Transmission to public health agencies — syndromic surveillance

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (f)(2) *Transmission to public health agencies – syndromic surveillance*—

Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

Standard(s) Referenced

Applies to entire criterion

§ 170.205(d)(4) Health Level 7 (HL7®) 2.5.1. *Implementation specifications*. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Care, Inpatient and Ambulatory Care, and Inpatient Settings, Release 2.0, April 21, 2015 and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015

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

HL7® Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1 - US Realm Standard for Trial Use, July 2019

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

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, 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)(2). 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	Final Test Procedure	03-11-2024

Regulation Text
Regulation Text

§ 170.315 (f)(2) *Transmission to public health agencies – syndromic surveillance*—

Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

Standard(s) Referenced

Applies to entire criterion

§ 170.205(d)(4) Health Level 7 (HL7®) 2.5.1. *Implementation specifications*. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Care, Inpatient and Ambulatory Care, and Inpatient Settings, Release 2.0, April 21, 2015 and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015

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

HL7® Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1 - US Realm Standard for Trial Use, July 2019

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

Certification Dependencies
Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, 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)(2). 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® v2 Syndromic Surveillance Test Suite

Test Tool Documentation

NIST Normative Test Process Document

Criterion Subparagraph	Test Data
(f)(2)	Refer to NIST HL7® v2 Syndromic Surveillance Test Suite

Revision History

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

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

ONC
Supplied
Test
Data

SVAP

Paragraph (f)(2) Transmission to public health agencies – syndromic surveillance

System Under Test

1. The health IT developer identifies which of the health care setting(s) (Emergency Department, Inpatient, Urgent Care) is applicable to the system under test. The Health IT Module creates syndromic surveillance content using ONC-supplied test data for each of the test cases for the identified health care setting(s) under the ONC Certification Test Plan on the Context-Based Validation Tab of the NIST HL7® v2 Syndromic Surveillance Test Suite. All test cases are required that apply to the health care setting(s) supported by the system under test. Input may be performed using manual or automated processes.
2. For each test case, the Health IT Module generates the indicated HL7® v2.5.1 ADT message type containing the Syndromic Surveillance information and using the provided test data and according to the § 170.205(d)(4) PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Care, Inpatient and Ambulatory Care, and Inpatient Settings, Release 2.0 and associated Erratum.

Test Lab Verification

Using theNormative Test Description section of the Normative Test Process Document:

1. The tester verifies the Health IT Module creates the source syndromic surveillance content correctly and without omission through visual inspection of the system under test using the test data specification of each Test Step associated with the selected test case.
2. The tester imports the syndromic surveillance message into the NIST HL7® v2 Syndromic Surveillance Test Suite and uses the Validation Report produced by the test tool to verify the Health IT Module passes without error to confirm that the syndromic surveillance message is conformant to the HL7® v2.5.1 ADT message type in the § 170.205(d)(4) standard and associated Erratum.

System Under Test	Test Lab Verification

System Under Test

1. The health IT developer identifies which of the health care setting(s) (Emergency Department, Inpatient, Urgent Care) is applicable to the system under test. The Health IT Module creates syndromic surveillance content using ONC-supplied test data for each of the test cases for the identified health care setting(s) under the ONC Certification Test Plan on the Context-Based Validation Tab of the NIST HL7® v2 Syndromic Surveillance Test Suite. All test cases are required that apply to the health care setting(s) supported by the system under test. Input may be performed using manual or automated processes.
2. For each test case, the Health IT Module generates the indicated HL7® v2.5.1 ADT message type containing the Syndromic Surveillance information and using the provided test data and according to the § 170.205(d)(4) PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Care, Inpatient and Ambulatory Care, and Inpatient Settings, Release 2.0 and associated Erratum.

Test Lab Verification

Using theNormative Test Description section of the Normative Test Process Document:

1. The tester verifies the Health IT Module creates the source syndromic surveillance content correctly and without omission through visual inspection of the system under test using the test data specification of each Test Step associated with the selected test case.
2. The tester imports the syndromic surveillance message into the NIST HL7® v2 Syndromic Surveillance Test Suite and uses the Validation Report produced by the test tool to verify the Health IT Module passes without error to confirm that the syndromic surveillance message is conformant to the HL7® v2.5.1 ADT message type in the § 170.205(d)(4) standard and associated Erratum.

Updated on 08-19-2024

Regulation Text

Regulation Text

§ 170.315 (f)(2) *Transmission to public health agencies – syndromic surveillance*—

Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

Standard(s) Referenced

Applies to entire criterion

§ 170.205(d)(4) Health Level 7 (HL7®) 2.5.1. *Implementation specifications*. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Care, Inpatient and Ambulatory Care, and Inpatient Settings, Release 2.0, April 21, 2015 and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015

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

HL7® Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1 - US Realm Standard for Trial Use, July 2019

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

Certification Dependencies

Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, 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)(2). 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	Final Test Procedure	03-11-2024

Regulation Text

Regulation Text

§ 170.315 (f)(2) *Transmission to public health agencies – syndromic surveillance—*

Create syndrome-based public health surveillance information for electronic transmission in accordance with the standard (and applicable implementation specifications) specified in § 170.205(d)(4).

Standard(s) Referenced

Applies to entire criterion

§ 170.205(d)(4) Health Level 7 (HL7®) 2.5.1. *Implementation specifications*. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent, Care, Inpatient and Ambulatory Care, and Inpatient Settings, Release 2.0, April 21, 2015 and Erratum to the CDC PHIN 2.0 Implementation Guide, August 2015

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

HL7® Version 2.5.1 Implementation Guide: Syndromic Surveillance, Release 1 - US Realm Standard for Trial Use, July 2019

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

Certification Dependencies
Conditions and Maintenance of Certification

Real World Testing:Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, 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)(2). 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	Standards Referenced updated to reflect 2024 Approved SVAP Standards	08-19-2024

Testing

Testing Tool

NIST HL7® v2 Syndromic Surveillance Test Suite

Test Tool Documentation

NIST Normative Test Process Document

Criterion Subparagraph	Test Data

Criterion Subparagraph	Test Data
(f)(2)	Refer to NIST HL7® v2 Syndromic Surveillance Test Suite

Certification Companion Guide: Transmission to public health agencies — syndromic surveillance

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

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

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

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Technical outcome – The health IT is able to create syndrome-based public health surveillance information for electronic transmission to public health agencies according to the HL7 2.5.1 standard, the Public Health Information Network (PHIN) Messaging Guide for Syndromic Surveillance Release 2.0, and the August 2015 Erratum to the PHIN Messaging Guide.

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.

- Health IT is not required to comply with the implementation guide's requirement that a sender's system (Health IT Module) support the ICD-9-CM value set.
- Health IT must be tested and certified to only one of the value sets for the implementation guide's "submitted messages" requirement. More specifically, this means that a Health IT Module can use either the ICD-10-CM or SNOMED CT® value sets in the submitted messages for all of the test steps in the Syndromic Surveillance Test Suite. Where the tool does not have test data that supports the Health IT Module's value set (either ICD-10-CM or SNOMED CT®), the developer of the Health IT Module must provide the codes and testers must perform a visual inspection of the messages for these test steps to ensure that equivalent and valid ICD-10-CM or SNOMED CT® are used to populate the messages.
- It is appropriate to distinguish between ambulatory settings and emergency department, urgent care and inpatient settings. This criterion requires the use of the HL7® 2.5.1 standard, PHIN Messaging Guide Release 2.0, and August 2015 Erratum to the PHIN Messaging Guide for the inpatient setting (which includes emergency departments).
- There is no certification requirement for the ambulatory setting. ONC notes that the PHIN Messaging Guide Release 2.0 and Erratum does support the urgent care ambulatory setting and would be appropriate to use to that particular setting. [see also 80 FR 62665]
- The CDC published an erratum to the PHIN Messaging Guide Release 2.0 (August 2015). The Erratum consolidates Release 2.0 information and clarifies existing conformance requirements of the implementation guide. ONC refers developers to the addendum for specific information about the clarifications it includes. [see also 80 FR 62665]
- There is no transport standard required for this criterion. Developers have the flexibility to determine the transport standard(s) to implement. [see also 77 FR 54243]

Technical outcome – The health IT is able to create syndrome-based public health surveillance information for electronic transmission to public health agencies according to the HL7 2.5.1 standard, the Public Health Information Network (PHIN) Messaging Guide for Syndromic Surveillance Release 2.0, and the August 2015 Erratum to the PHIN Messaging Guide.

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.
- Health IT is not required to comply with the implementation guide's requirement that a sender's system (Health IT Module) support the ICD-9-CM value set.
- Health IT must be tested and certified to only one of the value sets for the implementation guide's "submitted messages" requirement. More specifically, this means that a Health IT Module can use either the ICD-10-CM or SNOMED CT® value sets in the submitted messages for all of the test steps in the Syndromic Surveillance Test Suite. Where the tool does not have test data that supports the Health IT Module's value set (either ICD-10-CM or SNOMED CT®), the developer of the Health IT Module must provide the codes and testers must perform a visual inspection of the messages for these test steps to ensure that equivalent and valid ICD-10-CM or SNOMED CT® are used to populate the messages.
- It is appropriate to distinguish between ambulatory settings and emergency department, urgent care and inpatient settings. This criterion requires the use of the HL7® 2.5.1 standard, PHIN Messaging Guide Release 2.0, and August 2015 Erratum to the PHIN Messaging Guide for the inpatient setting (which includes emergency departments).
- There is no certification requirement for the ambulatory setting. ONC notes that the PHIN Messaging Guide Release 2.0 and Erratum does support the urgent care ambulatory setting and would be appropriate to use to that particular setting. [see also 80 FR 62665]
- The CDC published an erratum to the PHIN Messaging Guide Release 2.0 (August 2015). The Erratum consolidates Release 2.0 information and clarifies existing conformance requirements of the implementation guide. ONC refers developers to the addendum for specific information about the clarifications it includes. [see also 80 FR 62665]
- There is no transport standard required for this criterion. Developers have the flexibility to determine the transport standard(s) to implement. [see also 77 FR 54243]