HealthIT.gov

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

2015 Edition CCGs

Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-27-2015
1.1	Modified to provide methods and clarifications for demonstrating conformance with the certification criterion.	08-11-2017
1.2	Updated the Security requirements per 21st Century Cures Act.	06-15-2020

Regulation Text

Regulation Text

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

(i) Consume and maintain a table of trigger codes to determine which encounters may be reportable.

(ii) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.

(iii) *Case report creation.* Create a case report for electronic transmission:

(A) Based on a matched trigger from paragraph (f)(5)(ii).

(B) That includes, at a minimum:

(1) The Common Clinical Data Set.

(2) Encounter diagnoses. Formatted according to at least one of the following standards:

(i) The standard specified in §170.207(i).

(ii) At a minimum, the version of the standard specified in §170.207(a)(4).

(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.

Standard(s) Referenced

Paragraph (f)(5)(iii)

§ 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

§ 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:

(i) Diseases.
(ii) Injuries.
(iii) Impairments.
(iv) Other health problems and their manifestations.
(v) Causes of injury, disease, impairment, or other health problems.

Please refer to the Data Elements and Vocabularies applicable to the Common Clinical Data Set (CCDS) as outlined in the Common Clinical Data Set Reference Document

Resource Documents

Resource Document

- Privacy and Security Certification Companion Guide [PDF - 281 KB]
- 2015 Edition Network Time Protocol (NTP) [PDF - 157 KB]
- CHPL SED Guide [PDF - 690 KB]
- Master Table of Related and Required Criteria [PDF-251 KB]

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-27-2015
1.1	Modified to provide methods and clarifications for demonstrating conformance with the certification criterion.	08-11-2017
1.2	Updated the Security requirements per 21st Century Cures Act.	06-15-2020

Regulation Text

Regulation Text

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

(i) Consume and maintain a table of trigger codes to determine which encounters may be reportable.
(ii) Match a patient visit or encounter to the trigger code based on the parameters of the trigger code table.
(iii) *Case report creation.* Create a case report for electronic transmission:
(A) Based on a matched trigger from paragraph (f)(5)(ii).
(B) That includes, at a minimum:
(1) The Common Clinical Data Set.

(2) Encounter diagnoses. Formatted according to at least one of the following standards:
(i) The standard specified in §170.207(i).
(ii) At a minimum, the version of the standard specified in §170.207(a)(4).
(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.

Standard(s) Referenced

Paragraph (f)(5)(iii)

§ 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

§ 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:

(i) Diseases.
(ii) Injuries.
(iii) Impairments.
(iv) Other health problems and their manifestations.
(v) Causes of injury, disease, impairment, or other health problems.

Please refer to the Data Elements and Vocabularies applicable to the Common Clinical Data Set (CCDS) as outlined in the Common Clinical Data Set Reference Document

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 development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Not Included	Yes

Certification Requirements

Privacy and Security: 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.
- § 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.

Table for Privacy and Security

- 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 using 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 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.

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.

- 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.
- 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 for which a certificate would be requested.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

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.
- A specific content exchange standard for electronic case reporting (eCR) is not required to meet this criterion. [see also 80 FR 62667]
- 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 of participation in an initial eCR implementation as part of the Digital Bridge initiative and the ability to meet paragraph (i) of this criterion.

- The optional use of an ONC-approved test tool for case reporting using standards such as Consolidated Clinical Document Architecture (C-CDA), the Structured Data Capture (IHE SDC) Implementation Guide, or the Fast Health Interoperability Resources (FHIR®) Structured Data Capture Implementation Guide may be available in the future. While not required to meet this criterion, testing through an ONC-approved test tool for case reporting would meet the requirements of this criterion.

Paragraph (f)(5)(i)

Technical outcome – A Health IT Module is able to consume and maintain a table of trigger codes to determine which encounters should initiate an initial case report being sent to a public health agency.

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)(ii)

Technical outcome – A Health IT Module can match information recorded in a patient visit or encounter to a trigger code in the trigger code table.

Clarifications:

- No additional clarifications.

Paragraph (f)(5)(iii)

Technical outcome – When a trigger is matched in accordance with provision (f)(5)(ii), the Health IT Module electronically creates an initial case report with only the following subset of Common Clinical Data Set (CCDS) data elements:

- Patient Name
- Sex
- Date of Birth
- Race and Ethnicity
- Preferred language
- Problems
- Medications
- Laboratory Tests
- Laboratory Values(s)/Result(s)
- Vital Signs
- Procedures
- Care Team Member(s)
- Immunizations
- Assessment and Plan of Treatment

Clarifications

- ONC provides the following object identifiers (OID) to assist developers in the proper identification and exchange of health information coded to certain vocabulary standards [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 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 adopted in the 2015 Edition final rule [80 FR 62612]:
  - SNOMED CT®
  - LOINC®
  - RxNorm
  - CVX
  - NDC
  - CDC Race Ethnicity Code Set
- All data elements included in the CCDS are required to be available by the Health IT Module; however, the test procedure includes only a subset of elements that are required to be included in the case report by public health to support case reporting at this time.
- 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.

Content last reviewed on August 29, 2022