

2015 Edition §170.315(b)(8) Data Segmentation for Privacy - receive				
Testing Components:				
				
Test Procedure Version 1.0 – Last Updated 1/20/16				

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

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

Required Tests

(b)(8) 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);

Standards:

§170.205(o)(1): [Standard. HL7 Implementation Guide: Data Segmentation for Privacy \(DS4P\), Release 1](#) (incorporated by reference in § 170.299).

§170.205(a)(4): [HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1](#)

Criteria ¶	System Under Test	Test Lab Verification
(i)	<p><u>SUT Instruction</u></p> <ol style="list-style-type: none"> Summary records in accordance with the test steps below are provided by the health IT developer and/or the Test Lab for the health IT setting(s) to be certified. The health IT developer identifies the policies associated with the handling of the Data Segmentation for Privacy documents. <p><u>Receive</u></p> <ol style="list-style-type: none"> Using the Health IT Module, a user receives summary record document(s) formatted in accordance with the standard specified at §170.205(a)(4), HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, that is tagged as restricted and subject to restrictions on re-disclosure, according to the standard adopted at §170.205(o)(1), Standard. HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, which includes the following: <ul style="list-style-type: none"> Privacy Segmented Document Template; CDA Mandatory Document Provenance; CDA Mandatory Document Assigned Author Template; and If a document contains information protected by specific privacy policies, the CDA Privacy Markings Section. The document received in step 3 includes the following data elements: <ul style="list-style-type: none"> The originating document Individual Author or Organization; and Confidentiality Code constrained in accordance with the standard specified in §170.205(o)(1). <p style="text-align: right;">Continued on the next page</p> 	<p><u>Test Lab Instruction</u></p> <ol style="list-style-type: none"> The tester creates a human readable version for each of the documents received in steps 3-5 of the SUT to be used for verification. <p><u>Receive</u></p> <ol style="list-style-type: none"> The tester verifies that a Health IT Module can receive a summary record document formatted in accordance with the standard specified at §170.205(a)(4) that is document-level tagged as restricted, and contains restrictions on re-disclosure according to the standard adopted at §170.205(o)(1) for each health IT setting being certified, using Visual Inspection. The tester verifies that a Health IT Module can receive a summary record document formatted in accordance with the standard specified at §170.205(a)(4) that is not document-level tagged as restricted for each health IT setting being certified, using Visual Inspection.

Criteria ¶	System Under Test	Test Lab Verification
(i) continued	5. Using the Health IT Module, a user receives a summary record document(s) formatted in accordance with the standard specified at §170.205(a)(4), HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1 (Without any restrictions).	See previous page

(ii) Sequester the document-level tagged document from other documents received; and

Standards:

§170.205(o)(1): [Standard. HL7 Implementation Guide: Data Segmentation for Privacy \(DS4P\), Release 1](#) (incorporated by reference in § 170.299).

§170.205(a)(4): [HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1](#)

Criteria ¶	System Under Test	Test Lab Verification
(ii)	<ol style="list-style-type: none"> Using the restricted document received in (b)(8)(i), and the Health IT Module, a user demonstrates the ability to associate the restricted document to a patient's record, but sequester it from other health IT developer supplied summary documents formatted in accordance to the standard specified at §170.205(a)(4): HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1 that have been received for that specific patient but are not restricted. Negative Testing: Using the setup from step 1, the user demonstrates that an unauthorized user does not have access to the restricted document received in (b)(8)(i). 	<ol style="list-style-type: none"> The tester verifies that based upon the policies identified in (b)(8)(i), the Health IT Module can sequester a document-level tagged document, formatted in accordance to the standard specified at §170.205(a)(4), with restrictions on re-disclosure according to the standard adopted at §170.205(o)(1) from other summary documents formatted in accordance to the standard specified at §170.205(a)(4) for a specific patient, using Visual Inspection. Negative Testing: The tester verifies that based upon the policies identified in (b)(8)(i), an unauthorized user does not have access to a sequestered document using Visual Inspection.

(iii) View the restricted document without incorporating any of the data from the document.

Standards:

§170.205(o)(1): [Standard. HL7 Implementation Guide: Data Segmentation for Privacy \(DS4P\), Release 1](#)(incorporated by reference in § 170.299).

§170.205(a)(4): [HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1](#)

Criteria ¶	System Under Test	Test Lab Verification
(iii)	<p>Setup</p> <ol style="list-style-type: none"> The Health IT Module creates users on the system that are authorized to review sequestered documentation and users that are not authorized to review sequestered documentation. <p>Viewing</p> <ol style="list-style-type: none"> Using the sequestered document identified in (b)(8)(ii) and the Health IT Module, authorized users view the document data without incorporating the data into the patient’s record as discrete data elements. Negative Testing: The user demonstrates that an unauthorized user cannot view the documents sequestered in (b)(8)(ii). 	<p>Viewing</p> <ol style="list-style-type: none"> The tester verifies that the Health IT Module allows an authorized user to view the data in the restricted document without incorporating it into the patient’s record (e.g. medications, medication allergies, problems) using Visual Inspection. The tester verifies that the Health IT Module view of the document data includes the Data Segmentation for Privacy specific data, and that the data is complete and without omission; including: <ul style="list-style-type: none"> The General Header Author; and If a document contains information protected by specific privacy policies, text indicating the nature of the explicit notice to the provider receiving the disclosed information. If the author of document sections is different then the document author, using the health IT developer-identified health IT function(s), the tester verifies that the Health IT Module provides the correct data provenance. Negative Testing: The tester verifies that the Health IT Module does not allow unauthorized users to access or view restricted data or documents.

Document History

Version Number	Description of Change	Date
1.0	Final Test Procedure	January 20, 2016

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