

Application access — all data request

 healthit.gov/test-method/application-access-all-data-request

- [Certification Companion Guide \(CCG\)](#)
- [Test Procedure](#)

Updated on 03-21-2025

Regulation Text

Regulation Text

§ 170.315 (g)(9) *Application access – all data request*—

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

1. *Functional requirements.*

1.

1. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section for the time period up to and including December 31, 2025, or
2. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (6) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section.
3. The following data classes:
 1. *Assessment and plan of treatment.* In accordance with the “Assessment and Plan Section (V2)” of the standards specified in § 170.205(a)(4); or in accordance with the “Assessment Section (V2)” and “Plan of Treatment Section (V2)” of the standards specified in § 170.205(a)(4).
 2. *Goals.* In accordance with the “Goals Section” of the standard specified in § 170.205(a)(4).
 3. *Health concerns.* In accordance with the “Health Concerns Section” of the standard specified in § 170.205(a)(4).
 4. *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the “Product Instance” in the “Procedure Activity Procedure Section” of the standard specified in § 170.205(a)(4).

2. Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

2. *Documentation—*

1. The API must include accompanying documentation that contains, at a minimum:
 1. API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
 2. The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
2. The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Paragraph (g)(9)(i)(A)

§ 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)

§ 170.205(a)(4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015, June 2019 (with Errata)

§ 170.205(a)(5) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 2, October 2019 (Adoption of this standard expires on January 1, 2026)

§ 170.205(a)(6) Health Level 7 (HL7®) CDA R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 4.1 - US Realm (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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

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 must update their certification to the newer versions of USCDI and C-CDA Companion Guide as outlined in paragraphs (g)(9)(i)(A)(1-2).

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.
- Consolidated CDA creation performance (§ 170.315(g)(6)): Consolidated Clinical Document Architecture (C-CDA) creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA Creation Performance CCG for more details.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(9). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to this 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 criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “View, download and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging”, which are explicitly stated.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- If choosing Approach 1:
 - Authentication, access control, and authorization (§ 170.315(d)(1)).
 - Trusted connection (§ 170.315(d)(9)).
 - Either auditable events and tamper-resistance (§ 170.315(d)(2)) or auditing actions on health information (§ 170.315(d)(10)).
 - 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
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standards and new SITE UI language	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (g)(9) Application access – all data request—

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

1. *Functional requirements.*

1.

1. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section for the time period up to and including December 31, 2025, or
2. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (6) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section.
3. The following data classes:
 1. *Assessment and plan of treatment.* In accordance with the “Assessment and Plan Section (V2)” of the standards specified in § 170.205(a)(4); or in accordance with the “Assessment Section (V2)” and “Plan of Treatment Section (V2)” of the standards specified in § 170.205(a)(4).
 2. *Goals.* In accordance with the “Goals Section” of the standard specified in § 170.205(a)(4).
 3. *Health concerns.* In accordance with the “Health Concerns Section” of the standard specified in § 170.205(a)(4).
 4. *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the “Product Instance” in the “Procedure Activity Procedure Section” of the standard specified in § 170.205(a)(4).

2. Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

2. *Documentation—*

1. The API must include accompanying documentation that contains, at a minimum:
 1. API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
 2. The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
2. The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(9)(i)(A)

§ 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)

§ 170.205(a)(4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015, June 2019 (with Errata)

§ 170.205(a)(5) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 2, October 2019 (Adoption of this standard expires on January 1, 2026)

§ 170.205(a)(6) Health Level 7 (HL7®) CDA R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 4.1 - US Realm (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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

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 must update their certification to the newer versions of USCDI and C-CDA Companion Guide as outlined in paragraphs (g)(9)(i)(A)(1-2).

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.
- Consolidated CDA creation performance (§ 170.315(g)(6)): Consolidated Clinical Document Architecture (C-CDA) creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA Creation Performance CCG for more details.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(9). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to this 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 criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “View, download and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging”, which are explicitly stated.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- If choosing Approach 1:
 - Authentication, access control, and authorization (§ 170.315(d)(1)).
 - Trusted connection (§ 170.315(d)(9)).
 - Either auditable events and tamper-resistance (§ 170.315(d)(2)) or auditing actions on health information (§ 170.315(d)(10)).
 - 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.

Testing

Testing Tool

Standards Implementation & Testing Environment (SITE): C-CDA Validators

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
(g)(9)(i)	Inpatient setting: - 170.315_g9_api_access_inp_sample*.docx (All Samples) Ambulatory setting - 170.315_g9_api_access_amb_sample*.docx (All Samples)

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

Version #	Description of Change	Version Date
1.1	Updated test tool link	12-02-2024
1.2	Updated test steps with 2024 SVAP approved standards and new SITE UI language	03-21-2025

This Test Procedure illustrates the test steps required to certify a Health IT Module to this criterion. Please consult the most recent Final Rules on the [Certification Regulations page](#) for a detailed description of the certification criterion with which these testing steps are associated. ASTP/ONC also encourages developers to consult the Certification Companion Guide in tandem with the test procedure as it provides clarifications that may be useful for product development and testing.

Note: The test step order does not necessarily prescribe the order in which the tests should take place.

Testing components



ONC
Supplied
Test
Data

SVAP

Paragraph (g)(9) - (Conditional - For Modules with existing certification to (g)(9))

System Under Test

Required by December 31, 2025

A health IT developer of a Health IT Module currently certified to the § 170.315(g)(9) Application access — all data access will attest directly to the ONC-ACB to conformance with the updated § 170.315(g)(9) 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

The ONC-ACB verifies the health IT developer of a Health IT Module certified to § 170.315(g)(9) Application access — all data access attests conformance to the updated § 170.315(g)(9) criterion requirements.

System Under Test

Required by December 31, 2025

A health IT developer of a Health IT Module currently certified to the § 170.315(g)(9) Application access — all data access will attest directly to the ONC-ACB to conformance with the updated § 170.315(g)(9) requirements outlined in the *Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1)* Final Rule.

ONC-ACB Verification

Required by December 31, 2025

The ONC-ACB verifies the health IT developer of a Health IT Module certified to § 170.315(g)(9) Application access — all data access attests conformance to the updated § 170.315(g)(9) criterion requirements.

Paragraph (g)(9)(i)(A)(1-2) Functional requirements – respond to requests for patient data

System Under Test

Expires on January 1, 2026

Setup

1. Using the ASTP Standards Implementation & Testing Environment (SITE): C-CDA Validator – USCDI v1, the health IT developer downloads the ASTP/ONC-supplied data instructions through the sender download selections of the “APIAccess_Amb” or “APIAccess_Inp” criteria and one of the API instruction documents, and then executes the download.

Demonstrate API

2. Using the ASTP/ONC-supplied API instruction document returned in step 1, and the Health IT Module's identified API functions (including the ID or token generated as part of the "Application Access – patient selection" certification criterion at § 170.315(g)(7)), the user demonstrates that the API responds to and returns all data classes expressed in the standard in § 170.213 USCDI and the data classes in § 170.215(g)(9)(i)(A)(3) in a summary record formatted in accordance with the standard adopted at § 170.205(a) (4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes with Errata, DSTU Release 2.1 and § 170.205(a)(5) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 following the CCD document template for the unique patient identified by the ID or token.
3. For each CCD document created in step 2, the user submits the CCD document to the tester for verification.
4. Based on the health IT setting(s) to be certified, the user repeats steps 1-3, for each of the ambulatory and/or inpatient care plan instruction documents found in SITE: C-CDA Validator - USCDI v1. Demonstration of the API is required for all of the API instruction documents for a given health IT setting.

All Steps (Approved SVAP Version)

- Complete steps above using SITE C-CDA Validator – USCDI v4 and;
- Reference United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata, and;
- Use HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024 for § 170.205(a)(4), (a)(5) or (a)(6).

Required by December 31, 2025

1. Using SITE: C-CDA Validator - USCDI v3, the health IT developer downloads the ASTP/ONC-supplied data instructions through the sender download selections of the "APIAccess_Amb" or "APIAccess_Inp" criteria and one of the API instruction documents, and then executes the download.

Demonstrate API

2. Using the ASTP/ONC-supplied API instruction document returned in step 1, and the Health IT Module's identified API functions (including the ID or token generated as part of the "Application Access – patient selection" certification criterion at § 170.315(g)(7)), the user demonstrates that the API responds to and returns all data classes expressed in the standard in § 170.213 USCDI and the data classes in § 170.215(g)(9)(i)(A)(3) in a summary record formatted in accordance with the standard adopted at § 170.205(a) (4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes with Errata, DSTU Release 2.1 and § 170.205(a)(6) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 4.1 following the CCD document template for the unique patient identified by the ID or token.

3. For each CCD document created in step 2, the user submits the CCD document to the tester for verification.
4. Based on the health IT setting(s) to be certified, the user repeats steps 1-3, for each of the ambulatory and/or inpatient care plan instruction documents found in SITE: C-CDA Validator - USCDI v3. Demonstration of the API is required for all of the API instruction documents for a given health IT setting.

All Steps (Approved SVAP Version)

- Complete steps above using SITE C-CDA Validator – USCDI v4 and;
- Reference United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata, and;
- Use HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024 for § 170.205(a)(4), (a)(5) or (a)(6).

Test Lab Verification

Expires on January 1, 2026

Demonstrate API

1. For each API instruction set downloaded in step 1, of the System Under Test, the tester verifies the identified API routine(s) can respond to a request for “all patient data” and return all data in the USCDI in a single document using the CCD template.
2. Using SITE: C-CDA Validator – USCDI v1, the tester uploads the submitted CCD document returned from the identified API routine(s) through the sender upload selection of the “APIAccess_Amb” or “APIAccess_Inp” criteria and file name of the API instruction document, and the tester executes the upload of the submitted file to the SITE: C-CDA Validator.
3. The tester uses the validation report produced by the SITE: C-CDA Validator in step 2, to verify it indicates passing without error to confirm the CCD document returned by the API is in a summary record formatted in accordance with the standard adopted at § 170.205(a)(4), § 170.205(a)(5), and the data classes defined in § 170.215(g)(9)(i)(A)(3) using the CCD document template.
4. As required by the ASTP/ONC-supplied API instructions with the corresponding file names as uploaded in step 2, the tester uses the ASTP/ONC-supplied API instruction document and the SITE: C-CDA Validator Message Content Report to verify the additional checks for equivalent text for the content of all section level narrative text.

Required by December 31, 2025

Demonstrate API

1. For each API instruction set downloaded in step 1, of the System Under Test, the tester verifies the identified API routine(s) can respond to a request for “all patient data” and return all data in the USCDI in a single document using the Continuity of Care Document (CCD) template.
2. Using SITE: C-CDA Validator – USCDI v3, the tester uploads the submitted CCD document returned from the identified API routine(s) through the sender upload selection of the “APIAccess_Amb” or “APIAccess_Inp” criteria and file name of the API instruction document, and the tester executes the upload of the submitted file to the SITE: C-CDA Validator.
3. The tester uses the validation report produced by the SITE: C-CDA Validator in step 2, to verify it indicates passing without error to confirm the CCD document returned by the API is in a summary record formatted in accordance with the standard adopted at § 170.205(a)(4), § 170.205(a)(6), and the data classes defined in § 170.215(g)(9)(i)(A)(3) using the CCD document template.
4. As required by the ASTP/ONC-supplied API instructions with the corresponding file names as uploaded in step 2, the tester uses the ASTP/ONC-supplied API instruction document and the SITE: C-CDA Validator Message Content Report to verify the additional checks for equivalent text for the content of all section level narrative text.

The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

System Under Test

Expires on January 1, 2026

Setup

1. Using the ASTP Standards Implementation & Testing Environment (SITE): C-CDA Validator – USCDI v1, the health IT developer downloads the ASTP/ONC-supplied data instructions through the sender download selections of the “APIAccess_Amb” or “APIAccess_Inp” criteria and one of the API instruction documents, and then executes the download.

Demonstrate API

Test Lab Verification

Expires on January 1, 2026

Demonstrate API

1. For each API instruction set downloaded in step 1, of the System Under Test, the tester verifies the identified API routine(s) can respond to a request for “all patient data” and return all data in the USCDI in a single document using the CCD template.

System Under Test

2. Using the ASTP/ONC-supplied API instruction document returned in step 1, and the Health IT Module's identified API functions (including the ID or token generated as part of the "Application Access – patient selection" certification criterion at § 170.315(g) (7)), the user demonstrates that the API responds to and returns all data classes expressed in the standard in § 170.213 USCDI and the data classes in § 170.215(g)(9)(i)(A)(3) in a summary record formatted in accordance with the standard adopted at § 170.205(a) (4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes with Errata, DSTU Release 2.1 and § 170.205(a)(5) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 2 following the CCD document template for the unique patient identified by the ID or token.
3. For each CCD document created in step 2, the user submits the CCD document to the tester for verification.
4. Based on the health IT setting(s) to be certified, the user repeats steps 1-3, for each of the ambulatory and/or inpatient care plan instruction documents found in SITE: C-CDA Validator - USCDI v1. Demonstration of the API is required for all of the API instruction documents for a given health IT setting.

All Steps (Approved SVAP Version)

- Complete steps above using SITE C-CDA Validator – USCDI v4 and;
- Reference United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata, and;
- Use HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024 for § 170.205(a)(4), (a)(5) or (a)(6).

Required by December 31, 2025

1. Using SITE: C-CDA Validator - USCDI v3, the health IT developer downloads the ASTP/ONC-supplied data instructions through the sender download selections of the "APIAccess_Amb" or "APIAccess_Inp" criteria and one of the API instruction documents, and then executes the download.

Test Lab Verification

2. Using SITE: C-CDA Validator – USCDI v1, the tester uploads the submitted CCD document returned from the identified API routine(s) through the sender upload selection of the "APIAccess_Amb" or "APIAccess_Inp" criteria and file name of the API instruction document, and the tester executes the upload of the submitted file to the SITE: C-CDA Validator.
3. The tester uses the validation report produced by the SITE: C-CDA Validator in step 2, to verify it indicates passing without error to confirm the CCD document returned by the API is in a summary record formatted in accordance with the standard adopted at § 170.205(a)(4), § 170.205(a)(5), and the data classes defined in § 170.215(g)(9)(i)(A)(3) using the CCD document template.

Demonstrate API

System Under Test

2. Using the ASTP/ONC-supplied API instruction document returned in step 1, and the Health IT Module's identified API functions (including the ID or token generated as part of the "Application Access – patient selection" certification criterion at § 170.315(g) (7)), the user demonstrates that the API responds to and returns all data classes expressed in the standard in § 170.213 USCDI and the data classes in § 170.215(g)(9)(i)(A)(3) in a summary record formatted in accordance with the standard adopted at § 170.205(a) (4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes with Errata, DSTU Release 2.1 and § 170.205(a)(6) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 4.1 following the CCD document template for the unique patient identified by the ID or token.
3. For each CCD document created in step 2, the user submits the CCD document to the tester for verification.
4. Based on the health IT setting(s) to be certified, the user repeats steps 1-3, for each of the ambulatory and/or inpatient care plan instruction documents found in SITE: C-CDA Validator - USCDI v3. Demonstration of the API is required for all of the API instruction documents for a given health IT setting.

All Steps (Approved SVAP Version)

- Complete steps above using SITE C-CDA Validator – USCDI v4 and;
- Reference United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata, and;
- Use HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024 for § 170.205(a)(4), (a)(5) or (a)(6).

Test Lab Verification

4. As required by the ASTP/ONC-supplied API instructions with the corresponding file names as uploaded in step 2, the tester uses the ASTP/ONC-supplied API instruction document and the SITE: C-CDA Validator Message Content Report to verify the additional checks for equivalent text for the content of all section level narrative text.

Required by December 31, 2025 Demonstrate API

1. For each API instruction set downloaded in step 1, of the System Under Test, the tester verifies the identified API routine(s) can respond to a request for "all patient data" and return all data in the USCDI in a single document using the Continuity of Care Document (CCD) template.

System Under Test

Test Lab Verification

2. Using SITE: C-CDA Validator – USCDI v3, the tester uploads the submitted CCD document returned from the identified API routine(s) through the sender upload selection of the “APIAccess_Amb” or “APIAccess_Inp” criteria and file name of the API instruction document, and the tester executes the upload of the submitted file to the SITE: C-CDA Validator.
3. The tester uses the validation report produced by the SITE: C-CDA Validator in step 2, to verify it indicates passing without error to confirm the CCD document returned by the API is in a summary record formatted in accordance with the standard adopted at § 170.205(a)(4), § 170.205(a)(6), and the data classes defined in § 170.215(g)(9)(i)(A) (3) using the CCD document template.

System Under Test

Test Lab Verification

4. As required by the ASTP/ONC-supplied API instructions with the corresponding file names as uploaded in step 2, the tester uses the ASTP/ONC-supplied API instruction document and the SITE: C-CDA Validator Message Content Report to verify the additional checks for equivalent text for the content of all section level narrative text.

Paragraph (g)(9)(i)(A)(3) Functional requirements – data classes

System Under Test

The following data classes are to be present and expressed within the resultant CCD document:

- The Assessment and Plan of Treatment in accordance with either the Assessment and Plan Section (V2), or both the Assessment and Plan of Treatment Sections (V2), specified in accordance with the standard specified in § 170.205(a)(4). At a minimum, the Assessment and Plan of Treatment data includes the narrative text.
- The Goals specified in accordance with the standard specified at § 170.205(a)(4). At a minimum, the Goals data includes narrative text.
- The Health Concerns specified in accordance with the standard specified at § 170.205(a)(4). At a minimum, the Health concerns data includes narrative text.

Test Lab Verification

Using visual inspection, the tester verifies the data presented in section (g)(9)(A)(1) includes:

- The Assessment and plan or both the Assessment and Plan of Treatment are specified in accordance with the standard specified in § 170.205(a)(4) as narrative text.
- The Goals are specified in accordance with the standard specified in § 170.205(a)(4) as narrative text.

- The Health Concerns are specified in accordance with the standard specified in § 170.205(a)(4) as narrative text

Note: The system must consistently and independently represent the data as discrete data that are clearly distinguishable.

System Under Test

The following data classes are to be present and expressed within the resultant CCD document:

- The Assessment and Plan of Treatment in accordance with either the Assessment and Plan Section (V2), or both the Assessment and Plan of Treatment Sections (V2), specified in accordance with the standard specified in § 170.205(a)(4). At a minimum, the Assessment and Plan of Treatment data includes the narrative text.
- The Goals specified in accordance with the standard specified at § 170.205(a)(4). At a minimum, the Goals data includes narrative text.
- The Health Concerns specified in accordance with the standard specified at § 170.205(a)(4). At a minimum, the Health concerns data includes narrative text.

Test Lab Verification

Using visual inspection, the tester verifies the data presented in section (g)(9)(A)(1) includes:

- The Assessment and plan or both the Assessment and Plan of Treatment are specified in accordance with the standard specified in § 170.205(a)(4) as narrative text.
- The Goals are specified in accordance with the standard specified in § 170.205(a)(4) as narrative text.
- The Health Concerns are specified in accordance with the standard specified in § 170.205(a)(4) as narrative text

Note: The system must consistently and independently represent the data as discrete data that are clearly distinguishable.

Paragraph (g)(9)(i)(B) Functional requirements – Respond to patient data requests with a specific date

System Under Test

1. The Health IT Module's identified API returns data to the developer-identified requesting application for a specific date that the requesting application identifies.

2. The Health IT Module's identified API returns data to the developer-identified requesting application for a specific date range that the requesting application identifies.

Test Lab Verification

1. The tester verifies the API routine(s) can respond to a request for patient data for a specific date, and that the patient data returned is accurate and without omission based upon the health IT developer's documentation for data return based upon a date request.
2. The tester verifies the API routine(s) can respond to a request for patient data for a date range, and the patient data returned is accurate and without omission based upon the health IT developer's documentation for data return based upon a date range request.

System Under Test

1. The Health IT Module's identified API returns data to the developer-identified requesting application for a specific date that the requesting application identifies.
2. The Health IT Module's identified API returns data to the developer-identified requesting application for a specific date range that the requesting application identifies.

Test Lab Verification

1. The tester verifies the API routine(s) can respond to a request for patient data for a specific date, and that the patient data returned is accurate and without omission based upon the health IT developer's documentation for data return based upon a date request.
2. The tester verifies the API routine(s) can respond to a request for patient data for a date range, and the patient data returned is accurate and without omission based upon the health IT developer's documentation for data return based upon a date range request.

Paragraph (g)(9)(ii)(A)(1) Documentation – API Syntax

System Under Test

The health IT developer supplies documentation describing the API, with the intended audience of developers, and includes at a minimum:

- API syntax;
- function names;
- required and optional parameters and their data types;
- return variables and their types/structures; and

- exceptions and exception handling methods and their returns.

Test Lab Verification

The tester verifies the identified documentation for the Health IT Module's API definition is accurate and without omission, and that it matches the version of the software release.

System Under Test

The health IT developer supplies documentation describing the API, with the intended audience of developers, and includes at a minimum:

- API syntax;
- function names;
- required and optional parameters and their data types;
- return variables and their types/structures; and
- exceptions and exception handling methods and their returns.

Test Lab Verification

The tester verifies the identified documentation for the Health IT Module's API definition is accurate and without omission, and that it matches the version of the software release.

Paragraph (g)(9)(ii)(A)(2) Documentation – Software components and configurations

System Under Test

The health IT developer supplies accompanying documentation describing the Health IT Module's API implementation requirements, with the intended audience of developers, which must include:

The software components and configurations that would be necessary for an application to implement to be able to successfully interact with the API and process its response(s).

Test Lab Verification

The tester verifies the identified documentation for interfacing with the Health IT Module's API (including both the software components and the configuration) is accurate and without omission and that it matches the version of the software release.

System Under Test

Test Lab Verification

System Under Test

The health IT developer supplies accompanying documentation describing the Health IT Module's API implementation requirements, with the intended audience of developers, which must include:

The software components and configurations that would be necessary for an application to implement to be able to successfully interact with the API and process its response(s).

Test Lab Verification

The tester verifies the identified documentation for interfacing with the Health IT Module's API (including both the software components and the configuration) is accurate and without omission and that it matches the version of the software release.

Paragraph (g)(9)(ii)(B) Documentation availability

System Under Test

The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Test Lab Verification

The tester verifies the supplied documentation is publicly accessible by hyperlink.

System Under Test

The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Test Lab Verification

The tester verifies the supplied documentation is publicly accessible by hyperlink.

Archived Version:

§ 170.315(g)(9) Application access — all data request TP

Updated on 03-27-2025

Regulation Text

Regulation Text

§ 170.315 (g)(9) *Application access – all data request—*

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

1. *Functional requirements.*

1.

1. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section for the time period up to and including December 31, 2025, or
2. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (6) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section.

3. The following data classes:

1. *Assessment and plan of treatment.* In accordance with the “Assessment and Plan Section (V2)” of the standards specified in § 170.205(a)(4); or in accordance with the “Assessment Section (V2)” and “Plan of Treatment Section (V2)” of the standards specified in § 170.205(a)(4).
2. *Goals.* In accordance with the “Goals Section” of the standard specified in § 170.205(a)(4).
3. *Health concerns.* In accordance with the “Health Concerns Section” of the standard specified in § 170.205(a)(4).
4. *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the “Product Instance” in the “Procedure Activity Procedure Section” of the standard specified in § 170.205(a)(4).

2. Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

2. Documentation—

1. The API must include accompanying documentation that contains, at a minimum:
 1. API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
 2. The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
2. The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(9)(i)(A)

§ 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)

§ 170.205(a)(4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015, June 2019 (with Errata)

§ 170.205(a)(5) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 2, October 2019 (Adoption of this standard expires on January 1, 2026)

§ 170.205(a)(6) Health Level 7 (HL7®) CDA R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 4.1 - US Realm (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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

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 must update their certification to the newer versions of USCDI and C-CDA Companion Guide as outlined in paragraphs (g)(9)(i)(A)(1-2).

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.
- Consolidated CDA creation performance (§ 170.315(g)(6)): Consolidated Clinical Document Architecture (C-CDA) creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA Creation Performance CCG for more details.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(9). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to this 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 criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “View, download and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging”, which are explicitly stated.

For more information on the approaches to meet these Privacy and Security requirements, please review the [Privacy and Security CCG](#).

- If choosing Approach 1:
 - [Authentication, access control, and authorization \(§ 170.315\(d\)\(1\)\)](#)
 - [Trusted connection \(§ 170.315\(d\)\(9\)\)](#)
 - Either [auditable events and tamper-resistance \(§ 170.315\(d\)\(2\)\)](#) or [auditing actions on health information \(§ 170.315\(d\)\(10\)\)](#).
 - [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
1.1	Updated test tool link	12-02-2024

Version #	Description of Change	Version Date
1.2	Updated test steps with 2024 SVAP approved standards and new SITE UI language	03-21-2025

Regulation Text

Regulation Text

§ 170.315 (g)(9) *Application access – all data request—*

The following technical outcome and conditions must be met through the demonstration of an application programming interface.

1. *Functional requirements.*

1.

1. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (5) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section for the time period up to and including December 31, 2025, or
2. Respond to requests for patient data (based on an ID or other token) for all of the data classes expressed in the standards in § 170.213 at one time and return such data (according to the specified standards, where applicable) in a summary record formatted in accordance with § 170.205(a)(4) and (6) following the CCD document template, and as specified in paragraphs (g) (9)(i)(A)(3)(i) through (iv) of this section.
3. The following data classes:
 1. *Assessment and plan of treatment.* In accordance with the “Assessment and Plan Section (V2)” of the standards specified in § 170.205(a)(4); or in accordance with the “Assessment Section (V2)” and “Plan of Treatment Section (V2)” of the standards specified in § 170.205(a)(4).
 2. *Goals.* In accordance with the “Goals Section” of the standard specified in § 170.205(a)(4).
 3. *Health concerns.* In accordance with the “Health Concerns Section” of the standard specified in § 170.205(a)(4).
 4. *Unique device identifier(s) for a patient's implantable device(s).* In accordance with the “Product Instance” in the “Procedure Activity Procedure Section” of the standard specified in § 170.205(a)(4).

2. Respond to requests for patient data associated with a specific date as well as requests for patient data within a specified date range.

2. *Documentation—*

1. The API must include accompanying documentation that contains, at a minimum:
 1. API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
 2. The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
2. The documentation used to meet paragraph (g)(9)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(9)(i)(A)

§ 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)

§ 170.205(a)(4) HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015, June 2019 (with Errata)

§ 170.205(a)(5) HL7® CDA® R2 IG: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 2, October 2019 (Adoption of this standard expires on January 1, 2026)

§ 170.205(a)(6) Health Level 7 (HL7®) CDA R2 IG: C-CDA Templates for Clinical Notes R2.1 Companion Guide, Release 4.1 - US Realm (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

HL7® CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes Edition 3.0 - US Realm, May 2024

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

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 must update their certification to the newer versions of USCDI and C-CDA Companion Guide as outlined in paragraphs (g)(9)(i)(A)(1-2).

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.
- Consolidated CDA creation performance (§ 170.315(g)(6)): Consolidated Clinical Document Architecture (C-CDA) creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA Creation Performance CCG for more details.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(g)(9). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to this 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 criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) “View, download and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging”, which are explicitly stated.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- If choosing Approach 1:
 - Authentication, access control, and authorization (§ 170.315(d)(1)).
 - Trusted connection (§ 170.315(d)(9)).
 - Either auditable events and tamper-resistance (§ 170.315(d)(2)) or auditing actions on health information (§ 170.315(d)(10)).
 - 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
1.1	Standards Referenced updated to reflect 2024 Approved SVAP Standards.	08-19-2024
1.2	For entire criterion, added clarification regarding compliance with EO 14168 and OPM guidance	03-27-2025

Testing

Testing Tool

Standards Implementation & Testing Environment (SITE): C-CDA Validators

Test Tool Documentation

Test Tool Supplemental Guide

Criterion Subparagraph	Test Data
-------------------------------	------------------

Criterion Subparagraph	Test Data
(g)(9)(i)	Inpatient setting: - 170.315_g9_api_access_inp_sample*.docx (All Samples)

Ambulatory setting - 170.315_g9_api_access_amb_sample*.docx (All Samples)

Certification Companion Guide: Application access — all data request

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.

<u>Base EHR Definition</u>	<u>Real World Testing</u>	<u>Insights Condition</u>	<u>SVAP</u>	<u>Requires Updates</u>
Included	Yes	No	Yes	Yes

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- **Security:**
 - For the purposes of certification there is no conformance requirement related to the registration of third-party applications that use the application programming interfaces (APIs). If a Health IT module requires registration as a pre-condition for accessing the APIs, then, the process must be clearly specified in the API documentation as required by the criterion. We strongly believe that registration should not be used to block information sharing via APIs.
 - This criterion does not currently include any security requirements beyond the privacy and security approach detailed above, but ONC encourages organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate. ONC expects health IT developers to include information on how to securely use their APIs in the public documentation required by the certification criteria and follow industry best practices. [see also [80 FR 62676](#) and [85 FR 25642](#)]
 - ONC strongly encourages developers to build security into their APIs following industry best practice. [see also [80 FR 62677](#)]
 - A “trusted connection” means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, ONC does not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also [80 FR 62676](#)]
 - APIs could be used when consent or authorization by an individual is required. In circumstances where there is a requirement to document a patient’s request or particular preferences, APIs can enable compliance with documentation requirements. The Health Insurance Portability and Accountability Act of 1996 Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E) permits the use of electronic documents to qualify as writings for the purpose of proving signature, e.g., electronic signatures. [see also [80 FR 62677](#)]
- The audit record should be able to distinguish the specific user who accessed the data using a third-party application through the certified API to meet the requirements of § 170.315(d)(2) or (d)(10).
- A health IT developer must demonstrate the API functionality of the Health IT Module properly performs consistent with this certification criterion’s requirements. As part of the demonstration process, a health IT developer is permitted, but is not limited, to using existing tools for creating its own app or “client” to interact with the API or using a third-party application for demonstration.
- By requiring that documentation and terms of use be open and transparent to the public by requiring a hyperlink to such documentation to be published with the product on the ONC Certified Health IT Product List, ONC hopes to encourage an open ecosystem of diverse and innovative applications that can successfully and easily interact with different Health IT Modules’ APIs. [see also [80 FR 62679](#) and [85 FR 25642](#)]

- By no later than April 5, 2021, a Certified API Developer with Health IT Module(s) certified to the certification criteria in § 170.315(g)(7) or (9) must comply with paragraph (a) of this section, including revisions to their existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.
- 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:

- **Security:**
 - For the purposes of certification there is no conformance requirement related to the registration of third-party applications that use the application programming interfaces (APIs). If a Health IT module requires registration as a pre-condition for accessing the APIs, then, the process must be clearly specified in the API documentation as required by the criterion. We strongly believe that registration should not be used to block information sharing via APIs.
 - This criterion does not currently include any security requirements beyond the privacy and security approach detailed above, but ONC encourages organizations to follow security best practices and implement security controls, such as penetration testing, encryption, audits, and monitoring as appropriate. ONC expects health IT developers to include information on how to securely use their APIs in the public documentation required by the certification criteria and follow industry best practices. [see also [80 FR 62676](#) and [85 FR 25642](#)]
 - ONC strongly encourages developers to build security into their APIs following industry best practice. [see also [80 FR 62677](#)]
 - A “trusted connection” means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, ONC does not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion. [see also [80 FR 62676](#)]
 - APIs could be used when consent or authorization by an individual is required. In circumstances where there is a requirement to document a patient’s request or particular preferences, APIs can enable compliance with documentation requirements. The Health Insurance Portability and Accountability Act of 1996 Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E) permits the use of electronic documents to qualify as writings for the purpose of proving signature, e.g., electronic signatures. [see also [80 FR 62677](#)]
- The audit record should be able to distinguish the specific user who accessed the data using a third-party application through the certified API to meet the requirements of § 170.315(d)(2) or (d)(10).
- A health IT developer must demonstrate the API functionality of the Health IT Module properly performs consistent with this certification criterion’s requirements. As part of the demonstration process, a health IT developer is permitted, but is not limited, to using existing tools for creating its own app or “client” to interact with the API or using a third-party application for demonstration.
- By requiring that documentation and terms of use be open and transparent to the public by requiring a hyperlink to such documentation to be published with the product on the ONC Certified Health IT Product List, ONC hopes to encourage an open ecosystem of diverse and innovative applications that can successfully and easily interact with different Health IT Modules’ APIs. [see also [80 FR 62679](#) and [85 FR 25642](#)]
- By no later than April 5, 2021, a Certified API Developer with Health IT Module(s) certified to the certification criteria in § 170.315(g)(7) or (9) must comply with paragraph (a) of this section, including revisions to their existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

- 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 (g)(9)(i)(A) Functional requirements

Technical outcome – The API must be able to respond to requests for patient data (using an ID or other token) for all of the data categories specified in the United States Core Data for Interoperability Standard (USCDI) at one time in a summary record formatted according to the C-CDA Release 2.1 Continuity of Care Document (CCD) template.

Clarifications:

- Please refer to the USCDI for the data standards that are required.
- The technology specifications should be designed and implemented in such a way as to return meaningful responses to queries, particularly with regard to exceptions and exception handling, and should make it easy for applications to discover what data exists for the patient. [see also [80 FR 62678](#)]
- The term “token” that is used here is not to be interpreted as the token in the OAuth2 workflow, but simply as something that would uniquely identify a patient.

- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see also [Health IT Certification Program Overview](#)] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There will be a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., C-CDA 2.1 Validator). There will be an 18-month delay before a finding of a correction's absence in certified health IT during surveillance would constitute a non-conformity under the Certification Program.

Technical outcome – The API must be able to respond to requests for patient data (using an ID or other token) for all of the data categories specified in the United States Core Data for Interoperability Standard (USCDI) at one time in a summary record formatted according to the C-CDA Release 2.1 Continuity of Care Document (CCD) template.

Clarifications:

- Please refer to the USCDI for the data standards that are required.
- The technology specifications should be designed and implemented in such a way as to return meaningful responses to queries, particularly with regard to exceptions and exception handling, and should make it easy for applications to discover what data exists for the patient. [see also [80 FR 62678](#)]
- The term “token” that is used here is not to be interpreted as the token in the OAuth2 workflow, but simply as something that would uniquely identify a patient.
- In order to mitigate potential interoperability errors and inconsistent implementation of the HL7® Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes, Draft Standard for Trial Use, Release 2.1, ONC assesses, approves, and incorporates corrections as part of required testing and certification to this criterion. [see also [Health IT Certification Program Overview](#)] Certified health IT adoption and compliance with the following corrections are necessary because they implement updates to vocabularies, update rules for cardinality and conformance statements, and promote proper exchange of C-CDA documents. There will be a 90-day delay from the time the CCG has been updated with the ONC-approved corrections to when compliance with the corrections will be required to pass testing (i.e., C-CDA 2.1 Validator). 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.

Paragraph (g)(9)(i)(B) Functional requirements

Technical outcome – The API must be able to respond to requests for patient data associated with a specific date as well as with a specific date range.

Clarifications:

- Health IT returning an entire patient record that does not reflect the specific date or date range requested is not permissible when a specific date or date range is requested. [see also [80 FR 62678](#)]
- The health IT developer can determine the method and the amount of data by which the health IT uniquely identifies a patient. [see also [80 FR 62678](#)]
- The API must be able to send, at minimum all required data for a specified date range(s). ONC acknowledges that there will be organizational policies and/or safety best practices that will dictate additional data to be sent and when data is considered complete and/or ready for being sent. This should be appropriately described in the API documentation.
- The approach used to provide the CCD document(s) is set by the API. An approach based on providing one or more CCD documents matching to the patient's selected date or date range is a valid approach.

Technical outcome – The API must be able to respond to requests for patient data associated with a specific date as well as with a specific date range.

Clarifications:

- Health IT returning an entire patient record that does not reflect the specific date or date range requested is not permissible when a specific date or date range is requested. [see also [80 FR 62678](#)]
- The health IT developer can determine the method and the amount of data by which the health IT uniquely identifies a patient. [see also [80 FR 62678](#)]
- The API must be able to send, at minimum all required data for a specified date range(s). ONC acknowledges that there will be organizational policies and/or safety best practices that will dictate additional data to be sent and when data is considered complete and/or ready for being sent. This should be appropriately described in the API documentation.
- The approach used to provide the CCD document(s) is set by the API. An approach based on providing one or more CCD documents matching to the patient's selected date or date range is a valid approach.

Paragraph (g)(9)(ii)(A) Documentation

Technical outcome – The API must include accompanying documentation which contains, at a minimum:

- API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
- Software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s); and
- The terms of use for the API, including, at a minimum, any associated developer policies and required developer agreements.

Clarifications:

No additional clarifications.

Technical outcome – The API must include accompanying documentation which contains, at a minimum:

- API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
- Software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s); and
- The terms of use for the API, including, at a minimum, any associated developer policies and required developer agreements.

Clarifications:

No additional clarifications.

Paragraph (g)(9)(ii)(B) Documentation

Technical outcome – The documentation used to meet the provisions in (g)(9)(ii)(A)(1)-(3) must be available through a publicly accessible hyperlink.

Clarifications:

- The hyperlink provided for all of the documentation referenced by provision (g)(9)(ii)(A) must reflect the most current version of the health IT developer's documentation.
- All the documentation referenced by provision (g)(9)(ii)(A) must be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, "click-through" agreements, or requirement to provide contact details or other information prior to accessing the documentation.

Technical outcome – The documentation used to meet the provisions in (g)(9)(ii)(A)(1)-(3) must be available through a publicly accessible hyperlink.

Clarifications:

- The hyperlink provided for all of the documentation referenced by provision (g)(9)(ii)(A) must reflect the most current version of the health IT developer's documentation.
- All the documentation referenced by provision (g)(9)(ii)(A) must be accessible to the public via a hyperlink without additional access requirements, including, without limitation, any form of registration, account creation, “click-through” agreements, or requirement to provide contact details or other information prior to accessing the documentation.

Archived Version:

§ 170.315(g)(9) Application access — all data request CCG