Security tags - summary of care - send

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 03-21-2025

Regulation Text

Regulation Text

§ 170.315 (b)(7) *Security tags - summary of care – send*.

Enable a user to create a summary record 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.

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 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, 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)(7). 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 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	Final Test Procedure.	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standard and new SITE UI language. Updated regulatory language to reflect edits from HTI-2 Final Rule.	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (b)(7) *Security tags - summary of care – send*.

Enable a user to create a summary record 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.

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 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, 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)(7). 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 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)(7)	Inpatient setting: 170.315_b7_ds4p_imp_sample1_*.pdf Ambulatory setting: 170.315_b7_ds4p_amb_sample1_*.pdf

Revision History

Version #	Description of Change	Version Date
1.0	Final 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 standard and new SITE UI language. Updated regulatory language to reflect edits from 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

Paragraph (b)(7)

System Under Test

1. Using the ASTP Standards Implementation & Testing Environment (SITE): C-CDA Validator, the health IT developer downloads the ASTP/ONC-supplied data instructions through the sender download selections of the "170.315_b7_DS4P Amb" or "170.315_b7_DS4P_Inp" criteria and one of the DS4P instruction documents and executes the download.
2. Using the ASTP/ONC-supplied DS4P instruction document(s) the user enters the information as appropriate into the Health IT Module including the DS4P tags and notices.
3. The user will generate a summary record document(s) from the Health IT Module and submit the document(s) to the tester for verification. The generated summary record includes the following data elements:
    - Document Level Confidentiality Code, constrained in accordance with the standard specified in § 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1;
    - Document Level Author Element;
    - Document Level Provenance Element;
    - Privacy and Security Markings Section with Re-disclosure Notice;
    - Privacy Segmented Section(s);
    - Privacy Markings Entry(ies); and
    - Mandatory Entry Provenance Element(s).
4. A summary record document created by the Health IT Module must be submitted for each health IT setting being certified.

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

1. The tester verifies the health IT developer can download the ASTP/ONC-supplied instruction document for the summary of care with security tags.
2. The tester verifies the user can enter all of the summary of care with the required security tags as outlined in the ASTP/ONC-supplied Security tags – summary of care instruction document returned in step 1.

3. Using SITE: C-CDA Validator, the tester uploads the submitted summary record(s) with restrictions (xml file) from step 4, of the System Under Test, through the sender upload selection of the “Data Segmentation for Privacy – send – Ambulatory” or “Data Segmentation for Privacy – send – Inpatient” criteria and executes the upload of the submitted file(s) to SITE: C-CDA Validator. The tester uses the validation report(s) created by SITE: C-CDA Validator to verify the Health IT Module passes without error in order to confirm that the document is conformant to each of the standards adopted in § 170.205(a)(4). Using SITE: C-CDA Validator Message Content Report, the tester verifies that:
    - If the summary record(s) submitted includes unstructured text data elements, the tester uses the ASTP/ONC-supplied data instructions and the Message Content Report to verify the additional checks for equivalent text for the content of all section level narrative text;
    - The summary record(s) submitted is accurate and without omission using the ASTP/ONC-supplied data instructions; and
    - The summary record(s) indicates that the document(s) is restricted and subject to restrictions on re-disclosure. The resulting document retains these tags according to the standard adopted at § 170.205(o)(1):
        - Privacy Segmented Document Template;
        - Privacy Segmented Section Template(s);
        - Privacy Markings Entry Template(s);
        - Clinical Document Architecture (CDA) Mandatory Document Provenance;
        - Mandatory Entry Provenance Template(s);
        - CDA Mandatory Document Assigned Author Template;
        - If a document, section or entry contains information protected by specific privacy policies, CDA Privacy Markings Section with text indicating the nature of the explicit notice to the provider receiving the disclosed information;
        - If the metadata for a section is different than the overall document, the confidentiality levels and provenance information should be maintained; and
        - A Confidentiality Code with the value “R.”
4. For each of the health IT setting(s) to be certified, the tester repeats steps 2-3.

System Under Test	Test Lab Verification
1. Using the ASTP Standards Implementation & Testing Environment (SITE): C-CDA Validator, the health IT developer downloads the ASTP/ONC-supplied data instructions through	1. The tester verifies the health IT developer can download the ASTP/ONC-supplied instruction document for the summary of care with security tags. 2. The tester verifies the user can enter all of the summary of care with the required security tags as outlined in the ASTP/ONC-supplied Security tags – summary of care instruction document returned in step 1.

System Under Test	Test Lab Verification
the sender download selections of the "170.315_b7_DS4P Amb" or "170.315_b7_DS4P_Inp" criteria and one of the DS4P instruction documents and executes the download. 2. Using the ASTP/ONC-supplied DS4P instruction document(s) the user enters the information as appropriate into the Health IT Module including the DS4P tags and notices.	3. Using SITE: C-CDA Validator, the tester uploads the submitted summary record(s) with restrictions (xml file) from step 4, of the System Under Test, through the sender upload selection of the "Data Segmentation for Privacy – send – Ambulatory" or "Data Segmentation for Privacy – send – Inpatient" criteria and executes the upload of the submitted file(s) to SITE: C-CDA Validator. The tester uses the validation report(s) created by SITE: C-CDA Validator to verify the Health IT Module passes without error in order to confirm that the document is conformant to each of the standards adopted in § 170.205(a)(4). Using SITE: C-CDA Validator Message Content Report, the tester verifies that: ◦ If the summary record(s) submitted includes unstructured text data elements, the tester uses the ASTP/ONC-supplied data instructions and the Message Content Report to verify the additional checks for equivalent text for the content of all section level narrative text; ◦ The summary record(s) submitted is accurate and without omission using the ASTP/ONC-supplied data instructions; and

System Under Test

3. The user will generate a summary record document(s) from the Health IT Module and submit the document(s) to the tester for verification. The generated summary record includes the following data elements:
    - Document Level Confidentiality Code, constrained in accordance with the standard specified in § 170.205(o)(1) HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1;
    - Document Level Author Element;
    - Document Level Provenance Element;
    - Privacy and Security Markings Section with Re-disclosure Notice;
    - Privacy Segmented Section(s);
    - Privacy Markings Entry(ies); and
    - Mandatory Entry Provenance Element(s).
4. A summary record document created by the Health IT Module must be submitted for each health IT setting being certified.

All Steps (Approved SVAP Version)

Test Lab Verification

    - The summary record(s) indicates that the document(s) is restricted and subject to restrictions on re-disclosure. The resulting document retains these tags according to the standard adopted at § 170.205(o)(1):
        - Privacy Segmented Document Template;
        - Privacy Segmented Section Template(s);
        - Privacy Markings Entry Template(s);
        - Clinical Document Architecture (CDA) Mandatory Document Provenance;
        - Mandatory Entry Provenance Template(s);
        - CDA Mandatory Document Assigned Author Template;
        - If a document, section or entry contains information protected by specific privacy policies, CDA Privacy Markings Section with text indicating the nature of the explicit notice to the provider receiving the disclosed information;
        - If the metadata for a section is different than the overall document, the confidentiality levels and provenance information should be maintained; and
        - A Confidentiality Code with the value “R.”
4. For each of the health IT setting(s) to be certified, the tester repeats steps 2-3.

System Under Test	Test Lab Verification
• 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).	

Archived Version:
§ 170.315(b)(7) Data segmentation for privacy - send TP

Updated on 08-19-2024

Regulation Text

Regulation Text

§ 170.315 (b)(7) *Security tags - summary of care – send*.

Enable a user to create a summary record 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.

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 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, 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)(7). 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 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	Final Test Procedure.	03-11-2024
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standard and new SITE UI language. Updated regulatory language to reflect edits from HTI-2 Final Rule.	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (b)(7) *Security tags - summary of care – send*.

Enable a user to create a summary record 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.

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 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, 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)(7). 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 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

Criterion Subparagraph	Test Data
(b)(7)	Inpatient setting: 170.315_b7_ds4p_imp_sample1_*.pdf Ambulatory setting: 170.315_b7_ds4p_amb_sample1_*.pdf

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

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

Technical outcome – The Health IT Module can create a summary record (formatted to Consolidated Clinical Document Architecture (C-CDA) Release 2.1) that is tagged at the document, section, and entry level as restricted and subject to re-disclosure restrictions using the HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

Clarifications:

- This certification criterion in § 170.315(b)(7) focuses on a Health IT Module's ability to tag a C-CDA document as restricted and subject to re-disclosure restrictions using the HL7® DS4P standard, not on the content of the C-CDA document. As such, this certification criterion is not subject to the Consolidated CDA creation performance certification criterion (§ 170.315(g)(6)) because testing for § 170.315(g)(6) focuses on the content of the C-CDA document. We established a certification criterion for Consolidated CDA creation performance to promote the interoperability of C-CDA documents during exchange by testing conformance of the C-CDA's content to the variation permitted by the HL7® standard. [see also 80 FR 16859]
- 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 Module can create a summary record (formatted to Consolidated Clinical Document Architecture (C-CDA) Release 2.1) that is tagged at the document, section, and entry level as restricted and subject to re-disclosure restrictions using the HL7® Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1.

Clarifications:

- This certification criterion in § 170.315(b)(7) focuses on a Health IT Module's ability to tag a C-CDA document as restricted and subject to re-disclosure restrictions using the HL7® DS4P standard, not on the content of the C-CDA document. As such, this certification criterion is not subject to the Consolidated CDA creation performance certification criterion (§ 170.315(g)(6)) because testing for § 170.315(g)(6) focuses on the content of the C-CDA document. We established a certification criterion for Consolidated CDA creation performance to promote the interoperability of C-CDA documents during exchange by testing conformance of the C-CDA's content to the variation permitted by the HL7® standard. [see also 80 FR 16859]
- 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.

Archived Version:

§ 170.315(b)(7) Data segmentation for privacy - send CCG