Security tags - summary of care - receive

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 03-21-2025

Regulation Text

Regulation Text

§ 170.315 (b)(8) *Security tags – summary of care – receive.*

1. Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the document, section, and entry (data element) level; and
2. Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Standard(s) Referenced

Applies to entire criterion

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA Release 2 Consolidation CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1 C-CDA 2.1, August 2015, June 2019 (with Errata)

§ 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(b)(8). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.

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 for Approach 1, the health IT developer may certify for the criterion using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces that enable the Health IT Module 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 Test Procedure	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standards and new SITE UI language. Updated regulatory language to reflect changes in HTI-2 Final Rule.	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (b)(8) *Security tags – summary of care – receive.*

1. Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the document, section, and entry (data element) level; and
2. Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Standard(s) Referenced

Applies to entire criterion

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA Release 2 Consolidation CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1 C-CDA 2.1, August 2015, June 2019 (with Errata)

§ 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

Privacy & Security Requirements
This certification criterion was adopted at § 170.315(b)(8). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.

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

- 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))
  - 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))
  - Encrypt user credentials (§ 170.315(d)(12))
  - Multi-factor authentication (§ 170.315(d)(13))
- If choosing Approach 2:

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

Testing

Testing Tool

Standards Implementation & Testing Environment (SITE): C-CDA Validators

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(b)(8)(i)	Inpatient setting: 170.315_b8_ds4p_inp_sample1*.xml Ambulatory setting: 170.315_b8_ds4p_amb_sample1*.xml

Revision History

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

Version #	Description of Change	Version Date
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standards and new SITE UI language. Updated regulatory language to reflect changes in HTI-2 Final Rule.	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 tests step order does not necessarily prescribe the order in which the tests should take place.

Testing components

ONC
Supplied
Test
Data

SVAP

Paragraph (b)(8)(i) Security Tags document, section and entry (data element) level

System Under Test

System Under Test Instruction

1. Summary records in accordance with the test steps below, based on the health IT setting(s), are provided by the ASTP Standards Implementation & Testing Environment (SITE): C-CDA Validator under the “Receiver” system.
2. The health IT developer identifies the policies associated with the handling of the DS4P documents.

<u>Receive</u>

3. 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, DSTU 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) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, which includes the following:
    - Privacy Segmented Document Template;
    - Clinical Document Architecture (CDA) Mandatory Document Provenance;
    - CDA Mandatory Document Assigned Author Template;
    - If a document contains information protected by specific privacy policies, the CDA Privacy Markings Section and Privacy Marking Entry(ies);
    - Privacy Segmented Section Template(s); Privacy Annotation Template; and
    - Protected Problem Template.
4. The received Consolidated- Clinical Document Architecture (C- CDA) tagged as restricted document received in step 3, includes the following data elements:
    - The originating document Individual Author or Organization; and
    - Confidentiality Code constrained in accordance with the standard specified in § 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.
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, DSTU Release 2.1, without any restrictions.

All Steps (Approved SVAP Version)

- Complete steps above using SITE: C-CDA Validator for USCDI v4 and;
- Use HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024 for § 170.205(a)(4), (a)(5) or (a)(6).

Test Lab Verification

<u>Test Lab Instruction</u>

1. The tester creates a human-readable version for each of the documents received in steps 3-5, of the System Under Test to be used for verification.

2. The tester verifies the health IT developer has provided identification of the policies associated with the handling of the DS4P documents.

Receive

3. The tester verifies 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 section-level and entry-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 of the following:
    - Privacy Segmented Document Template;
    - CDA Mandatory Document Provenance;
    - CDA Mandatory Document Assigned Author Template;
    - If a document contains information protected by specific privacy policies, the CDA Privacy Markings Section and Privacy Marking Entry(ies);
    - Privacy Segmented Section Template(s);Privacy Annotation Template; and
    - Protected Problem Template.
4. The tester verifies the document received includes the following data elements:
    - The originating document Individual Author or Organization; and
    - Confidentiality Code constrained in accordance with the standard specified in § 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.
5. The tester verifies 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.

System Under Test

System Under Test Instruction

1. Summary records in accordance with the test steps below, based on the health IT setting(s), are provided by the ASTP Standards Implementation & Testing Environment (SITE): C-CDA Validator under the “Receiver” system.
2. The health IT developer identifies the policies associated with the handling of the DS4P documents.

Receive

Test Lab Verification

Test Lab Instruction

1. The tester creates a human-readable version for each of the documents received in steps 3-5, of the System Under Test to be used for verification.
2. The tester verifies the health IT developer has provided identification of the policies associated with the handling of the DS4P documents.

Receive

System Under Test

3. 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, DSTU 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) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, which includes the following:
    - Privacy Segmented Document Template;
    - Clinical Document Architecture (CDA) Mandatory Document Provenance;
    - CDA Mandatory Document Assigned Author Template;
    - If a document contains information protected by specific privacy policies, the CDA Privacy Markings Section and Privacy Marking Entry(ies);
    - Privacy Segmented Section Template(s); Privacy Annotation Template; and
    - Protected Problem Template.
4. The received Consolidated- Clinical Document Architecture (C- CDA) tagged as restricted document received in step 3, includes the following data elements:
    - The originating document Individual Author or Organization; and
    - Confidentiality Code constrained in accordance with the standard specified in § 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.
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, DSTU Release 2.1, without any restrictions.

Test Lab Verification

3. The tester verifies 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 section-level and entry-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 of the following:
    - Privacy Segmented Document Template;
    - CDA Mandatory Document Provenance;
    - CDA Mandatory Document Assigned Author Template;
    - If a document contains information protected by specific privacy policies, the CDA Privacy Markings Section and Privacy Marking Entry(ies);
    - Privacy Segmented Section Template(s);Privacy Annotation Template; and
    - Protected Problem Template.
4. The tester verifies the document received includes the following data elements:
    - The originating document Individual Author or Organization; and
    - Confidentiality Code constrained in accordance with the standard specified in § 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

All Steps (Approved SVAP Version)

System Under Test

- Complete steps above using SITE: C-CDA Validator for USCDI v4 and;
- Use HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024 for § 170.205(a)(4), (a)(5) or (a)(6).

Test Lab Verification

5. The tester verifies 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.

Paragraph (b)(8)(ii) Preserve privacy markings

System Under Test

1. The health IT developer attests that privacy markings are preserved by the Health IT Module to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Test Lab Verification

1. The tester verifies the health IT developer attests that the Health IT Module preserves privacy markings to ensure fidelity to the tagged based on consent and with respect to sharing and re-disclosure restrictions.

System Under Test

1. The health IT developer attests that privacy markings are preserved by the Health IT Module to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Test Lab Verification

1. The tester verifies the health IT developer attests that the Health IT Module preserves privacy markings to ensure fidelity to the tagged based on consent and with respect to sharing and re-disclosure restrictions.

Archived Version:

§ 170.315(b)(8) Data segmentation for privacy - receive TP

Updated on 08-19-2024

Regulation Text

Regulation Text

§ 170.315 (b)(8) *Security tags – summary of care – receive.*

1. Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the document, section, and entry (data element) level; and
2. Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Standard(s) Referenced

Applies to entire criterion

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA Release 2 Consolidation CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1 C-CDA 2.1, August 2015, June 2019 (with Errata)

§ 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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 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, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.

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

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(b)(8). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.

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

- 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))
    - 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))
    - Encrypt user credentials (§ 170.315(d)(12))
    - Multi-factor authentication (§ 170.315(d)(13))

- If choosing Approach 2:

  For each applicable privacy and security certification criterion not certified for Approach 1, the health IT developer may certify for the criterion using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces that enable the Health IT Module 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 Test Procedure	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standards and new SITE UI language. Updated regulatory language to reflect changes in HTI-2 Final Rule.	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (b)(8) *Security tags – summary of care – receive.*

1. Enable a user to receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) that is tagged as restricted and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1) at the document, section, and entry (data element) level; and
2. Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Standard(s) Referenced

Applies to entire criterion

§ 170.205(a)(4) Health Level 7 (HL7®) Implementation Guide for CDA Release 2 Consolidation CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1 C-CDA 2.1, August 2015, June 2019 (with Errata)

§ 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

Privacy & Security Requirements
This certification criterion was adopted at § 170.315(b)(8). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.

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 for Approach 1, the health IT developer may certify for the criterion using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces that enable the Health IT Module 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	Standards Referenced updated to reflect 2024 Approved SVAP Standards	08-19-2024

Testing

Testing Tool

Standards Implementation & Testing Environment (SITE): C-CDA Validators

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(b)(8)(i)	Inpatient setting: 170.315_b8_ds4p_inp_sample1*.xml Ambulatory setting: 170.315_b8_ds4p_amb_sample1*.xml

Certification Companion Guide: Security tags - summary of care - receive

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

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

Base EHR Definition	Real World Testing	Insights Condition	SVAP	Requires Updates
Not Included	Yes	No	Yes	No

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

No additional clarifications.

Clarifications:

No additional clarifications.

Paragraph (b)(8)(i) Enable a user to receive a summary record

Technical outcome - The health IT must be able to receive a summary record (formatted to Consolidated CDA (C-CDA) Release 2.1) that is document, section, and entry level tagged as restricted and subject to re-disclosure restrictions using the HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

Clarifications:

- The DS4P standard does not have a service discovery mechanism to determine if a potential recipient is able to receive a tagged document. ONC expects that providers will have to determine the receiving capabilities of their exchange partners. This is similar to how providers have to work with their exchange partners today when manually exchanging sensitive health information via fax. [see 80 FR 62648]
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see the Health IT Certification Program Overview] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There is a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., Edge Testing Tool: Message Validators). Similarly, there will be an 18-month delay before a finding of a correction’s absence in certified health IT during surveillance would constitute a non-conformity under the Certification Program.

Technical outcome - The health IT must be able to receive a summary record (formatted to Consolidated CDA (C-CDA) Release 2.1) that is document, section, and entry level tagged as restricted and subject to re-disclosure restrictions using the HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

Clarifications:

- The DS4P standard does not have a service discovery mechanism to determine if a potential recipient is able to receive a tagged document. ONC expects that providers will have to determine the receiving capabilities of their exchange partners. This is similar to how providers have to work with their exchange partners today when manually exchanging sensitive health information via fax. [see 80 FR 62648]
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see the Health IT Certification Program Overview] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There is a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., Edge Testing Tool: Message Validators). Similarly, there will be an 18-month delay before a finding of a correction’s absence in certified health IT during surveillance would constitute a non-conformity under the Certification Program.

Paragraph (b)(8)(ii) Privacy markings

Technical outcome – The privacy markings must be preserved to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Clarifications:

No additional clarifications.

Technical outcome – The privacy markings must be preserved to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Clarifications:

No additional clarifications.

Archived Version:
§ 170.315(b)(8) Data segmentation for privacy - receive CCG