Direct Project | HealthIT.gov

healthit.gov/test-method/direct-project

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 03-21-2025

Regulation Text

Regulation Text

§ 170.315 (h)(1) *Direct Project—*

1. *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message.
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)(1)(i)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, June 26, 2018

Paragraph (h)(1)(ii)

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

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

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.
- Transitions of care (§ 170.315(b)(1)): An ONC-ACB can only issue a certification to a Health IT Module for this criterion at § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1) "Transitions of care."

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(h)(1). 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

Version #	Description of Change	Version Date
1.2	Updated tool references to reflect new SITE tool names	03-21-2025

Regulation Text
Regulation Text

§ 170.315 (h)(1) *Direct Project—*

1. *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message.
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)(1)(i)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, June 26, 2018

Paragraph (h)(1)(ii)

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

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

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.

- Transitions of care (§ 170.315(b)(1)): An ONC-ACB can only issue a certification to a Health IT Module for this criterion at § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1) "Transitions of care."

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(h)(1). 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

SITE: Direct Certificate Discovery Tool (DCDT)

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(h)(1)	Refer to 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 tool references to reflect new SITE tool names	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

Paragraph (h)(1)(i) - Send

System Under Test

Discover Certificates

1. The user performs setup tasks by visiting ASTP Standards Implementation & Testing Environment (SITE)'s Direct Tooling for H1. In the dropdown menu, select paragraph (i) Certificate Discovery / Hosting (DCDT) and download the DCDT Trust Anchor. Then, upload it into the Health IT Module's Direct instance, and map 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 H1 and registers a Direct address within SITE and corresponding Contact Email address for receipt of the SITE validation report.

Send Health Information Using Direct

3. The user identifies the payload for sending to SITE. ASTP/ONC-supplied payloads are available for download from SITE: Direct Tooling.
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 using identified health IT function(s).

Based upon the types of Direct messages the Health IT Module supports for sending of information ("wrapped" RFC-5751, messages only), 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.

Approved SVAP Version(s)

- Complete step 1 using DCDT as described above.
- Complete steps 3-4 using SITE: Direct Tooling for H1, paragraph (i) Send Direct Message, using Direct v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (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 DCDT. All listed certificates listed in both DNS and LDAP must be tested corresponding to the standard 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 the SITE validation report.

Send Health Information Using Direct

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 the 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), and using the RFC-5751, "wrapped" message format.
5. Using the validation report, the tester verifies that SITE was able to successfully decrypt the message, and that the payload was successfully received by SITE.

System Under Test	Test Lab Verification
Discover Certificates	**Discover Certificates**

System Under Test

1. The user performs setup tasks by visiting ASTP Standards Implementation & Testing Environment (SITE)'s Direct Tooling for H1. In the dropdown menu, select paragraph (i) Certificate Discovery / Hosting (DCDT) and download the DCDT Trust Anchor. Then, upload it into the Health IT Module's Direct instance, and map 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 H1 and registers a Direct address within SITE and corresponding Contact Email address for receipt of the SITE validation report.

Send Health Information Using Direct

3. The user identifies the payload for sending to SITE. ASTP/ONC-supplied payloads are available for download from SITE: Direct Tooling.
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 using identified health IT function(s).

Based upon the types of Direct messages the Health IT Module supports for sending of information ("wrapped" RFC-5751, messages only), 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.

Approved SVAP Version(s)

- Complete step 1 using DCDT as described above.
- Complete steps 3-4 using SITE: Direct Tooling for H1, paragraph (i) Send Direct Message, using Direct v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

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 DCDT. All listed certificates listed in both DNS and LDAP must be tested corresponding to the standard 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 the SITE validation report.

Send Health Information Using Direct

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 the 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), and using the RFC-5751, "wrapped" message format.
5. Using the validation report, the tester verifies that SITE was able to successfully decrypt the message, and that the payload was successfully received by SITE.

Paragraph (h)(1)(i) - 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 H1 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 tool.

SUT Connection

2. The user selects "Send Direct Message" within SITE: Direct Tooling for H1 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.
    - Installation of the SITE/Direct Tooling's Valid Trust Anchor within the Health IT Module.
    - Identification 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, and sends corresponding Message Delivery Notifications (MDNs).

Reject Receipt of Direct Message (Negative Testing)

4. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Invalid Certificate.
5. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Expired Certificate.
6. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).
7. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
8. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Invalid Message Digest.

Approved SVAP Version(s)

- Complete step 1 using DCDT as described above.
- Complete step 2 using SITE: Direct Tooling for H1, paragraph (i) Receive - Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

- Complete step 3 using SITE: Direct Tooling for H1, paragraph (i) Receive - Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).
- Complete following additional steps:
    - The user receives messages using certificates with 3072 bits sent from SITE using Direct in accordance with ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022, and sends corresponding Message Delivery Notifications (MDNs).
    - The user receives messages using certificates with 4096 bits sent from SITE using Direct in accordance with ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022, and sends corresponding Message Delivery Notifications (MDNs).
    - The user receives messages created using different signature algorithms specified on SITE using Direct in accordance with ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022, and sends corresponding Message Delivery Notifications (MDNs).
- Complete steps 4-8 using SITE: Direct Tooling for H1, paragraph (i) Receive - Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).
- Complete the following additional steps:
    - *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: WILD_CARD_DOMAIN_CERT.*
    - *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_EMAIL_ADDRESS*
    - *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_LESS_THAN_2048_BITS*
    - *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_NO_CRL*
    - *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_NO_NOTBEFORE_ATTR.*
    - *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_NO_NOTAFTER_ATTR*

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 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-5751, messages and that a MDN from the Health IT Module was received on SITE for all messages SITE sent.

Reject Receipt of Direct Message (Negative Testing)

4. Invalid Certificate: The tester verifies the Health IT Module rejects a Direct message received with an invalid Trust Anchor and no corresponding MDN was received by SITE from the Health IT Module.
5. Expired Certificate: The tester verifies the Health IT Module rejects a Direct message 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 a Direct message received with an invalid Trust Relationship. The tester verifies 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 a Direct message received without an Authority Information Access (AIA) extension 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 a Direct message received with an invalid message digest that no corresponding MDN was received by SITE from the Health IT Module.

Approved SVAP Version(s)

- Complete step 1 verification for the DCDT SVAP 2022 test cases executed.
- Complete step 3 verification using SITE: Direct Tooling for H1, paragraph (i) Receive – Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

- Complete the following additional verifications:
    - *The tester verifies health information can be successfully received by the Health IT Module from SITE, in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct), and a MDN from the Health IT Module was received on SITE for all messages the SITE sent using certificates with 3072 bits.*
        NOTE: This is an optional requirement, so not receiving a MDN amounts to only a WARNING and not a failure.
    - *The tester verifies health information can be successfully received by the Health IT Module from SITE, in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct), and a MDN from the Health IT Module was received on SITE for all messages SITE sent using certificates with 4096 bits.*
        NOTE: This is an optional requirement, so not receiving a MDN amounts to only a WARNING and not a failure.
    - *The tester verifies health information can be successfully received by the Health IT Module from SITE, in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct), and a MDN from the Health IT Module was received on SITE for all messages SITE sent using different signature algorithms specified on SITE.*
        NOTE: ECDSA based signature algorithms are optional requirement, so not receiving a MDN amounts to only a WARNING and not a failure.
- Complete step 4-8 verifications in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).
- Complete the following additional verifications:
    - *WILD_CARD_DOMAIN_CERT: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
    - *CERT_WITH_EMAIL_ADDRESS: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
    - *CERT_LESS_THAN_2048_BITS: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
    - *CERT_WITH_NO_CRL: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
    - *CERT_WITH_NO_NOTBEFORE_ATTR: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
    - *CERT_WITH_NO_NOTAFTER_ATTR: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*

System Under Test	Test Lab Verification
Hosting Certificates	**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.

System Under Test

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 H1 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 tool.

SUT Connection

2. The user selects "Send Direct Message" within SITE: Direct Tooling for H1 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.
    - Installation of the SITE/Direct Tooling's Valid Trust Anchor within the Health IT Module.
    - Identification 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, and sends corresponding Message Delivery Notifications (MDNs).

Reject Receipt of Direct Message (Negative Testing)

4. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Invalid Certificate.

SUT Connection
Test Lab Verification

2. No action required.

Receive Direct 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(a)(2), using "wrapped" RFC-5751, messages and that a MDN from the Health IT Module was received on SITE for all messages SITE sent.

Reject Receipt of Direct Message (Negative Testing)

4. Invalid Certificate: The tester verifies the Health IT Module rejects a Direct message received with an invalid Trust Anchor and no corresponding MDN was received by SITE from the Health IT Module.
5. Expired Certificate: The tester verifies the Health IT Module rejects a Direct message 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 a Direct message received with an invalid Trust Relationship. The tester verifies 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 a Direct message received without an Authority Information Access (AIA) extension 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 a Direct message received with an invalid message digest that no corresponding MDN was received by SITE from the Health IT Module.

Approved SVAP Version(s)

- Complete step 1 verification for the DCDT SVAP 2022 test cases executed.
- Complete step 3 verification using SITE: Direct Tooling for H1, paragraph (i) Receive – Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

System Under Test

5. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Expired Certificate.
6. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Invalid Trust Relationship (Different Trust Anchor).
7. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: No Authority Information Access (AIA) Extension.
8. The user rejects health information 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 the SITE to the Health IT Module using the following tool option: Invalid Message Digest.

Approved SVAP Version(s)

- Complete step 1 using DCDT as described above.
- Complete step 2 using SITE: Direct Tooling for H1, paragraph (i) Receive - Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).
- Complete step 3 using SITE: Direct Tooling for H1, paragraph (i) Receive - Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

- Complete the following additional verifications:
  - *The tester verifies health information can be successfully received by the Health IT Module from SITE, in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct), and a MDN from the Health IT Module was received on SITE for all messages the SITE sent using certificates with 3072 bits.*
    NOTE: This is an optional requirement, so not receiving a MDN amounts to only a WARNING and not a failure.
  - *The tester verifies health information can be successfully received by the Health IT Module from SITE, in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct), and a MDN from the Health IT Module was received on SITE for all messages SITE sent using certificates with 4096 bits.*
    NOTE: This is an optional requirement, so not receiving a MDN amounts to only a WARNING and not a failure.
  - *The tester verifies health information can be successfully received by the Health IT Module from SITE, in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct), and a MDN from the Health IT Module was received on SITE for all messages SITE sent using different signature algorithms specified on SITE.*
    NOTE: ECDSA based signature algorithms are optional requirement, so not receiving a MDN amounts to only a WARNING and not a failure.
- Complete step 4-8 verifications in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

System Under Test

- Complete following additional steps:
  - The user receives messages using certificates with 3072 bits sent from SITE using Direct in accordance with ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022, and sends corresponding Message Delivery Notifications (MDNs).
  - The user receives messages using certificates with 4096 bits sent from SITE using Direct in accordance with ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022, and sends corresponding Message Delivery Notifications (MDNs).
  - The user receives messages created using different signature algorithms specified on SITE using Direct in accordance with ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022, and sends corresponding Message Delivery Notifications (MDNs).
- Complete steps 4-8 using SITE: Direct Tooling for H1, paragraph (i) Receive - Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

- Complete the following additional verifications:
  - *WILD_CARD_DOMAIN_CERT: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
  - *CERT_WITH_EMAIL_ADDRESS: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
  - *CERT_LESS_THAN_2048_BITS: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
  - *CERT_WITH_NO_CRL: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
  - *CERT_WITH_NO_NOTBEFORE_ATTR: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*
  - *CERT_WITH_NO_NOTAFTER_ATTR: The tester verifies the Health IT Module rejects a Direct message received with an invalid message digest that no corresponding MDN was received by the Health IT Module from SITE.*

System Under Test	Test Lab Verification

• Complete the following additional steps:
  ◦ *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: WILD_CARD_DOMAIN_CERT.*
  ◦ *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_EMAIL_ADDRESS*
  ◦ *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_LESS_THAN_2048_BITS*
  ◦ *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_NO_CRL*
  ◦ *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_NO_NOTBEFORE_ATTR.*
  ◦ *The user rejects health information not in accordance with the ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct) adopted via the SVAP 2022 sent from SITE to the Health IT Module using the following tool option: CERT_WITH_NO_NOTAFTER_ATTR*	

Paragraph (h)(1)(ii) – Message Disposition Notification: Processed

System Under Test

Disposition-Notification-Options Header

1. Using SITE: HISP Testing Portal “Message Tracking” using “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 includes it in the message to the destination via SMTP MT Test 39.
2. Negative Testing: 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 includes it in the message to the destination via SMTP MT Test 40.

Approved SVAP Version(s)

Complete steps 1-2 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3).

Test Lab Verification

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.

Approved SVAP Version(s)

Complete verifications against the test outcome by SITE: Direct Tooling for H1, paragraph (ii) Delivery Notifications, v1.3 for SMTP MT Test 39 and 40.

System Under Test

Disposition-Notification-Options Header

1. Using SITE: HISP Testing Portal “Message Tracking” using “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 includes it in the message to the destination via SMTP MT Test 39.
2. Negative Testing: 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 includes it in the message to the destination via SMTP MT Test 40.

Approved SVAP Version(s)

Complete steps 1-2 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct v1.3).

Test Lab Verification

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.

Approved SVAP Version(s)

Complete verifications against the test outcome by SITE: Direct Tooling for H1, paragraph (ii) Delivery Notifications, v1.3 for SMTP MT Test 39 and 40.

Paragraph (h)(1)(ii) – Message Disposition Notification: Failed

System Under Test

Failure Notification

1. Using SITE: HISP Testing Portal “Message Tracking” using “Your system as “Receiver”, the Health IT Module successfully validates security and trust returning a Processed MDN, but cannot deliver the message to its final destination (mailbox full, unavailable, mailbox does not exist) - generating a MDN failed or a failure Delivery Status Notification via SMTP MT Test 41.

Approved SVAP Version(s)

Complete this test using SITE: Direct Tooling for H1 paragraph (ii) Delivery Notifications, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

Failure Notification

1. The SITE test results for SMTP MT Test 41 are successful.

Approved SVAP Version(s)

Complete verifications against the test outcome using SITE: Direct Tooling for H1 paragraph (ii) Delivery Notifications, v1.3 for this test.

System Under Test	Test Lab Verification
Failure Notification 1. Using SITE: HISP Testing Portal “Message Tracking” using “Your system as “Receiver”, the Health IT Module successfully validates security and trust returning a Processed MDN, but cannot deliver the message to its final destination (mailbox full, unavailable, mailbox does not exist) - generating a MDN failed or a failure Delivery Status Notification via SMTP MT Test 41. **Approved SVAP Version(s)** Complete this test using SITE: Direct Tooling for H1 paragraph (ii) Delivery Notifications, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).	**Failure Notification** 1. The SITE test results for SMTP MT Test 41 are successful. **Approved SVAP Version(s)** Complete verifications against the test outcome using SITE: Direct Tooling for H1 paragraph (ii) Delivery Notifications, v1.3 for this test.

Paragraph (h)(1)(i) – Required Enhanced Testing, Send

System Under Test

The Health IT Module provides evidence and demonstration 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 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, which includes:

- Documentation of the Health IT Module sending “Wrapped” RFC-5751, messages to three partner HISPs; and
- Documentation of the Health IT Module receiving processed 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 using SITE: Direct Tooling for H1, paragraph (i) Send Direct Message, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

The tester verifies the Health IT Module has successfully sent encrypted and signed health information to three partner HISPs using Direct v1.2, in accordance with the standard specified at § 170.202(a)(2). 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 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 against the test outcome by using SITE: Direct Tooling for H1, paragraph (i) Send Direct Message, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Required Enhanced Testing

The Health IT Module submits evidence of multi-partner testing with three different and unrelated partner HISPs using SITE: Direct Tooling for H1 v1.2, (in accordance with the standard specified at § 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2), 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 using SITE: Direct Tooling for H1, v1.3, (in accordance with the standard specified at ONC Applicability Statement for Secure Health Transport, Version 1.3, May 2021 (Direct)), formatted only as a “wrapped” message.

System Under Test	Test Lab Verification

System Under Test

The Health IT Module provides evidence and demonstration 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 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, which includes:

- Documentation of the Health IT Module sending "Wrapped" RFC-5751, messages to three partner HISPs; and
- Documentation of the Health IT Module receiving processed 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 using SITE: Direct Tooling for H1, paragraph (i) Send Direct Message, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

The tester verifies the Health IT Module has successfully sent encrypted and signed health information to three partner HISPs using Direct v1.2, in accordance with the standard specified at § 170.202(a)(2). 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 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 against the test outcome by using SITE: Direct Tooling for H1, paragraph (i) Send Direct Message, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

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

[1] Partners the Health IT Module chooses to test with do not have to be certified at the time of testing as long as the testing uses the 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), formatted only as a "wrapped" message.

Approved SVAP Version(s)

[1] Partners who the Health IT Module chooses to test with do not have to be certified at the time of testing as long as the testing uses the Direct v1.3 (in accordance with the standard specified at ONC Applicability Statement for Secure Health Transport, Version 1.3, 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 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. The evidence includes:

- Documentation of the Health IT Module receiving “Wrapped” RFC-5751 messages from three partner HISPs; and
- Documentation that the Health IT Module generates and sends processed 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 using SITE: Direct Tooling for H1, paragraph (i) Receive – Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

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

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

Approved SVAP Version(s)

Complete verifications against the test outcome using SITE: Direct Tooling for H1, paragraph (i) Receive – Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

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 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. The evidence includes:

- Documentation of the Health IT Module receiving "Wrapped" RFC-5751 messages from three partner HISPs; and
- Documentation that the Health IT Module generates and sends processed 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 using SITE: Direct Tooling for H1, paragraph (i) Receive – Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Test Lab Verification

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

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

Approved SVAP Version(s)

Complete verifications against the test outcome using SITE: Direct Tooling for H1, paragraph (i) Receive – Message Status, v1.3 in accordance with the standards specified in ONC Applicability Statement for Secure Health Transport, v1.3, May 2021 (Direct).

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (h)(1) *Direct Project*—

1. *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message.
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)(1)(i)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, June 26, 2018

Paragraph (h)(1)(ii)

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

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

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.
- Transitions of care (§ 170.315(b)(1)): An ONC-ACB can only issue a certification to a Health IT Module for this criterion at § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1) "Transitions of care."

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(h)(1). 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 tool references to reflect new SITE tool names	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (h)(1) *Direct Project*—

1. *Applicability Statement for Secure Health Transport.* Able to send and receive health information in accordance with the standard specified in § 170.202(a)(2), including formatted only as a "wrapped" message.
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)(1)(i)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, v1.2, June 26, 2018

Paragraph (h)(1)(ii)

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

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

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.
- Transitions of care (§ 170.315(b)(1)): An ONC-ACB can only issue a certification to a Health IT Module for this criterion at § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1) "Transitions of care."

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(h)(1). 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

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

Testing
Testing Tool

SITE: Direct Certificate Discovery Tool (DCDT)

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(h)(1)	Refer to SITE

Certification Companion Guide: Direct Project

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 ONC Regulations page for links to all 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)(1) or the "Direct Project, Edge Protocol, and XDR/XDM" criterion at § 170.315(h)(2).
- Use of the Applicability Statement for Secure Health Transport ("Direct") is required to meet this certification criterion. There is no exemption or additional possible transport standard for certification to this criterion.

- 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.
- As specified in § 170.550(j), an ONC-ACB can only issue a certification to a Health IT Module for § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1). For example, if Developer X seeks certification to (b)(1) and (h)(1) with its homegrown integrated health information service provider (HISP) solution, then their ONC-ACB can issue a certificate with (h)(1) included. Likewise, if Developer X seeks certification to (b)(1) and partners with/integrates a third party HISP for (h)(1) consistent with the "relied upon software" paradigm, then their ONC-ACB can issue a certificate with (h)(1) included. To note, in this instance, the certification would be specific to Developer X and the third party HISP. Each developer that would want to work with the third party HISP in a similar manner would need to seek the same type of relied upon software certification. Thus, HISPs may want to consider certifying to § 170.315(h)(2), which would not require separate testing/certifications with each developer certified to § 170.315(b)(1).
- Consistent with the Implementation Guide 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.

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)(1) or the "Direct Project, Edge Protocol, and XDR/XDM" criterion at § 170.315(h)(2).
- Use of the Applicability Statement for Secure Health Transport ("Direct") is required to meet this certification criterion. There is no exemption or additional possible transport standard for certification to this criterion.
- 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.
- As specified in § 170.550(j), an ONC-ACB can only issue a certification to a Health IT Module for § 170.315(h)(1) if the Health IT Module's certification also includes § 170.315(b)(1). For example, if Developer X seeks certification to (b)(1) and (h)(1) with its homegrown integrated health information service provider (HISP) solution, then their ONC-ACB can issue a certificate with (h)(1) included. Likewise, if Developer X seeks certification to (b)(1) and partners with/integrates a third party HISP for (h)(1) consistent with the "relied upon software" paradigm, then their ONC-ACB can issue a certificate with (h)(1) included. To note, in this instance, the certification would be specific to Developer X and the third party HISP. Each developer that would want to work with the third party HISP in a similar manner would need to seek the same type of relied upon software certification. Thus, HISPs may want to consider certifying to § 170.315(h)(2), which would not require separate testing/certifications with each developer certified to § 170.315(b)(1).
- Consistent with the Implementation Guide 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.

Paragraph (h)(1)(i) Applicability statement for secure health transport

Technical outcome – The health IT can electronically transmit (send and receive) health information to a 3rd party which must be formatted only as a "wrapped" message using the Applicability Statement for Secure Health Transport, Version 1.2.

Clarifications:

For certification to this criterion, ONC has made it a requirement to send and receive messages in only "wrapped" format even though the specification 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]

Technical outcome – The health IT can electronically transmit (send and receive) health information to a 3rd party which must be formatted only as a "wrapped" message using the Applicability Statement for Secure Health Transport, Version 1.2.

Clarifications:

> For certification to this criterion, ONC has made it a requirement to send and receive messages in only "wrapped" format even though the specification 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]

Paragraph (h)(1)(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. It provides guidance for 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 standard specified in § 170.202(e)(1).

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. It provides guidance for 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 standard specified in § 170.202(e)(1).