

2015 Edition Certification Companion Guide

Data Segmentation for Privacy – receive - 45 CFR 170.315(b)(8)

[Final Rule Preamble](#) – [Test Procedure](#) – [Test Tool](#)

Version 1.0 – Last Updated 12/30/2015

New/Revised/Unchanged Compared to 2014 Edition	Gap Certification Eligible	Base EHR Definition	In Scope for Certified EHR Technology Definition	Associated EHR Incentive Program Objective(s)
New	No	No	No	N/A

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(b)(8). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(b) “paragraph (b)” 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 (b) 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.

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.

- 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.

Privacy and Security (§ 170.315(d))	Design and Performance (§ 170.315(g))
<ul style="list-style-type: none"> • If choosing Approach 1: <ul style="list-style-type: none"> ○ Authentication, access control, and authorization (§ 170.315(d)(1)) ○ Auditable events and tamper-resistance (§ 170.315(d)(2)) ○ Audit reports (§ 170.315(d)(3)) ○ Automatic access time-out (§ 170.315(d)(5)) ○ Emergency access (§ 170.315(d)(6)) ○ End-user device encryption (§ 170.315(d)(7)) ○ Integrity (§ 170.315(d)(8)) • If choosing Approach 2: <ul style="list-style-type: none"> ○ 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. 	<ul style="list-style-type: none"> • Quality management system (§ 170.315(g)(4)) • Accessibility-centered design (§ 170.315(g)(5))

Regulation Text

Data segmentation for privacy – receive. Enable a user to:

- (i) Receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is document-level tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1);
- (ii) Sequester the document-level tagged document from other documents received; and
- (iii) View the restricted document without incorporating any of the data from the document.

Criterion Subparagraph	Technical Explanations and Clarifications	Standard(s) Referenced
(i)	<ul style="list-style-type: none"> Technical outcome – The health IT must be able to receive a summary record (formatted to Consolidated CDA Release 2.1) that is document-level tagged as restricted and subject to re-disclosure restrictions using the HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1. <p>Clarifications:</p> <ul style="list-style-type: none"> The DS4P standard does not have a service discovery mechanism to determine if a potential recipient is able to receive a tagged document. We expect that providers will have to determine the receiving capabilities of their exchange partners, similar to how they have to work with their exchange partners today when they are manually exchanging sensitive health information via fax. [see 80 FR 62648] 	<p>§ 170.205(a)(4) HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015</p> <p>§ 170.205(o)(1) HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1</p>
(ii)	<ul style="list-style-type: none"> Technical outcome – A user must be to separate the document-level tagged document from other documents received. <p>Clarifications:</p> <ul style="list-style-type: none"> “Sequester” in this case means that only authorized users will have the ability to view the document. Once document-level tagged documents are received and stored in the Health IT Module they must only be accessible and viewable by authorized users and separated from other documents. The developer has full design and development discretion to implement a solution which handles this capability properly. Specific functionality other than authorized user access is not required, but if a developer opts to implement a more complex solution than described that is permissible and acceptable. 	N/A
(iii)	<ul style="list-style-type: none"> Technical outcome – A user must be able to view the restricted document without having to incorporate any of the data from the document. <p>Clarifications:</p> <ul style="list-style-type: none"> No additional clarifications available. 	N/A

Note: This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not 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.

Version History

Version #	Change(s) Summary	Date Made
1.0	Initial Publication	Dec 30, 2015