Transmission to cancer registries | HealthIT.gov

healthit.gov/test-method/transmission-cancer-registries

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 05-16-2024

Regulation Text

Regulation Text

§ 170.315 (f)(4) *Transmission to cancer registries—*

Create cancer case information for electronic transmission in accordance with:

1. The standard (and applicable implementation specifications) specified in § 170.205(i)(2).
2. At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

Standard(s) Referenced

Paragraph (f)(4)(i)

§ 170.205(i)(2) Health Level 7 (HL7®) Implementation Guide for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1, April 2015

Paragraph (f)(4)(ii)

§ 170.207(a)(4) International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), U.S. Edition, September 2015 Release (Adoption of this standard expires on January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release (This standard is required by December 31, 2025)

§ 170.207(c)(3) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, Released June 2015, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (Adoption of this standard expires on January 1, 2026)

§ 170.207(c)(1) Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, February 16, 2022, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (This standard is required by December 31, 2025)

Required Update Deadlines

The following outlines deadlines for required updates for this criterion as they relate to changes published in recent ONC final rules. Developers must update their products to the requirements outlined and provide them to their customers by the stated deadlines. These represent one-time deadlines as set by recent regulatory updates and do not encompass ongoing deadlines related to the Conditions and Maintenance of Certification. Please review those requirements for additional compliance activities related to one's certification under Certification Dependencies.

Deadline: December 31, 2025

Action to be taken: Developers certified to this criterion must utilize updated code sets to reflect, at a minimum, the code sets outlined in subparagraph 170.315(f)(4)(ii).

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, the QMS' need to be 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(f)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(f) 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 (f) 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.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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 the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* 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	Added conditional test step for Modules with existing certification to (f)(4).	05-16-2024

Regulation Text

Regulation Text

§ 170.315 (f)(4) *Transmission to cancer registries—*

Create cancer case information for electronic transmission in accordance with:

1. The standard (and applicable implementation specifications) specified in § 170.205(i)(2).
2. At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

Standard(s) Referenced

Paragraph (f)(4)(i)

§ 170.205(i)(2) Health Level 7 (HL7®) Implementation Guide for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1, April 2015

Paragraph (f)(4)(ii)

§ 170.207(a)(4) International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), U.S. Edition, September 2015 Release (Adoption of this standard expires on January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release (This standard is required by December 31, 2025)

§ 170.207(c)(3) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, Released June 2015, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (Adoption of this standard expires on January 1, 2026)

§ 170.207(c)(1) Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, February 16, 2022, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (This standard is required by December 31, 2025)

Required Update Deadlines

The following outlines deadlines for required updates for this criterion as they relate to changes published in recent ONC final rules. Developers must update their products to the requirements outlined and provide them to their customers by the stated deadlines. These represent one-time deadlines as set by recent regulatory updates and do not encompass ongoing deadlines related to the Conditions and Maintenance of Certification. Please review those requirements for additional compliance activities related to one's certification under Certification Dependencies.

Deadline: December 31, 2025

Action to be taken: Developers certified to this criterion must utilize updated code sets to reflect, at a minimum, the code sets outlined in subparagraph 170.315(f)(4)(ii).

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, the QMS' need to be 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(f)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(f) 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 (f) 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.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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))
  - End-user device encryption (§ 170.315(d)(7))
  - Encrypt authentication credentials (§ 170.315(d)(12))
  - Multi-factor authentication (MFA) (§ 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 the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Testing

Testing Tool

NIST HL7® CDA Cancer Registry Reporting Validation Tool

Criterion Subparagraph	Test Data
(f)(4)(i)	Refer to NIST HL7® CDA Cancer Registry Reporting Validation Tool

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Added conditional test step for Modules with existing certification to (f)(4).	05-16-2024

This Test Procedure illustrates the test steps required to certify a Health IT Module to this criterion. Please consult the most recent ONC Final Rule on the Certification Regulations page for a detailed description of the certification criterion with which these testing steps are

associated. 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 test step order does not necessarily prescribe the order in which the tests should take place.

Testing components

Paragraph (f)(4) – (Conditional – For Modules with existing certification to (f)(4))

System Under Test

Required by December 31, 2025

1. The health IT developer of a Health IT Module currently certified to the 170.315(f)(4) Transmission to cancer registries will attest directly to the ONC-ACB to conformance with the updated 170.315(f)(4) requirements outlined in the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule.

Test Lab Verification

Required by December 31, 2025

1. The ONC-ACB verifies the health IT developer of a Health IT Module certified to the 170.315(f)(4) Transmission to cancer registries attests conformance to updated 170.315(f)(4) criteria requirements.

System Under Test	Test Lab Verification
Required by December 31, 2025 1. The health IT developer of a Health IT Module currently certified to the 170.315(f)(4) Transmission to cancer registries will attest directly to the ONC-ACB to conformance with the updated 170.315(f)(4) requirements outlined in the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule.	**Required by December 31, 2025** 1. The ONC-ACB verifies the health IT developer of a Health IT Module certified to the 170.315(f)(4) Transmission to cancer registries attests conformance to updated 170.315(f)(4) criteria requirements.

Paragraph (f)(4)(i) Create cancer case information based on CDA R2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, R1.1

System Under Test

1. The user enters the cancer information for each of the test cases referenced from the Home Tab of the CRV. All test cases are required. Note that health IT developers should select the appropriate test case for Test Case 1, based on their module's capability.
2. The Health IT Module creates a cancer case document based on the standard specified in § 170.205(i)(2) HL7® Implementation Guide for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1.1 for each test case as outlined below:

Modules that collect radiation treatment data:

Test_Case_1a_Complete_Record_With_Radiation

Modules that do not collect radiation treatment data:

Test_Case_1b_Complete_Record_Without_Radiation

ALL Health IT Modules :

- Test_Case_2_Cancer_Diagnosis_With_No_Treatment
- Test_Case_3_Two_Cancer_Diagnoses
- Test_Case_4_Two_Cancer_Diagnoses_Update
- Test_Case_5_Non-reportable

Test Lab Verification

1. The tester verifies that the Health IT Module includes the source cancer information correctly and without omission through visual inspection, using the test data associated with the selected test case.
2. The tester imports the cancer reports into the test tool for validation based on each test case listed, and uses the Validation Report produced by the test tool to verify the report indicates passing without error to confirm that the cancer report is conformant to the standard specified in § 170.205(i)(2).
3. The tester verifies that the Health IT Module's supplied cancer document in step 2, is accurate and without omission using the Context-based Validation Report, the Juror Document, and through additional visual inspection, checking for equivalent text for:
    1. content for all section level narrative text; and
    2. display names: if the context-based validation indicates a mismatch, equivalent entries are allowable.
4. Negative Test: For Test_Case_5_Non-reportable, the tester verifies using Documentation that the non-reportable test case does not generate a CDA report.

System Under Test	Test Lab Verification
1. The user enters the cancer information for each of the test cases referenced from the Home Tab of the CRV. All test cases are required. Note that health IT developers should select the appropriate test case for Test Case 1, based on their module's capability. 2. The Health IT Module creates a cancer case document based on the standard specified in § 170.205(i)(2) HL7® Implementation Guide for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1.1 for each test case as outlined below:	1. The tester verifies that the Health IT Module includes the source cancer information correctly and without omission through visual inspection, using the test data associated with the selected test case.

Modules that collect radiation treatment data:

Test_Case_1a_Complete_Record_With_Radiation

Modules that do not collect radiation treatment data:

Test_Case_1b_Complete_Record_Without_Radiation

ALL Health IT Modules :

- Test_Case_2_Cancer_Diagnosis_With_No_Treatment

System Under Test

- Test_Case_3_Two_Cancer_Diagnoses
- Test_Case_4_Two_Cancer_Diagnoses_Update
- Test_Case_5_Non-reportable

Test Lab Verification

2. The tester imports the cancer reports into the test tool for validation based on each test case listed, and uses the Validation Report produced by the test tool to verify the report indicates passing without error to confirm that the cancer report is conformant to the standard specified in § 170.205(i)(2).
3. The tester verifies that the Health IT Module's supplied cancer document in step 2, is accurate and without omission using the Context-based Validation Report, the Juror Document, and through additional visual inspection, checking for equivalent text for:
    1. content for all section level narrative text; and
    2. display names: if the context-based validation indicates a mismatch, equivalent entries are allowable.
4. Negative Test: For Test_Case_5_Non-reportable, the tester verifies using Documentation that the non-reportable test case does not generate a CDA report.

Paragraph (f)(4)(ii) Create cancer case information in accordance with SNOMED CT® and LOINC®

System Under Test

Expires on January 1, 2026
The cancer case information is in accordance with § 170.207(a)(4) SNOMED CT® and § 170.207(c)(3) LOINC®.

Required by December 31, 2025
The cancer case information is in accordance with § 170.207(a)(1) SNOMED CT® and § 170.207(c)(1) LOINC®.

Test Lab Verification

Expires on January 1, 2026
The tester uses visual inspection of the Health IT Module configuration file or Documentation to verify cancer case information are represented using the named § 170.207(a)(4) standard and the named § 170.207(c)(3) standard.

Required by December 31, 2025
The tester uses visual inspection of the Health IT Module configuration file or Documentation to verify cancer case information are represented using the named § 170.207(a)(1) standard and the named § 170.207(c)(1) standard.

System Under Test	Test Lab Verification
Expires on January 1, 2026 The cancer case information is in accordance with § 170.207(a)(4) SNOMED CT® and § 170.207(c)(3) LOINC®. **Required by December 31, 2025** The cancer case information is in accordance with § 170.207(a)(1) SNOMED CT® and § 170.207(c)(1) LOINC®.	**Expires on January 1, 2026** The tester uses visual inspection of the Health IT Module configuration file or Documentation to verify cancer case information are represented using the named § 170.207(a)(4) standard and the named § 170.207(c)(3) standard. **Required by December 31, 2025** The tester uses visual inspection of the Health IT Module configuration file or Documentation to verify cancer case information are represented using the named § 170.207(a)(1) standard and the named § 170.207(c)(1) standard.

Updated on 08-19-2024

Regulation Text

Regulation Text

§ 170.315 (f)(4) *Transmission to cancer registries—*

Create cancer case information for electronic transmission in accordance with:

1. The standard (and applicable implementation specifications) specified in § 170.205(i)(2).
2. At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

Standard(s) Referenced

Paragraph (f)(4)(i)

§ 170.205(i)(2) Health Level 7 (HL7®) Implementation Guide for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1, April 2015

Paragraph (f)(4)(ii)

§ 170.207(a)(4) International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), U.S. Edition, September 2015 Release (Adoption of this standard expires on January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release (This standard is required by December 31, 2025)

§ 170.207(c)(3) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, Released June 2015, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (Adoption of this standard expires on January 1, 2026)

§ 170.207(c)(1) Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, February 16, 2022, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (This standard is required by December 31, 2025)

Required Update Deadlines

The following outlines deadlines for required updates for this criterion as they relate to changes published in recent ONC final rules. Developers must update their products to the requirements outlined and provide them to their customers by the stated deadlines. These represent one-time deadlines as set by recent regulatory updates and do not encompass

ongoing deadlines related to the Conditions and Maintenance of Certification. Please review those requirements for additional compliance activities related to one's certification under Certification Dependencies.

Deadline: December 31, 2025

Action to be taken: Developers certified to this criterion must utilize updated code sets to reflect, at a minimum, the code sets outlined in subparagraph 170.315(f)(4)(ii).

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, the QMS' need to be 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(f)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(f) 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 (f) 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.

- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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))
  - End-user device encryption (§ 170.315(d)(7))
  - Encrypt authentication credentials (§ 170.315(d)(12))
  - Multi-factor authentication (MFA) (§ 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 the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* 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	Added conditional test step for Modules with existing certification to (f)(4).	05-16-2024

Regulation Text

Regulation Text

§ 170.315 (f)(4) *Transmission to cancer registries—*

Create cancer case information for electronic transmission in accordance with:

1. The standard (and applicable implementation specifications) specified in § 170.205(i)(2).
2. At a minimum, the versions of the standards specified in § 170.207(a)(1) and (c)(1).

Standard(s) Referenced

Paragraph (f)(4)(i)

§ 170.205(i)(2) Health Level 7 (HL7®) Implementation Guide for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1, April 2015

Paragraph (f)(4)(ii)

§ 170.207(a)(4) International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®), U.S. Edition, September 2015 Release (Adoption of this standard expires on January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release (This standard is required by December 31, 2025)

§ 170.207(c)(3) Logical Observation Identifiers Names and Codes (LOINC®) Database version 2.52, Released June 2015, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (Adoption of this standard expires on January 1, 2026)

§ 170.207(c)(1) Logical Observation Identifiers Names and Codes (LOINC®) Database Version 2.72, February 16, 2022, a universal code system for identifying laboratory and clinical observations produced by the Regenstrief Institute, Inc. (This standard is required by December 31, 2025)

Required Update Deadlines

The following outlines deadlines for required updates for this criterion as they relate to changes published in recent ONC final rules. Developers must update their products to the requirements outlined and provide them to their customers by the stated deadlines. These represent one-time deadlines as set by recent regulatory updates and do not encompass ongoing deadlines related to the Conditions and Maintenance of Certification. Please review those requirements for additional compliance activities related to one's certification under Certification Dependencies.

Deadline: December 31, 2025

Action to be taken: Developers certified to this criterion must utilize updated code sets to reflect, at a minimum, the code sets outlined in subparagraph 170.315(f)(4)(ii).

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, the QMS' need to be 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(f)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(f) 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 (f) 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.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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 the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* 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	Removed a typo in the Required Update Deadlines section to indicate updates must be made for all Health IT Modules certified to this criterion.	04-25-2024
1.2	Updated standard referenced at § 170.207(c)(1) from version 2.76 to version 2.72 to align with regulation.	08-14-2024
1.3	Standards Referenced updated to reflect 2024 Approved SVAP Standards	08-19-2024

Testing

Testing Tool

NIST HL7® CDA Cancer Registry Reporting Validation Tool

Criterion Subparagraph	Test Data
(f)(4)(i)	Refer to NIST HL7® CDA Cancer Registry Reporting Validation Tool

Certification Companion Guide: Transmission to cancer registries

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	No	Yes

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- For the public health certification criteria in § 170.315(f), health IT will only need to be certified to those criteria that are required to meet the measures the provider intends to report on to meet Objective 8: Public Health and Clinical Data Registry Reporting.
- This certification criterion is intended for technology designed for the ambulatory setting.
- We have not adopted a "cancer case information" certification criterion. This decision has no impact on the requirements of the "transmission to cancer registries" certification criterion or the requirements of the Implementation Guide (IG). Certification to the "Transmission to cancer registries" criterion requires a Health IT Module to demonstrate that it can create a file with the necessary cancer case information in accordance with the IG. [see also 80 FR 62667]
- "Cancer case information" is synonymous with the "cancer event reports" or "cancer reports" referred to in the HL7® IG for CDA Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, DSTU Release 1.1.

Clarifications:

- For the public health certification criteria in § 170.315(f), health IT will only need to be certified to those criteria that are required to meet the measures the provider intends to report on to meet Objective 8: Public Health and Clinical Data Registry Reporting.
- This certification criterion is intended for technology designed for the ambulatory setting.
- We have not adopted a "cancer case information" certification criterion. This decision has no impact on the requirements of the "transmission to cancer registries" certification criterion or the requirements of the Implementation Guide (IG). Certification to the "Transmission to cancer registries" criterion requires a Health IT Module to demonstrate that it can create a file with the necessary cancer case information in accordance with the IG. [see also 80 FR 62667]
- "Cancer case information" is synonymous with the "cancer event reports" or "cancer reports" referred to in the HL7® IG for CDA Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, DSTU Release 1.1.

Paragraph (f)(4)(i) Create cancer case information based on CDA® R2: Reporting to Public Health Cancer Registries from Ambulatory Care Providers, R1.1

Technical outcome – The health IT can create cancer case information for electronic transmission in accordance with the HL7® IG for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, DSTU Release 1.1.

Clarifications:

- The CDC published an updated version of the Implementation Guide for reporting to cancer registries (HL7® IG for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1, U.S. Realm ("Release 1.1.")). Release 1.1 involves technical corrections to Release 1. No new content has been included. ONC refers developers to the DSTU Release 1.1 for a full list of the updates. [see also 80 FR 62666]

- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® CDA® Release 2 IG: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1 – US Realm, ONC assesses, approves, and incorporates corrections (Errata) as part of required testing and certification to this criterion. Compliance with the following corrections is 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. 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.

    Version: HL7® IG for CDA© Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1, October 2017. Effective for testing on February 04, 2021. Surveillance compliance date on May 06, 2022.
- Mapping to the North American Association of Central Cancer Registries (NAACCR) format is not included in the IG because the mapping rules are complex and can change over time based on continued input and refinement by the cancer registry community. It is ONC's understanding that the CDC will work closely with the cancer registry community to develop mapping rules for the IG and will incorporate the rules into the software tools CDC provides state cancer registries. In regard to concerns expressed about jurisdictional variations, all public health jurisdictions have adopted the HL7® IG Release 1 for cancer reporting and will be moving to the updated version published by the CDC. [see also 80 FR 62666]
- The CDC National Program of Cancer Registries (NCPR), and the North American Association of Central Cancer Registries (NAACCR), no longer require state cancer registries to collect "Stager Clinical Cancer" and "Stager Pathologic Cancer" (also referred to as "Staged By") data elements for cases diagnosed in 2018 or later. For testing of this criterion, ONC will allow for any valid value in the specified value set to be provided for the "Stager Clinical Cancer" and "Stager Pathologic Cancer" elements.

Technical outcome – The health IT can create cancer case information for electronic transmission in accordance with the HL7® IG for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, DSTU Release 1.1.

Clarifications:

- The CDC published an updated version of the Implementation Guide for reporting to cancer registries (HL7® IG for CDA® Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1; DSTU Release 1.1, U.S. Realm ("Release 1.1.")). Release 1.1 involves technical corrections to Release 1. No new content has been included. ONC refers developers to the DSTU Release 1.1 for a full list of the updates. [see also 80 FR 62666]
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® CDA® Release 2 IG: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1 – US Realm, ONC assesses, approves, and incorporates corrections (Errata) as part of required testing and certification to this criterion. Compliance with the following corrections is 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. 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.

  Version: HL7® IG for CDA© Release 2: Reporting to Public Health Cancer Registries from Ambulatory Healthcare Providers, Release 1, DSTU Release 1.1, October 2017. Effective for testing on February 04, 2021. Surveillance compliance date on May 06, 2022.
- Mapping to the North American Association of Central Cancer Registries (NAACCR) format is not included in the IG because the mapping rules are complex and can change over time based on continued input and refinement by the cancer registry community. It is ONC's understanding that the CDC will work closely with the cancer registry community to develop mapping rules for the IG and will incorporate the rules into the software tools CDC provides state cancer registries. In regard to concerns expressed about jurisdictional variations, all public health jurisdictions have adopted the HL7® IG Release 1 for cancer reporting and will be moving to the updated version published by the CDC. [see also 80 FR 62666]
- The CDC National Program of Cancer Registries (NCPR), and the North American Association of Central Cancer Registries (NAACCR), no longer require state cancer registries to collect "Stager Clinical Cancer" and "Stager Pathologic Cancer" (also referred to as "Staged By") data elements for cases diagnosed in 2018 or later. For testing of this criterion, ONC will allow for any valid value in the specified value set to be provided for the "Stager Clinical Cancer" and "Stager Pathologic Cancer" elements.

Paragraph (f)(4)(ii) Create cancer case information in accordance with SNOMED CT® and LOINC®

Technical outcome – The health IT can create cancer case information for electronic transmission using, at a minimum, the March 2022 Release of the U.S. Edition of SNOMED CT® and Version 2.76 of LOINC®.

Clarifications:

- ONC provides the following object identifiers (OIDs) to assist developers in the proper identification and exchange of health information coded to certain vocabulary standards.
    - SNOMED CT® OID: 2.16.840.1.113883.6.96
    - LOINC® OID: 2.16.840.1.113883.6.1 [see also 80 FR 62612]
- Health IT Modules can present for certification to a more recent version of SNOMED CT®, and LOINC® than what is outlined in regulation per ONC's policy that permits certification to a more recent version of certain vocabulary standards. [see also 80 FR 62620]

Technical outcome – The health IT can create cancer case information for electronic transmission using, at a minimum, the March 2022 Release of the U.S. Edition of SNOMED CT® and Version 2.76 of LOINC®.

Clarifications:

- ONC provides the following object identifiers (OIDs) to assist developers in the proper identification and exchange of health information coded to certain vocabulary standards.
    - SNOMED CT® OID: 2.16.840.1.113883.6.96
    - LOINC® OID: 2.16.840.1.113883.6.1 [see also 80 FR 62612]
- Health IT Modules can present for certification to a more recent version of SNOMED CT®, and LOINC® than what is outlined in regulation per ONC's policy that permits certification to a more recent version of certain vocabulary standards. [see also 80 FR 62620]