§170.315(h)(1) Direct Project

2015 Edition CCGs

Version 1.4 Updated on 10-07-2016

Revision History		
Version #	**Description of Change**	**Version Date**
1.0	Initial Publication	10-30-2015
1.1	Removed email protocol clarification that's not applicable for 2015 Edition certification. Added update reference for Delivery Notification in Direct.	03-26-2016
1.2	Corrected the title for paragraph (h)(1)(ii) in regulation text to read "Delivery Notification in Direct" per the 2015 Edition final rule correction notice.	04-14-2016
1.3	Reference to § 170.550(j) requirement added, which clarifies that 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). Examples of certification options provided.	06-30-2016
1.4	Added HISP guidance in regards to sending dispatched MDNs in production.	10-07-2016

Regulation Text

Regulation Text

§170.315 (h)(1) *Direct Project—*

(i) *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.

(ii) *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, Version 1.2, August 2015

Paragraph (h)(1)(ii)

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

Certification Companion Guide: Direct Project

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is <u>not</u> a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Link to Correction Notice Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
Revised	No	Included	Yes

Certification Requirements

<u>Privacy and Security</u>: This certification criterion was adopted at § 170.315(h)(1). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(h) "paragraph (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) "VDT" and (e)(2) "secure messaging," which are explicitly stated.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify for the criterion using system documentation which provides a clear description of how the external services necessary to meet the P&S criteria would be deployed and used. Please see the 2015 Edition final rule correction notice at 80 FR 76870 for additional clarification.

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

- 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.
- 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.
- 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."

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))
- Transitions of care (§ 170.315(b)(1))

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 XYZ seeks certification to (b)(1) and (h)(1) with its homegrown integrated 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 3rd 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 3rd party HISP. Each developer that would want to work with the 3rd 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)

Technical outcome – The Health IT can electronically transmit (send and receive) health information to a third 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, we have 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)

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

Clarifications:

- The Implementation Guide 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 health information service providers (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).

Content last reviewed on December 6, 2018