Transmission to public health agencies — electronic case reporting

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (f)(5) *Transmission to public health agencies – electronic case reporting*—Enable a user to create a case report for electronic transmission meeting the requirements described in paragraphs (f)(5)(i) of this section for the time period up to and including December 31, 2025; or the requirements described in paragraph (f)(5)(ii) of this section.

1. *Functional electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and maintain a table of trigger codes to determine which encounters may be reportable.
    2. Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.
    3. *Case report creation.* Create a case report for electronic transmission:
        1. Based on a matched trigger from paragraph (f)(5)(i)(B).
        2. That includes, at a minimum:
            1. The data classes expressed in the standards in § 170.213
            2. *Encounter diagnoses.* Formatted according to at least one of the following standards specified in
                1. § 170.207(i) or
                2. § 170.207(a)(1).
            3. The provider's name, office contact information, and reason for visit.
            4. An identifier representing the row and version of the trigger table that triggered the case report.

2. *Standards-based electronic care reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4).
    2. Create a case report consistent with at least one of the following standards:
        1. The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1); or
        2. The HL7 CDA eICR IG in § 170.205(t)(2).
    3. Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in (f)(5)(ii)(B) of this section.
    4. Transmit a case report electronically to a system capable of receiving a case report.

Standard(s) Referenced

Paragraph (f)(5)(i)(C)(2)

§ 170.213(a) United States Core Data for Interoperability (USCDI), July 2020 Errata, Version 1 (v1) (Adoption of this standard expires on January 1, 2026)

§ 170.213(b) United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) (This standard is required by December 31, 2025)

§ 170.207(a)(4) IHTSDO SNOMED CT®, U.S. Edition, September 2019 Release (Adoption of this standard expires January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release

§ 170.207(i) Encounter diagnoses: The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions ICD-10-CM as maintained and distributed by HHS, for the following conditions:

1. Diseases.
2. Injuries.
3. Impairments.
4. Other health problems and their manifestations.
5. Causes of injury, disease, impairment, or other health problems.

Paragraph (f)(5)(ii)(A)

§ 170.205(t)(4) Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022 (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(B)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(2) HL7® CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7® CDA® eICR IG) (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(C)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(3) HL7® CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7® CDA® RR IG) (This standard is required by December 31, 2025)

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

United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

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 § 170.315(f)(5) must update their Health IT Modules to be compliant with the requirements outlined at paragraph (f)(5)(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 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(f)(5). 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 presented 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 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

Regulation Text

Regulation Text

§ 170.315 (f)(5) *Transmission to public health agencies – electronic case reporting*—Enable a user to create a case report for electronic transmission meeting the requirements described in paragraphs (f)(5)(i) of this section for the time period up to and including December 31, 2025; or the requirements described in paragraph (f)(5)(ii) of this section.

1. *Functional electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and maintain a table of trigger codes to determine which encounters may be reportable.
    2. Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.
    3. *Case report creation.* Create a case report for electronic transmission:
        1. Based on a matched trigger from paragraph (f)(5)(i)(B).
        2. That includes, at a minimum:
            1. The data classes expressed in the standards in § 170.213
            2. *Encounter diagnoses.* Formatted according to at least one of the following standards specified in
                1. § 170.207(i) or
                2. § 170.207(a)(1).
            3. The provider's name, office contact information, and reason for visit.
            4. An identifier representing the row and version of the trigger table that triggered the case report.

2. *Standards-based electronic care reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4).
    2. Create a case report consistent with at least one of the following standards:
        1. The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1); or
        2. The HL7 CDA eICR IG in § 170.205(t)(2).
    3. Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in (f)(5)(ii)(B) of this section.
    4. Transmit a case report electronically to a system capable of receiving a case report.

Standard(s) Referenced

Paragraph (f)(5)(i)(C)(2)

§ 170.213(a) United States Core Data for Interoperability (USCDI), July 2020 Errata, Version 1 (v1) (Adoption of this standard expires on January 1, 2026)

§ 170.213(b) United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) (This standard is required by December 31, 2025)

§ 170.207(a)(4) IHTSDO SNOMED CT®, U.S. Edition, September 2019 Release (Adoption of this standard expires January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release

§ 170.207(i) Encounter diagnoses: The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions ICD-10-CM as maintained and distributed by HHS, for the following conditions:

1. Diseases.
2. Injuries.
3. Impairments.
4. Other health problems and their manifestations.
5. Causes of injury, disease, impairment, or other health problems.

Paragraph (f)(5)(ii)(A)

§ 170.205(t)(4) Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022 (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(B)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(2) HL7® CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7® CDA® eICR IG) (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(C)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(3) HL7® CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7® CDA® RR IG) (This standard is required by December 31, 2025)

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

United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

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 § 170.315(f)(5) must update their Health IT Modules to be compliant with the requirements outlined at paragraph (f)(5)(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 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(f)(5). 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 presented 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))
  - 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 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

Testing components

Attestation: As of September 21, 2017, the testing approach for this criterion is satisfied by attestation.

The archived version of the Test Procedure is attached below for reference.

System Under Test	ONC-ACB Verification
The health IT developer will attest directly to the ONC-ACB to conformance with the § 170.315 (f)(5) *Transmission to public health agencies — electronic case reporting* requirements.	The ONC-ACB verifies the health IT developer attests conformance to the § 170.315 (f)(5) *Transmission to public health agencies — electronic case reporting* requirements.

Archived Version:
§170.315(f)(5) Test Procedure
Reference Documents

Trigger Code Table Examples 08-11-2016

Archived Version:
§ 170.315(f)(5) Transmission to public health agencies — electronic case reporting TP

Updated on 03-27-2025

Regulation Text

Regulation Text

§ 170.315 (f)(5) *Transmission to public health agencies – electronic case reporting*—Enable a user to create a case report for electronic transmission meeting the requirements described in paragraphs (f)(5)(i) of this section for the time period up to and including December 31, 2025; or the requirements described in paragraph (f)(5)(ii) of this section.

1. *Functional electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and maintain a table of trigger codes to determine which encounters may be reportable.
    2. Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.
    3. *Case report creation.* Create a case report for electronic transmission:
        1. Based on a matched trigger from paragraph (f)(5)(i)(B).
        2. That includes, at a minimum:
            1. The data classes expressed in the standards in § 170.213
            2. *Encounter diagnoses.* Formatted according to at least one of the following standards specified in
                1. § 170.207(i) or
                2. § 170.207(a)(1).
            3. The provider's name, office contact information, and reason for visit.
            4. An identifier representing the row and version of the trigger table that triggered the case report.

2. *Standards-based electronic care reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4).
    2. Create a case report consistent with at least one of the following standards:
        1. The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1); or
        2. The HL7 CDA eICR IG in § 170.205(t)(2).
    3. Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in (f)(5)(ii)(B) of this section.
    4. Transmit a case report electronically to a system capable of receiving a case report.

Standard(s) Referenced

Paragraph (f)(5)(i)(C)(2)

§ 170.213(a) United States Core Data for Interoperability (USCDI), July 2020 Errata, Version 1 (v1) (Adoption of this standard expires on January 1, 2026)

§ 170.213(b) United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) (This standard is required by December 31, 2025)

§ 170.207(a)(4) IHTSDO SNOMED CT®, U.S. Edition, September 2019 Release (Adoption of this standard expires January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release

§ 170.207(i) Encounter diagnoses: The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions ICD-10-CM as maintained and distributed by HHS, for the following conditions:

1. Diseases.
2. Injuries.
3. Impairments.
4. Other health problems and their manifestations.
5. Causes of injury, disease, impairment, or other health problems.

Paragraph (f)(5)(ii)(A)

§ 170.205(t)(4) Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022 (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(B)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(2) HL7® CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7® CDA® eICR IG) (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(C)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(3) HL7® CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7® CDA® RR IG) (This standard is required by December 31, 2025)

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

United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

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 § 170.315(f)(5) must update their Health IT Modules to be compliant with the requirements outlined at paragraph (f)(5)(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 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(f)(5). 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 presented 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))
  - 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 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

Regulation Text

Regulation Text

§ 170.315 (f)(5) *Transmission to public health agencies – electronic case reporting*—Enable a user to create a case report for electronic transmission meeting the requirements described in paragraphs (f)(5)(i) of this section for the time period up to and including December 31, 2025; or the requirements described in paragraph (f)(5)(ii) of this section.

1. *Functional electronic case reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and maintain a table of trigger codes to determine which encounters may be reportable.
    2. Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.
    3. *Case report creation.* Create a case report for electronic transmission:
        1. Based on a matched trigger from paragraph (f)(5)(i)(B).
        2. That includes, at a minimum:
            1. The data classes expressed in the standards in § 170.213
            2. *Encounter diagnoses.* Formatted according to at least one of the following standards specified in
                1. § 170.207(i) or
                2. § 170.207(a)(1).
            3. The provider's name, office contact information, and reason for visit.
            4. An identifier representing the row and version of the trigger table that triggered the case report.
2. *Standards-based electronic care reporting.* A Health IT Module must enable a user to create a case report for electronic transmission in accordance with the following:
    1. Consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code value set in § 170.205(t)(4).
    2. Create a case report consistent with at least one of the following standards:
        1. The eICR profile of the HL7 FHIR eCR IG in § 170.205(t)(1); or
        2. The HL7 CDA eICR IG in § 170.205(t)(2).
    3. Receive, consume, and process a case report response that is formatted to either the reportability response profile of the HL7 FHIR eCR IG in § 170.205(t)(1) or the HL7 CDA RR IG in § 170.205(t)(3) as determined by the standard used in (f)(5)(ii)(B) of this section.
    4. Transmit a case report electronically to a system capable of receiving a case report.

Standard(s) Referenced

Paragraph (f)(5)(i)(C)(2)

§ 170.213(a) United States Core Data for Interoperability (USCDI), July 2020 Errata, Version 1 (v1) (Adoption of this standard expires on January 1, 2026)

§ 170.213(b) United States Core Data for Interoperability (USCDI), October 2022 Errata, Version 3 (v3) (This standard is required by December 31, 2025)

§ 170.207(a)(4) IHTSDO SNOMED CT®, U.S. Edition, September 2019 Release (Adoption of this standard expires January 1, 2026)

§ 170.207(a)(1) SNOMED CT®, U.S. Edition, March 2022 Release

§ 170.207(i) Encounter diagnoses: The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions ICD-10-CM as maintained and distributed by HHS, for the following conditions:

1. Diseases.
2. Injuries.
3. Impairments.
4. Other health problems and their manifestations.
5. Causes of injury, disease, impairment, or other health problems.

Paragraph (f)(5)(ii)(A)

§ 170.205(t)(4) Reportable Conditions Trigger Codes Value Set for Electronic Case Reporting. RCTC OID: 2.16.840.1.114222.4.11.7508, Release March 29, 2022 (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(B)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(2) HL7® CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 - US Realm (HL7® CDA® eICR IG) (This standard is required by December 31, 2025)

Paragraph (f)(5)(ii)(C)

§ 170.205(t)(1) HL7® FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.0 – STU 2 US (HL7® FHIR® eCR IG) (This standard is required by December 31, 2025)

§ 170.205(t)(3) HL7® CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm (HL7® CDA® RR IG) (This standard is required by December 31, 2025)

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

United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata

For more information, please visit the Standards Version Advancement Process (SVAP) Version(s) page.

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 § 170.315(f)(5) must update their Health IT Modules to be compliant with the requirements outlined at paragraph (f)(5)(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 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(f)(5). 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 presented 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 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	Added clarification on effective date regarding standard at § 170.207(a)(1), "*Standard.* SNOMED CT®, U.S. Edition, March 2022 Release (incorporated by reference, see § 170.299).	03-19-2024
1.2	Standards Referenced updated to reflect 2024 Approved SVAP Standards	08-19-2024
1.3	For entire criterion, added clarification regarding compliance with EO 14168 and OPM guidance	03-27-2025

Certification Companion Guide: Transmission to public health agencies — electronic case reporting

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	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: Public Health and Clinical Data Registry Reporting.
- For the functional requirements in § 170.315(f)(5)(i), a specific content exchange standard for electronic case reporting (eCR) is not required to meet this criterion. [see also 80 FR 62667]
- For the functional requirements in § 170.315(f)(5)(i), this criterion may be met through one of the following two ways:
    - Documentation that sufficiently describes how the Health IT Module meets the functional requirements of the criterion.
    - Documentation eCR implementation using the eCR Now Fast Health Interoperability Resources (FHIR®) application and the ability to meet paragraph § 170.315(f)(5)(i)(A) of this criterion. Note that this optional certification pathway using the eCR Now FHIR® application may require a different set of data elements than specified in § 170.315(f)(5)(i)(C)(2).

- For the time period up to and including December 31, 2025, Health IT Modules certified to § 170.315(f)(5)(i) may meet the requirements in § 170.315(f)(5)(i)(C)(2)(ii) using SNOMED CT® September 2015 Release or any later version. On and after December 31, 2025, Health IT Modules that wish to remain certified to 170.315(f)(5) must meet the requirements at 170.315(f)(5)(ii).
- Consistent with Executive Order (EO) 14168 and OPM guidance, Health IT Modules certifying and/or currently certified to certification criteria that cross-reference the USCDI standard at 45 CFR 170.213 are only required to demonstrate the capability to categorize data on individuals for the sex data element in accordance with the following SNOMED CT® codes:
    - 248152002 |Female (finding)| and
    - 248153007 |Male (finding)|
- Further, these Health IT Modules are no longer required to support the following USCDI data elements for purposes of certification:
    - Sexual orientation in USCDI version 4;
    - Gender identity in USCDI version 4;
    - Sex parameter for clinical use in USCDI version 5;
    - Name to use in USCDI version 5;
    - Pronouns in USCDI version 5.

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: Public Health and Clinical Data Registry Reporting.
- For the functional requirements in § 170.315(f)(5)(i), a specific content exchange standard for electronic case reporting (eCR) is not required to meet this criterion. [see also 80 FR 62667]
- For the functional requirements in § 170.315(f)(5)(i), this criterion may be met through one of the following two ways:
    - Documentation that sufficiently describes how the Health IT Module meets the functional requirements of the criterion.
    - Documentation eCR implementation using the eCR Now Fast Health Interoperability Resources (FHIR®) application and the ability to meet paragraph § 170.315(f)(5)(i)(A) of this criterion. Note that this optional certification pathway using the eCR Now FHIR® application may require a different set of data elements than specified in § 170.315(f)(5)(i)(C)(2).
- For the time period up to and including December 31, 2025, Health IT Modules certified to § 170.315(f)(5)(i) may meet the requirements in § 170.315(f)(5)(i)(C)(2)(ii) using SNOMED CT® September 2015 Release or any later version. On and after December 31, 2025, Health IT Modules that wish to remain certified to 170.315(f)(5) must meet the requirements at 170.315(f)(5)(ii).
- Consistent with Executive Order (EO) 14168 and OPM guidance, Health IT Modules certifying and/or currently certified to certification criteria that cross-reference the USCDI standard at 45 CFR 170.213 are only required to demonstrate the capability to categorize data on individuals for the sex data element in accordance with the following SNOMED CT® codes:
    - 248152002 |Female (finding)| and
    - 248153007 |Male (finding)|
- Further, these Health IT Modules are no longer required to support the following USCDI data elements for purposes of certification:
    - Sexual orientation in USCDI version 4;
    - Gender identity in USCDI version 4;
    - Sex parameter for clinical use in USCDI version 5;
    - Name to use in USCDI version 5;
    - Pronouns in USCDI version 5.

Paragraph (f)(5)(i)(A) Functional eCR – Consume and maintain

Technical outcome – A Health IT Module is able to consume and maintain a table of trigger codes to determine which encounters may be reportable.

Clarifications:

> An example table of trigger codes is in "Trigger Code Table Examples" under the Reference Documents section on the Test Procedures tab.

Technical outcome – A Health IT Module is able to consume and maintain a table of trigger codes to determine which encounters may be reportable.

Clarifications:

An example table of trigger codes is in "Trigger Code Table Examples" under the Reference Documents section on the Test Procedures tab.

Paragraph (f)(5)(i)(B) Functional eCR - Match

Technical outcome – A Health IT Module can match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

Clarifications:

No additional clarifications.

Technical outcome – A Health IT Module can match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

Clarifications:

No additional clarifications.

Paragraph (f)(5)(i)(C) Functional eCR – Case report creation

Technical outcome – A Health IT Module can create a case report for electronic transmission.

Clarifications

- For attestation, a health IT developer must attest to their product's ability to support the referenced standard(s) in § 170.315(f)(5)(iii)(B)(*1*) or (*2*). However, individual public health authorities may require a subset of this data for reporting.

- ONC provides the following object identifier (OID) to assist developers in the proper identification and exchange of health information coded to certain vocabulary standards [see also 80 FR 62612-13]:
    - SNOMED CT® OID: 2.16.840.1.113883.6.96
    - LOINC® OID: 2.16.840.1.113883.6.1
    - RxNorm OID: 2.16.840.1.113883.6.88
    - HL7® Standard Code Set CVX-Vaccines Administered OID: 2.16.840.1.113883.12.292
    - National Drug Code (NDC) Directory OID: 2.16.840.1.113883.6.69
    - International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS) OID: 2.16.840.1.113883.6.4
    - CDC Race and Ethnicity Code Set Version 1.0 (March 2000) OID: 2.16.840.1.113883.6.238
    - Tags for Identifying Languages—Request for Comment (RFC) 5646 (preferred language) OID: 2.16.840.1.113883.6.316
    - Healthcare Provider Taxonomy OID: 2.16.840.1.113883.6.101
- A Health IT Module can present for testing and certification to more recent versions of the following vocabulary standards than the versions outlined in regulation:
    - SNOMED CT®
    - LOINC®
    - RxNorm
    - CVX
    - NDC
    - CDC Race Ethnicity Code Set
- The requirement for an identifier representing the row and version of the trigger table that triggered the case report in (f)(5)(iii)(B) can be met by providing an identifier that will uniquely identify the original file from which the “matched trigger” described above originated (the version of the trigger table) as well as uniquely identify the individual trigger (row) itself.
- Support for the USCDI standard at § 170.213 as part of this criterion is only required for the time period up to and including December 31, 2025.

Technical outcome – A Health IT Module can create a case report for electronic transmission.

Clarifications

- For attestation, a health IT developer must attest to their product's ability to support the referenced standard(s) in § 170.315(f)(5)(iii)(B)(*1*) or (*2*). However, individual public health authorities may require a subset of this data for reporting.
- ONC provides the following object identifier (OID) to assist developers in the proper identification and exchange of health information coded to certain vocabulary standards [see also 80 FR 62612-13]:
  - SNOMED CT® OID: 2.16.840.1.113883.6.96
  - LOINC® OID: 2.16.840.1.113883.6.1
  - RxNorm OID: 2.16.840.1.113883.6.88
  - HL7® Standard Code Set CVX-Vaccines Administered OID: 2.16.840.1.113883.12.292
  - National Drug Code (NDC) Directory OID: 2.16.840.1.113883.6.69
  - International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS) OID: 2.16.840.1.113883.6.4
  - CDC Race and Ethnicity Code Set Version 1.0 (March 2000) OID: 2.16.840.1.113883.6.238
  - Tags for Identifying Languages—Request for Comment (RFC) 5646 (preferred language) OID: 2.16.840.1.113883.6.316
  - Healthcare Provider Taxonomy OID: 2.16.840.1.113883.6.101
- A Health IT Module can present for testing and certification to more recent versions of the following vocabulary standards than the versions outlined in regulation:
  - SNOMED CT®
  - LOINC®
  - RxNorm
  - CVX
  - NDC
  - CDC Race Ethnicity Code Set
- The requirement for an identifier representing the row and version of the trigger table that triggered the case report in (f)(5)(iii)(B) can be met by providing an identifier that will uniquely identify the original file from which the "matched trigger" described above originated (the version of the trigger table) as well as uniquely identify the individual trigger (row) itself.
- Support for the USCDI standard at § 170.213 as part of this criterion is only required for the time period up to and including December 31, 2025.

Paragraph (f)(5)(ii)(A) Standards-based eCR – Consume and process trigger codes

Technical outcome – Health IT Module is able to consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code (RCTC) value set.

Clarifications

- Health IT Modules do not need to support the eRSD profiles, including the eRSD PlanDefinition, Supplemental Library, and Specification Library as part of certification to this criterion. This is to allow developers flexibility to support the consumption of the RCTC value set in the way that best suits their technology and does not constrain how the RCTC value set is consumed as the underlying standards mature. [see also 89 FR 1228]
- The RCTC value set defined at § 170.205(t)(4) is a minimum standard code set and Health IT Modules may voluntarily support an updated version of the RCTC value set. [see also 89 FR 1228]
- The RCTC value set is currently available for distribution by the Association of Public Health Laboratories. [see also 89 FR 1228]

Technical outcome – Health IT Module is able to consume and process case reporting trigger codes and identify a reportable patient visit or encounter based on a match from the Reportable Conditions Trigger Code (RCTC) value set.

Clarifications

- Health IT Modules do not need to support the eRSD profiles, including the eRSD PlanDefinition, Supplemental Library, and Specification Library as part of certification to this criterion. This is to allow developers flexibility to support the consumption of the RCTC value set in the way that best suits their technology and does not constrain how the RCTC value set is consumed as the underlying standards mature. [see also 89 FR 1228]
- The RCTC value set defined at § 170.205(t)(4) is a minimum standard code set and Health IT Modules may voluntarily support an updated version of the RCTC value set. [see also 89 FR 1228]
- The RCTC value set is currently available for distribution by the Association of Public Health Laboratories. [see also 89 FR 1228]

Paragraph (f)(5)(ii)(B) Standards-based eCR – Create a case report

Technical outcome –A Health IT Module can create a case report for electronic transmission using the HL7® FHIR® eCR IG or CDA® eICR IG standards.

Clarifications

No additional clarifications.

Technical outcome –A Health IT Module can create a case report for electronic transmission using the HL7® FHIR® eCR IG or CDA® eICR IG standards.

Clarifications

No additional clarifications.

Paragraph (f)(5)(ii)(C) Standards-based eCR – Receive, consume and process a case report response

Technical outcome –A Health IT Module can receive, consume and process a case report response for electronic transmission using the HL7® FHIR® eCR IG or CDA® RR IG standards.

Clarifications

No additional clarifications.

Technical outcome –A Health IT Module can receive, consume and process a case report response for electronic transmission using the HL7® FHIR® eCR IG or CDA® RR IG standards.

Clarifications

No additional clarifications.

Paragraph (f)(5)(ii)(D) Standards-based eCR – Transmit a case report electronically

Technical outcome –A Health IT Module can transmit a case report electronically to a system capable of receiving a case report.

Clarifications

These requirements remain agnostic as to which reporting platform and which decision support tool(s) are used. [see also 89 FR 1231]

Technical outcome –A Health IT Module can transmit a case report electronically to a system capable of receiving a case report.

Clarifications

> These requirements remain agnostic as to which reporting platform and which decision support tool(s) are used. [see also 89 FR 1231]

Archived Version:

§ 170.315(f)(5) Transmission to public health agencies — electronic case reporting CCG