP, or when it is specifically requested to do so by the sending HISP. A HISP is not compelled to request delivery notifications, but a certified HISP is required to produce them if requested.
- A secure network is generally recognized as one where all of the nodes (endpoints) are known, uniquely identified, access controlled, with strong end-to-end encryption. For example, a virtual private network (VPN) or a network physically isolated from any other with specialized equipment using endpoint encryption.

Paragraph (h)(2)(i) Send and receive health information

Technical outcome – The Health IT Module can electronically transmit (send and receive) health information to and from a third party using each of:

- Applicability Statement for Secure Health Transport, Version 1.2 (the “Direct Project” specification);
- The ONC XDR and XDM for Direct Messaging Specification, Version 1, including support for both limited and full XDS metadata profiles;
- And both of the protocols in the ONC Implementation Guide for Direct Edge Protocols, Version 1.1.

Clarifications:

- This criterion requires the three capabilities specified (Direct Project specification, Edge Protocol compliance, and XDR/XDM processing) because it must support interoperability and all potential certified exchange options. A provider could use an “independent” HISP to meet the Base EHR definition. In such a case, the HISP would need to be certified to this criterion in order for the provider to use it to meet the Base EHR definition, which is part of the CEHRT definition under the Promoting Interoperability Programs. [see also 80 FR 62681]
- For developers implementing the ONC XDR/XDM for Direct Messaging Specification, when converting an SMTP message into XDR (with limited metadata), UUID URNs formatted as OIDs should be used for DocumentEntry.uniqueId, SubmissionSet.sourceId, and SubmissionSet.uniqueId ONC expects testing to this specification to reflect this clarification.
- Even though the IG for Edge Protocols requires support for XDS limited metadata, XDR/XDM supports capability to transform messages using full metadata wherever appropriate. Therefore, ONC requires that a Health IT Module must support both the XDS Metadata profiles (limited and full), as specified in the underlying IHE specifications, to ensure that the transformation between messages packaged using XDR/XDM are done with as much appropriate metadata as possible. [see also 80 FR 62681]
- For certification to this criterion, ONC has made it a requirement to send and receive messages in only “wrapped” format even though the specification (IG) allows use of “unwrapped” messages. This requirement will further improve interoperability among Security/Trust Agents (STAs) while having minor development impact on health IT developers. [see also 80 FR 62679]

- The protocols listed in the IG, section 1.3.1 explicitly list conformance to RFC 3501. The RFC, then originally published, mandated using the TLS_RSA_WITH_RC4_128_MD5 cipher suite within the TLS 1.0 bundle. RFC 3501 has had subsequent updates making the listed cipher suite obsolete and rescinded within the TLS 1.0 bundle. Current industry practice is to implement cipher suites that are compliant with TLS 1.1(shall), TLS 1.2 (should), and TLS 1.0 (may).

Technical outcome – The Health IT Module can electronically transmit (send and receive) health information to and from a third party using each of:

- Applicability Statement for Secure Health Transport, Version 1.2 (the “Direct Project” specification);
- The ONC XDR and XDM for Direct Messaging Specification, Version 1, including support for both limited and full XDS metadata profiles;
- And both of the protocols in the ONC Implementation Guide for Direct Edge Protocols, Version 1.1.

Clarifications:

- This criterion requires the three capabilities specified (Direct Project specification, Edge Protocol compliance, and XDR/XDM processing) because it must support interoperability and all potential certified exchange options. A provider could use an “independent” HISP to meet the Base EHR definition. In such a case, the HISP would need to be certified to this criterion in order for the provider to use it to meet the Base EHR definition, which is part of the CEHRT definition under the Promoting Interoperability Programs. [see also 80 FR 62681]
- For developers implementing the ONC XDR/XDM for Direct Messaging Specification, when converting an SMTP message into XDR (with limited metadata), UUID URNs formatted as OIDs should be used for DocumentEntry.uniqueId, SubmissionSet.sourceId, and SubmissionSet.uniqueId ONC expects testing to this specification to reflect this clarification.
- Even though the IG for Edge Protocols requires support for XDS limited metadata, XDR/XDM supports capability to transform messages using full metadata wherever appropriate. Therefore, ONC requires that a Health IT Module must support both the XDS Metadata profiles (limited and full), as specified in the underlying IHE specifications, to ensure that the transformation between messages packaged using XDR/XDM are done with as much appropriate metadata as possible. [see also 80 FR 62681]
- For certification to this criterion, ONC has made it a requirement to send and receive messages in only “wrapped” format even though the specification (IG) allows use of “unwrapped” messages. This requirement will further improve interoperability among Security/Trust Agents (STAs) while having minor development impact on health IT developers. [see also 80 FR 62679]
- The protocols listed in the IG, section 1.3.1 explicitly list conformance to RFC 3501. The RFC, then originally published, mandated using the TLS_RSA_WITH_RC4_128_MD5 cipher suite within the TLS 1.0 bundle. RFC 3501 has had subsequent updates making the listed cipher suite obsolete and rescinded within the TLS 1.0 bundle. Current industry practice is to implement cipher suites that are compliant with TLS 1.1(shall), TLS 1.2 (should), and TLS 1.0 (may).

Paragraph (h)(2)(ii) Delivery notification in Direct

Technical outcome – The health IT can electronically transmit (send and receive) health information to a 3rd party using Direct in accordance with the Implementation Guide (IG) for Delivery Notification in Direct, Version 1.0.

Clarifications:

- The IG for Delivery Notification in Direct, Version 1.0, June 29, 2012 functionality supports interoperability and exchange, particularly for both sending and receiving parties, guidance enabling HISPs to provide a high level of assurance to senders that a message has arrived at its destination, a necessary component to interoperability. The IG also outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system. [see also 80 FR 62729]
- For Delivery Notification in Direct, the capability to send and receive health information must be in accordance with the Implementation Guide for Delivery Notification in Direct v1.0.

Technical outcome – The health IT can electronically transmit (send and receive) health information to a 3rd party using Direct in accordance with the Implementation Guide (IG) for Delivery Notification in Direct, Version 1.0.

Clarifications:

- The IG for Delivery Notification in Direct, Version 1.0, June 29, 2012 functionality supports interoperability and exchange, particularly for both sending and receiving parties, guidance enabling HISPs to provide a high level of assurance to senders that a message has arrived at its destination, a necessary component to interoperability. The IG also outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system. [see also 80 FR 62729]
- For Delivery Notification in Direct, the capability to send and receive health information must be in accordance with the Implementation Guide for Delivery Notification in Direct v1.0.