HealthIT.gov

§170.315(g)(10) Standardized API for patient and population services

Test Procedure

Updated on 08-12-2024

Regulation Text

Regulation Text

§ 170.315(g)(10) *Standardized API for patient and population services—*

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

(i) *Data response*.

(A) Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a) and in § 170.215(b)(1), including the mandatory capabilities described in "US Core Server CapabilityStatement," for each of the data included in the standards adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standards and implementation specifications adopted in § 170.215(a), (b)(1), and (d), for each of the data included in the standards adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(ii) *Supported search operations*.

(A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specifications adopted in § 170.215(b)(1), specifically the mandatory capabilities described in "US Core Server CapabilityStatement."

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).

(iii) *Application registration*. Enable an application to register with the Health IT Module's "authorization server."

(iv) *Secure connection*.

(A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(b)(1) and (c).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(d).

(v) *Authentication and authorization.*

(A) *Authentication and authorization for patient and user scopes.*

(1) First time connections.

(i) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(c) and standard adopted in § 170.215(e).

(ii) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).

(iii) A Health IT Module's authorization server must issue a refresh token for a period of no less than three months to native applications capable of securing a refresh token.

(2) Subsequent connections.

(i) Access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(c) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

HealthIT.gov

process of granting an application access to patient data in accordance with the "SMART Backend Services: Authorization Guide" section of the implementation specification adopted in § 170.215(d) and the application must be issued a valid access token.

(vi) *Patient authorization revocation.* A Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request.

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with an implementation specification in § 170.215(c).

(viii) *Documentation*.

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported 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).

(3) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(B) The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

Standard(s) Referenced

Paragraph (g)(10)(i)(A)

§ 170.215(a)(1) Health Level 7 (HL7®) Version 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, October 30, 2019

§ 170.215(b)(1)(i) HL7®FHIR® US Core Implementation Guide STU V3.1.1 (Adoption of this standard expires on January 1, 2026)

§ 170.215(b)(1)(ii) HL7® FHIR® US Core Implementation Guide STU 6.1.0 (This standard is required by December 31, 2025)

§ 170.213(a) United States Core Data for Interoperability (USCDI), Version 1 (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)

Paragraph (g)(10)(i)(B)

§ 170.215(a)(1) HL7® Version 4.0.1 FHIR® Release 4, October 30, 2019

§ 170.215(b)(1)(i) HL7®FHIR® US Core Implementation Guide STU V3.1.1 (Adoption of this standard expires on January 1, 2026)

§ 170.215(b)(1)(ii) HL7® FHIR® US Core Implementation Guide STU 6.1.0 (This standard is required by December 31, 2025)

§ 170.213(a) United States Core Data for Interoperability (USCDI), Version 1 (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)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(ii)(A)

HealthIT.gov

Paragraph (g)(10)(ii)(B)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(iii)

None

Paragraph (g)(10)(iv)(A)

§ 170.215(b)(1)(i) HL7®FHIR® US Core Implementation Guide STU V3.1.1 (Adoption of this standard expires on January 1, 2026)

§ 170.215(b)(1)(ii) HL7 FHIR® US Core Implementation Guide STU 6.1.0 (This standard is required by December 31, 2025)

§ 170.215(c)(1) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (Adoption of this standard expires on January 1, 2026)

§ 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities," excepting the "permission-online" capability; "Token Introspection" as defined in "7 Token Introspection" (This standard is required by December 31, 2025)

Paragraph (g)(10)(iv)(B)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(v)(A)(1)

§ 170.215(c)(1) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (Adoption of this standard expires on January 1, 2026)

§ 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities," excepting the "permission-online" capability; "Token Introspection" as defined in "7 Token Introspection" (This standard is required by December 31, 2025)

§ 170.215(e)(1) OpenID Connect Core 1.0 incorporating errata set 1

Paragraph (g)(10)(v)(A)(2)

§ 170.215(c)(1) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (Adoption of this standard expires on January 1, 2026)

§ 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities," excepting the "permission-online" capability; "Token Introspection" as defined in "7 Token Introspection" (This standard is required by December 31, 2025.)

Paragraph (g)(10)(v)(B)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(vi)

HealthIT.gov

None

Paragraph (g)(10)(viii)

None

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

HL7® FHIR® US Core Implementation Guide STU 4.0.0, June 2021 (Adoption of this standard expires on January 1, 2026)

HL7® FHIR® US Core Implementation Guide STU 7.0.0, May 2024

HL7® FHIR® Bulk Data Access (Flat FHIR®) (v2.0.0: STU 2), November 26, 2021
HL7® FHIR® SMART Application Launch Framework Implementation Guide Release 2.2.0, April 30, 2024
United States Core Data for Interoperability (USCDI), Version 4, October 2023 Errata

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

Required Update Deadlines

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

Deadline: By March 11, 2024

Actions to be taken: Developers must support the new patient access revocation requirements detailed in subparagraph (g)(10)(vi).

Deadline: December 31, 2024

Actions to be taken: Developers must publish service base URLs and related organization details according to the API Maintenance of Certification requirements at § 170.404(b)(2).

Deadline: December 31, 2025

Actions to be taken: Developers must update functionality to the newly required versions of the US Core and SMART App Launch implementation guides detailed at § 170.215(b)(1) and § 170.215(c) respectively. Developers must also support standardized token introspection as detailed in subparagraph (g)(10)(vii).

Certification Dependencies

Conditions and Maintenance of Certification

API: Products certified to this criterion have specific requirements related to the certification of API Modules

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

HealthIT.gov

- Use of FHIR bulk data access through certified health IT

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, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.

Privacy & Security Requirements

This certification criterion was adopted in § 170.315(g)(10). 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.

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 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	Clarified in the “Required Update Deadlines” that the new patient access revocation requirements introduced in HTI-1 Final Rule for	05-16-2024

HealthIT.gov

	removed duplicate text for AUT-PAT-25 and clarified for AUT-PAT-28 specific components are only applicable if using the specified version of the US Core implementation guide.	

Regulation Text

Regulation Text

§ 170.315(g)(10) *Standardized API for patient and population services—*

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

(i) *Data response*.

(A) Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a) and in § 170.215(b)(1), including the mandatory capabilities described in "US Core Server CapabilityStatement," for each of the data included in the standards adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standards and implementation specifications adopted in § 170.215(a), (b)(1), and (d), for each of the data included in the standards adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(ii) *Supported search operations*.

(A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specifications adopted in § 170.215(b)(1), specifically the mandatory capabilities described in "US Core Server CapabilityStatement."

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).

(iii) *Application registration*. Enable an application to register with the Health IT Module's "authorization server."

(iv) *Secure connection*.

(A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(b)(1) and (c).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(d).

(v) *Authentication and authorization.*

(A) *Authentication and authorization for patient and user scopes.*

(1) First time connections.

(i) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(c) and standard adopted in § 170.215(e).

(ii) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).

(iii) A Health IT Module's authorization server must issue a refresh token for a period of no less than three months to native applications capable of securing a refresh token.

(2) Subsequent connections.

(i) Access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(c) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

HealthIT.gov

the process of granting an application access to patient data in accordance with the "SMART Backend Services: Authorization Guide" section of the implementation specification adopted in § 170.215(d) and the application must be issued a valid access token.

(vi) *Patient authorization revocation.* A Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request.

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued in accordance with an implementation specification in § 170.215(c).

(viii) *Documentation*.

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported 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).

(3) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(B) The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

Standard(s) Referenced

Paragraph (g)(10)(i)(A)

§ 170.215(a)(1) Health Level 7 (HL7®) Version 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, October 30, 2019

§ 170.215(b)(1)(i) HL7®FHIR® US Core Implementation Guide STU V3.1.1 (Adoption of this standard expires on January 1, 2026)

§ 170.215(b)(1)(ii) HL7® FHIR® US Core Implementation Guide STU 6.1.0 (This standard is required by December 31, 2025)

§ 170.213(a) United States Core Data for Interoperability (USCDI), Version 1 (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)

Paragraph (g)(10)(i)(B)

§ 170.215(a)(1) HL7® Version 4.0.1 FHIR® Release 4, October 30, 2019

§ 170.215(b)(1)(i) HL7®FHIR® US Core Implementation Guide STU V3.1.1 (Adoption of this standard expires on January 1, 2026)

§ 170.215(b)(1)(ii) HL7® FHIR® US Core Implementation Guide STU 6.1.0 (This standard is required by December 31, 2025)

§ 170.213(a) United States Core Data for Interoperability (USCDI), Version 1 (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)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(ii)(A)

HealthIT.gov

Paragraph (g)(10)(ii)(B)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(iii)

None

Paragraph (g)(10)(iv)(A)

§ 170.215(b)(1)(i) HL7®FHIR® US Core Implementation Guide STU V3.1.1 (Adoption of this standard expires on January 1, 2026)

§ 170.215(b)(1)(ii) HL7 FHIR® US Core Implementation Guide STU 6.1.0 (This standard is required by December 31, 2025)

§ 170.215(c)(1) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (Adoption of this standard expires on January 1, 2026)

§ 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities," excepting the "permission-online" capability; "Token Introspection" as defined in "7 Token Introspection" (This standard is required by December 31, 2025)

Paragraph (g)(10)(iv)(B)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(v)(A)(1)

§ 170.215(c)(1) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (Adoption of this standard expires on January 1, 2026)

§ 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities," excepting the "permission-online" capability; "Token Introspection" as defined in "7 Token Introspection" (This standard is required by December 31, 2025)

§ 170.215(e)(1) OpenID Connect Core 1.0 incorporating errata set 1

Paragraph (g)(10)(v)(A)(2)

§ 170.215(c)(1) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (Adoption of this standard expires on January 1, 2026)

§ 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0, including mandatory support for the "Capability Sets" of "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch"; all "Capabilities" as defined in "8.1.2 Capabilities," excepting the "permission-online" capability; "Token Introspection" as defined in "7 Token Introspection" (This standard is required by December 31, 2025.)

Paragraph (g)(10)(v)(B)

§ 170.215(d)(1) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(vi)

HealthIT.gov

None

Paragraph (g)(10)(viii)

None

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

HL7® FHIR® US Core Implementation Guide STU 4.0.0, June 2021 (Adoption of this standard expires on January 1, 2026)

HL7® FHIR® US Core Implementation Guide STU 7.0.0, May 2024

HL7® FHIR® Bulk Data Access (Flat FHIR®) (v2.0.0: STU 2), November 26, 2021

HL7® FHIR® SMART Application Launch Framework Implementation Guide Release 2.2.0, April 30, 2024

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

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

Required Update Deadlines

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

Deadline: By March 11, 2024

Actions to be taken: Developers must support the new patient access revocation requirements detailed in subparagraph (g)(10)(vi).

Deadline: December 31, 2024

Actions to be taken: Developers must publish service base URLs and related organization details according to the API Maintenance of Certification requirements at § 170.404(b)(2).

Deadline: December 31, 2025

Actions to be taken: Developers must update functionality to the newly required versions of the US Core and SMART App Launch implementation guides detailed at § 170.215(b)(1) and § 170.215(c) respectively. Developers must also support standardized token introspection as detailed in subparagraph (g)(10)(vii).

Certification Dependencies

Conditions and Maintenance of Certification

API: Products certified to this criterion have specific requirements related to the certification of API Modules

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

Insights: Products certified to this criterion must submit responses for the following measures:

- Individuals' access to electronic health information through certified health IT

HealthIT.gov

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, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.

Privacy & Security Requirements

This certification criterion was adopted in § 170.315(g)(10). 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.

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 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

ONC Certification (g)(10) Standardized API Test Kit using Inferno Framework

Test Tool Documentation

ONC Certification (g)(10) Standardized API Test Kit User's Guide

ONC Certification (g)(10) Standardized API Test Kit Local Installation Instruction

HealthIT.gov

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024
1.1	Clarified in the “Required Update Deadlines” that the new patient access revocation requirements introduced in HTI-1 Final Rule for paragraph (g)(10)(vi) are required by March 11, 2024.	05-16-2024
1.2	For Paragraph (g)(10)(v)(A), removed duplicate text for AUT-PAT-25 and clarified for AUT-PAT-28 specific components are only applicable if using the specified version of the US Core implementation guide.	08-12-2024

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 steps are listed to reflect the order in which the tests should take place.

Testing components

			ONC Supplied Test Data	SVAP

HealthIT.gov

Required by December 31, 2025

A health IT developer of a Health IT Module currently certified to the § 170.315(g)(10) "Standardized API for patient and population services" criterion will attest directly to the ONC-ACB to conformance with the updated § 170.315(g)(10) 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)(10) "Standardized API for patient and population services" criterion attests conformance to § 170.315(g)(10) criterion update requirements.

Paragraph (g)(10)(iii) – Application registration

System Under Test

Applies to all applicable base regulatory and SVAP standards

Application Registration

1. APP-REG-1: The health IT developer demonstrates the Health IT Module supports application registration with an authorization server for the purposes of Electronic Health Information (EHI) access for single patients, including support for application registration functions to enable authentication and authorization in § 170.315(g)(10)(v).
2. APP-REG-2: The health IT developer demonstrates the Health IT Module supports application registration with an authorization server for the purposes of EHI access for multiple patients including support for application registration functions to enable authentication and authorization in § 170.315(g)(10)(v).

Test Lab Verification

Applies to all applicable base regulatory and SVAP standards

Application Registration

1. APP-REG-1: The tester verifies the Health IT Module supports application registration with an authorization server for the purposes of EHI access for single patients, including support for application registration functions to enable authentication and authorization in § 170.315(g)(10)(v).
2. APP-REG-2: The tester verifies the Health IT Module supports application registration with an authorization server for the purposes of EHI access for multiple patients including support for application registration functions to enable authentication and authorization in § 170.315(g)(10)(v).

HealthIT.gov

Certification Option: Applies to all applicable base regulatory and SVAP standards

Secure Connection

1. SEC-CNN-1: For all transmissions between the Health IT Module and the application, the health IT developer demonstrates the use of a secure and trusted connection in accordance with an implementation specification adopted in § 170.215(b)(1) and § 170.215(c), including:
   - Using TLS version 1.2 or higher; and
   - Conformance to FHIR® Communications Security requirements.

Test Lab Verification

Certification Option: Applies to all applicable base regulatory and SVAP standards

Secure Connection

1. SEC-CNN-1: For all transmissions between the Health IT Module and the application, the tester verifies the use of a secure and trusted connection in accordance with an implementation specification adopted in § 170.215(b)(1) and § 170.215(c), including:
   - Using TLS version 1.2 or higher; and
   - Conformance to FHIR® Communications Security requirements.

HealthIT.gov

Expires on January 1, 2026: SMART App Launch 1.0.0

Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-1: The health IT developer demonstrates the ability of the Health IT Module to support the following for "EHR-Launch," "Standalone-Launch," and "Both" ("EHR-Launch" and "Standalone-Launch") as specified in the implementation specification adopted in § 170.215(c)(1).
2. AUT-PAT-2: [EHR-Launch] The health IT developer demonstrates the ability of the Health IT Module to initiate a "launch sequence" using the "launch-ehr" "SMART on FHIR® Core Capability" SMART EHR Launch mode detailed in the implementation specification adopted in § 170.215(c)(1), including:
   - Launching the registered launch URL of the application; and
   - Passing the parameters: "iss" and "launch".
3. AUT-PAT-3: [Standalone-Launch] The health IT developer demonstrates the ability of the Health IT Module to launch using the "launch-standalone" "SMART on FHIR® Core Capability" SMART Standalone Launch mode detailed in the implementation specification adopted in § 170.215(c)(1).
4. AUT-PAT-4: [Standalone-Launch] The health IT developer demonstrates the ability of the Health IT Module to support SMART's public client profile.
5. AUT-PAT-5: [Both] The health IT developer demonstrates the ability of the Health IT Module to support the following as detailed in the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(a)(1):
   - The ".well-known/smart-configuration" path; and
   - A FHIR® "CapabilityStatement".
6. AUT-PAT-6: [Both] The health IT developer demonstrates the ability of the ".well-known/smart-configuration" path to support at least the following as detailed in the implementation specification adopted in § 170.215(c)(1):
   - "authorization_endpoint";
   - "token_endpoint"; and
   - "capabilities" (including support for all the "SMART on FHIR® Core Capabilities").
7. AUT-PAT-7: [Both] The health IT developer demonstrates the ability of the FHIR® "CapabilityStatement" to support at least the following components as detailed in the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(a)(1), including:
   - "authorize"; and
   - "token".
8. AUT-PAT-8: [Both] The health IT developer demonstrates the ability of the Health IT Module to receive an authorization request according to the implementation specification adopted in § 170.215(c)(1), including support for the following parameters:
   - "response_type";
   - "client_id";
   - "redirect_uri";
   - "launch" (for EHR-Launch mode only);
   - "scope";
   - "state"; and
   - "aud".
9. AUT-PAT-9: [Both] The health IT developer demonstrates the ability of the Health IT Module to support the receipt of the following scopes and capabilities according to the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(e)(1):
   - "openid" (to support "sso-openid-connect" "SMART on FHIR® Core Capability");
   - "fhirUser" (to support "sso-openid-connect" "SMART on FHIR® Core Capability");
   - "need_patient_banner" (to support "context-banner" "SMART on FHIR® Core Capability" for EHR-Launch mode only);
   - "smart_style_url" (to support "context-style" "SMART on FHIR® Core Capability" for EHR-Launch mode only);

HealthIT.gov

- Patient-level scopes (to support “permission-patient” “SMART on FHIR® Core Capability”); and
- User-level scopes (to support “permission-user” “SMART on FHIR® Core Capability”).

10. AUT-PAT-10: [Both] The health IT developer demonstrates the ability of the Health IT Module to evaluate the authorization request and request end-user input, if applicable (required for patient-facing applications), including the ability for the end-user to authorize an application to receive EHI based on FHIR® resource-level scopes for all of the FHIR® resources associated with the profiles specified in a standard adopted in § 170.213 and the corresponding implementation specification adopted in § 170.215(b)(1).
If using US Core 3.1.1, 4.0.0, or 6.1.0 these resources include:

- “AllergyIntolerance”;
- “CarePlan”;
- “CareTeam”;
- “Condition”;
- “Device”;
- “DiagnosticReport”;
- “DocumentReference”;
- “Goal”;
- “Immunization”;
- “Medication” (if supported);
- “MedicationRequest”;
- “Observation”;
- “Patient”;
- “Procedure”; and
- “Provenance”.

The following resources must also be supported if using US Core 6.1.0:

- “Encounter”
- “Coverage”
- “Specimen”
- “MedicationDispense”
- “RelatedPerson”; and
- “ServiceRequest”

11. AUT-PAT-11: [Both] The health IT developer demonstrates the ability of the Health IT Module to evaluate the authorization request and request end-user input, if applicable (required for patient-facing applications), including either the ability for the end-user to explicitly enable / disable the “offline_access” scope or information communicating the application’s request for the “offline_access” scope.
12. AUT-PAT-12: [Both] The health IT developer demonstrates the ability of the Health IT Module to deny an application’s authorization request according to a patient’s preferences selected in AUT-PAT-10, and AUT-PAT-11, of this section in accordance with the implementation specification adopted in § 170.215(c)(1).
13. AUT-PAT-13: [Both] The health IT developer demonstrates the ability of the Health IT Module to return an error response if the "aud" parameter provided by an application to the Health IT Module in AUT-PAT-8, is not a valid FHIR® resource server associated with the Health IT Module's authorization server.
14. AUT-PAT-14: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant an application access to EHI by returning an authorization code to the application according to the implementation specification adopted in § 170.215(c)(1), including the following parameters:

- “code”; and
- “state”.

15. AUT-PAT-15: [Both] The health IT developer demonstrates the ability of the Health IT Module to receive the following parameters from an application according to the implementation specification adopted in § 170.215(c)(1):

- “grant_type”;
- “code”;

HealthIT.gov

16. AUT-PAT-16: [Both] The health IT developer demonstrates the ability of the Health IT Module to return a JSON object to applications according to the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(e)(1), including the following:
    - “access_token”;
    - “token_type”;
    - “scope”;
    - “id_token”;
    - “refresh_token” (valid for a period of no shorter than three months);
    - HTTP “Cache-Control” response header field with a value of “no-store”;
    - HTTP “Pragma” response header field with a value of “no-cache”;
    - “patient” (to support “context-ehr-patient” and “context-standalone-patient” “SMART on FHIR® Core Capabilities”);
    - “need_patient_banner” (to support “context-banner” “SMART on FHIR® Core Capability” for EHR-Launch mode only); and
    - “smart_style_url” (to support “context-style” “SMART on FHIR® Core Capability” for EHR-Launch mode only).

    Additionally, the following must be supported if using US Core 6.1.0:

    - “encounter” (to support "context-ehr-encounter" “SMART on FHIR® Capability”)
17. AUT-PAT-17: [Both] The health IT developer demonstrates the ability of the Health IT Module to provide an OpenID Connect well-known URI in accordance with the implementation specification adopted in § 170.215(e)(1), including:
    - All required fields populated according to implementation specification adopted in § 170.215(e)(1); and
    - Valid JWKS populated according to implementation specification can be retrieved via JWKS URI.
18. AUT-PAT-18: [Both] The health IT developer demonstrates the ability of the Health IT Module to deny an application’s authorization request in accordance with the implementation specification adopted in § 170.215(c)(1).
19. AUT-PAT-19: [Both] The health IT developer demonstrates the ability of the Health IT Module to return a “Patient” FHIR® resource that matches the patient context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
20. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 6.1.0: The health IT developer demonstrates the ability of the Health IT Module to return an “Encounter” FHIR® resource that matches the encounter context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
21. AUT-PAT-20: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant an access token when a refresh token is supplied according to an implementation specification adopted in § 170.215(b)(1).
22. AUT-PAT-21: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant a refresh token valid for a period of no less than three months to native applications capable of securing a refresh token.

Subsequent Connections: Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-22: The health IT developer demonstrates the ability of the Health IT Module to issue a refresh token valid for a new period of no shorter than three months without requiring re-authentication and re-authorization when a valid refresh token is supplied by the application according to the implementation specification adopted in § 170.215(c)(1).
2. AUT-PAT-23: The health IT developer demonstrates the ability of the Health IT Module to return an error response when supplied an invalid refresh token as specified in the implementation specification adopted in § 170.215(c)(1).

Required by December 31, 2025: SMART App Launch 2.0.0 (Note: US Core 3.1.1 and 4.0.0 expire on January 1, 2026)

Authentication and Authorization for Patient and User Scopes

HealthIT.gov

"launch sequence" using the "launch-ehr" "SMART on FHIR Core Capability" SMART EHR Launch mode detailed in the implementation specification adopted in § 170.215(c)(2), including:

- Launching the registered launch URL of the application; and
- Passing the parameters: "iss" and "launch".

3. AUT-PAT-3: [Standalone-Launch] The health IT developer demonstrates the ability of the Health IT Module to launch using the "launch-standalone" "SMART on FHIR® Core Capability" SMART Standalone Launch mode detailed in the implementation specification adopted in § 170.215(c)(2).
4. AUT-PAT-4: [Standalone-Launch] The health IT developer demonstrates the ability of the Health IT Module to support SMART's public client profile.
5. AUT-PAT-24: [Both] The health IT developer demonstrates the ability of the Health IT Module to support a ".well-known/smart-configuration" path as detailed in the implementation specification adopted in § 170.215(c)(2) and standard adopted in § 170.215(a)(1).
6. AUT-PAT-25: [Both] The health IT developer demonstrates the ability of the ".well-known/smart-configuration" path to support at least the following as detailed in the implementation specification adopted in § 170.215(c)(2):

- "authorization_endpoint";
- "token_endpoint";
- "capabilities" including support for "launch-ehr", "launch-standalone", "authorize-post", "client-public", "client-confidential-symmetric", "client-confidential-asymmetric", "sso-openid-connect", "context-banner", "context-style", "context-ehr-patient", "context-standalone-patient", "permission-offline", "permission-patient", "permission-user", "permission-v1", "permission-v2";
- "grant_types_supported" with support for "authorization_code" and "client_credentials"; and
- "code_challenge_methods_supported" with support for "S256" and shall not include support for "plain"

Additionally, the following "capabilities" must be supported if using US Core 6.1.0:

- "context-ehr-encounter"

7. AUT-PAT-26: [Both] The health IT developer demonstrates the ability of the Health IT Module to receive an authorization request according to the implementation specification adopted in § 170.215(c)(2), including support for the following parameters:

- "response_type";
- "client_id";
- "redirect_uri";
- "launch" (for EHR-Launch mode only);
- "scope";
- "state";
- "aud";
- "code_challenge"; and
- "code_challenge_method"

8. AUT-PAT-27: [Both] The health IT developer demonstrates the ability of the Health IT Module's Authorization Server to support the use of the HTTP GET and POST methods at the Authorization Endpoint as detailed in the implementation specification adopted in § 170.215(c)(2).
9. AUT-PAT-28: [Both] The health IT developer demonstrates the ability of the Health IT Module to support the receipt of the following scopes and capabilities according to the implementation specification adopted in § 170.215(c)(2) and standard adopted in § 170.215(e)(1):

- "openid" (to support "sso-openid-connect" "SMART on FHIR® Capability");
- "fhirUser" (to support "sso-openid-connect" "SMART on FHIR® Capability");
- "need_patient_banner" (to support "context-banner" "SMART on FHIR® Capability" for EHR-Launch mode only);
- "smart_style_url" (to support "context-style" "SMART on FHIR® Capability" for EHR-Launch mode only);
- "launch/patient" (to support "context-standalone-patient" "SMART on FHIR® Capability" for Standalone-Launch mode only);
- "launch" (for EHR-Launch mode only);
- "offline_access" (to support "permission-offline" "SMART on FHIR® Capability");
- Patient-level scopes (to support "permission-patient" and "SMART on FHIR® Capability");

HealthIT.gov

Capability". If using US Core 6.1.0, this includes support for finer-grained resource constraints using search parameters according to section 3.0.2.3 of the implementation specification at § 170.215(c)(2) for the "category" parameter for the following resources: (1) Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern; and (2) Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs

10. AUT-PAT-10: [Both] The health IT developer demonstrates the ability of the Health IT Module to evaluate the authorization request and request end-user input, if applicable (required for patient-facing applications), including the ability for the end-user to authorize an application to receive EHI based on FHIR® resource-level scopes for all of the FHIR® resources associated with the profiles specified in a standard adopted in § 170.213 and the corresponding implementation specification adopted in § 170.215(b)(1).

If using US Core 3.1.1, 4.0.0, or 6.1.0 these resources include:

- "AllergyIntolerance";
- "CarePlan";
- "CareTeam";
- "Condition";
- "Device";
- "DiagnosticReport";
- "DocumentReference";
- "Goal";
- "Immunization";
- "Medication" (if supported);
- "MedicationRequest";
- "Observation";
- "Patient";
- "Procedure"; and
- "Provenance".

The following resources must also be supported if using US Core 6.1.0:

- "Encounter"
- "Coverage"
- "Specimen"
- "MedicationDispense"
- "RelatedPerson"; and
- "ServiceRequest"

11. AUT-PAT-11: [Both] The health IT developer demonstrates the ability of the Health IT Module to evaluate the authorization request and request end-user input, if applicable (required for patient-facing applications), including either the ability for the end-user to explicitly enable / disable the "offline_access" scope or information communicating the application's request for the "offline_access" scope.
12. AUT-PAT-12: [Both] The health IT developer demonstrates the ability of the Health IT Module to deny an application's authorization request according to a patient's preferences selected in AUT-PAT-10, and AUT-PAT-11, of this section in accordance with the implementation specification adopted in § 170.215(c)(2).
13. AUT-PAT-29: [EHR-Launch] The health IT developer demonstrates the ability of the Health IT Module to establish a patient in context if an application requests a clinical scope which is restricted to a single patient as detailed in the implementation specification adopted in § 170.215(c)(2).
14. AUT-PAT-13: [Both] The health IT developer demonstrates the ability of the Health IT Module to return an error response if the "aud" parameter provided by an application to the Health IT Module in AUT-PAT-8, is not a valid FHIR® resource server associated with the Health IT Module's authorization server.
15. AUT-PAT-14: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant an application access to EHI by returning an authorization code to the application according to the implementation specification adopted in § 170.215(c)(2), including the following parameters:
- "code"; and

HealthIT.gov

- "grant_type";
- "code";
- "redirect_uri";
- "code_verifier";
- "client_id" (to support "client-public" "SMART on FHIR® Capability");
- Authorization header including "client_id" and "client_secret" (to support "client-confidential-symmetric" "SMART on FHIR® Capability"); and
- Authentication JSON Web Token (to support "client-confidential-asymmetric" "SMART on FHIR® Capability")

17. AUT-PAT-31: [Both] The health IT developer demonstrates the ability of the Health IT Module to return an error response if an invalid "code_verifier" value is supplied with an access token request according to the implementation specification adopted in § 170.215(c)(2).
18. AUT-PAT-16: [Both] The health IT developer demonstrates the ability of the Health IT Module to return a JSON object to applications according to the implementation specification adopted in § 170.215(c)(2) and standard adopted in § 170.215(e)(1), including the following:
    - "access_token";
    - "token_type";
    - "scope";
    - "id_token";
    - "refresh_token" (valid for a period of no shorter than three months);
    - HTTP "Cache-Control" response header field with a value of "no-store";
    - HTTP "Pragma" response header field with a value of "no-cache";
    - "patient" (to support "context-ehr-patient" and "context-standalone-patient" "SMART on FHIR® Core Capabilities");
    - "need_patient_banner" (to support "context-banner" "SMART on FHIR® Core Capability" for EHR-Launch mode only); and
    - "smart_style_url" (to support "context-style" "SMART on FHIR® Core Capability" for EHR-Launch mode only).
    - Additionally, the following must be supported if using US Core 6.1.0"encounter" (to support "context-ehr-encounter" "SMART on FHIR® Capability")
19. AUT-PAT-17: [Both] The health IT developer demonstrates the ability of the Health IT Module to provide an OpenID Connect well-known URI in accordance with the implementation specification adopted in § 170.215(e)(1), including:
    - All required fields populated according to implementation specification adopted in § 170.215(e)(1); and
    - Valid JWKS populated according to implementation specification can be retrieved via JWKS URI.
20. AUT-PAT-18: [Both] The health IT developer demonstrates the ability of the Health IT Module to deny an application's authorization request in accordance with the implementation specification adopted in § 170.215(c)(2).
21. AUT-PAT-19: [Both] The health IT developer demonstrates the ability of the Health IT Module to return a "Patient" FHIR® resource that matches the patient context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
22. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 6.1.0: The health IT developer demonstrates the ability of the Health IT Module to return an "Encounter" FHIR® resource that matches the encounter context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
23. AUT-PAT-20: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant an access token when a refresh token is supplied according to an implementation specification adopted in § 170.215(b)(1).
24. AUT-PAT-21: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant a refresh token valid for a period of no less than three months to native applications capable of securing a refresh token.

Subsequent Connections: Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-22: The health IT developer demonstrates the ability of the Health IT Module to issue a refresh token valid for a new period of no shorter than three months without requiring re-authentication and re-authorization

(2).

HealthIT.gov

Expires on January 1, 2026: SMART App Launch 1.0.0

Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-1: The tester verifies the ability of the Health IT Module to support the following for “EHR-Launch,” “Standalone-Launch,” and “Both” (“EHR-Launch” and “Standalone-Launch”) as specified in the implementation specification adopted in § 170.215(c)(1).
2. AUT-PAT-2: [EHR-Launch] The tester verifies the ability of the Health IT Module to initiate a “launch sequence” using the “launch-ehr" “SMART on FHIR® Core Capability” SMART EHR Launch mode detailed in the implementation specification adopted in § 170.215(c)(1), including:
   - Launching the registered launch URL of the application; and
   - Passing the parameters: “iss” and “launch”.
3. AUT-PAT-3: [Standalone-Launch] The tester verifies the ability of the Health IT Module to launch using the “launch-standalone" “SMART on FHIR® Core Capability” SMART Standalone Launch mode detailed in the implementation specification adopted in § 170.215(c)(1).
4. AUT-PAT-4: [Standalone-Launch] The tester verifies the ability of the Health IT Module to support SMART’s public client profile.
5. AUT-PAT-5: [Both] The tester verifies the ability of the Health IT Module to support the following as detailed in the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(a)(1):
   - The “.well-known/smart-configuration” path; and
   - A FHIR® “CapabilityStatement”.
6. AUT-PAT-6: [Both] The tester verifies the ability of the “.well-known/smart-configuration” path to support at least the following as detailed in the implementation specification adopted in § 170.215(c)(1):
   - “authorization_endpoint”;
   - “token_endpoint”; and
   - “capabilities” (including support for all the “SMART on FHIR® Core Capabilities”).
7. AUT-PAT-7: [Both] The tester verifies the ability of the FHIR® “CapabilityStatement” to support at least the following components as detailed in the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(a)(1), including:
   - “authorize”; and
   - “token”.
8. AUT-PAT-8: [Both] The tester verifies the ability of the Health IT Module to receive an authorization request according to the implementation specification adopted in § 170.215(c)(1), including support for the following parameters:
   - “response_type”;
   - “client_id”;
   - “redirect_uri”;
   - “launch” (for EHR-Launch mode only);
   - “scope”;
   - “state”; and
   - “aud”.
9. AUT-PAT-9: [Both] The tester verifies the ability of the Health IT Module to support the receipt of the following scopes according to the implementation specification adopted in § 170.215(c)(1) and standard adopted in § 170.215(e)(1):
   - “openid” (to support “sso-openid-connect” “SMART on FHIR® Core Capability”);
   - “fhirUser” (to support “sso-openid-connect” “SMART on FHIR® Core Capability”);
   - “need_patient_banner” (to support “context-banner” “SMART on FHIR® Core Capability” for EHR-Launch mode only);
   - “smart_style_url” (to support “context-style” “SMART on FHIR® Core Capability” for EHR-Launch mode only);
   - “launch/patient” (to support “context-standalone-patient” “SMART on FHIR® Core Capability” for Standalone-Launch mode only);
   - “launch” (for EHR-Launch mode only);

HealthIT.gov

and request end-user input, if applicable (required for patient-facing applications), including the ability for the end-user to authorize an application to receive EHI based on FHIR® resource-level scopes for all of the FHIR® resources associated with the profiles specified in a standard adopted in § 170.213 and the corresponding implementation specification adopted in § 170.215(b)(1).
If using US Core 3.1.1, 4.0.0, or 6.1.0 these resources include:

- "AllergyIntolerance";
- "CarePlan";
- "CareTeam";
- "Condition";
- "Device";
- "DiagnosticReport";
- "DocumentReference";
- "Goal";
- "Immunization";
- "Medication" (if supported);
- "MedicationRequest";
- "Observation";
- "Patient";
- "Procedure"; and
- "Provenance".

The following resources must also be supported if using US Core 6.1.0:

- "Encounter"
- "Coverage"
- "Specimen"
- "MedicationDispense"
- "RelatedPerson"; and
- "ServiceRequest"

11. AUT-PAT-11: [Both] The tester verifies the ability of the Health IT Module to evaluate the authorization request and request end-user input, if applicable (required for patient-facing applications), including either the ability for the end-user to explicitly enable / disable the "offline_access" scope or information communicating the application's request for the "offline_access" scope.
12. AUT-PAT-12: [Both] The tester verifies the ability of the Health IT Module to deny an application's authorization request according to a patient's preferences selected in AUT-PAT-10, and AUT-PAT-11, of this section in accordance with the implementation specification adopted in § 170.215(c)(1).
13. AUT-PAT-13: [Both] The tester verifies the ability of the Health IT Module to return an error response if the "aud" parameter provided by an application to the Health IT Module in AUT-PAT-8, is not a valid FHIR® resource server associated with the Health IT Module's authorization server.
14. AUT-PAT-14: [Both] The tester verifies the ability of the Health IT Module to grant an application access to EHI by returning an authorization code to the application according to the implementation specification adopted in § 170.215(c)(1), including the following parameters:

- "code"; and
- "state".

15. AUT-PAT-15: [Both] The tester verifies the ability of the Health IT Module to receive the following parameters from an application according to the implementation specification adopted in § 170.215(c)(1):

- "grant_type";
- "code";
- "redirect_uri";
- "client_id" (to support "client-public" "SMART on FHIR® Capability"); and
- Authorization header including "client_id" and "client_secret" (to support "client-confidential-symmetric" "SMART on FHIR® Capability").

HealthIT.gov

- "token_type";
- "scope";
- "id_token";
- "refresh_token" (valid for a period of no shorter than three months);
- HTTP "Cache-Control" response header field with a value of "no-store";
- HTTP "Pragma" response header field with a value of "no-cache";
- "patient" (to support "context-ehr-patient" and "context-standalone-patient" "SMART on FHIR® Core Capabilities");
- "need_patient_banner" (to support "context-banner" "SMART on FHIR® Core Capability" for EHR-Launch mode only); and
- "smart_style_url" (to support "context-style" "SMART on FHIR® Core Capability" for EHR-Launch mode only).

Additionally, the following must be supported if using US Core or 6.1.0:

- "encounter" (to support "context-ehr-encounter" "SMART on FHIR® Capability")

17. AUT-PAT-17: [Both] The tester verifies the ability of the Health IT Module to provide an OpenID Connect well-known URI in accordance with the implementation specification adopted in § 170.215(e)(1) , including:
    - All required fields populated according to implementation specification adopted in § 170.215(e)(1); and
    - Valid JWKS populated according to implementation specification can be retrieved via JWKS URI.
18. AUT-PAT-18: [Both] The tester verifies the ability of the Health IT Module to deny an application's authorization request in accordance with the implementation specification adopted in § 170.215(c)(1).
19. AUT-PAT-19: [Both] The tester verifies the ability of the Health IT Module to return a "Patient" FHIR® resource that matches the patient context provided in step AUT-PAT-16 of this section according to the implementation specification adopted in § 170.215(b)(1).
20. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 6.1.0: The tester verifies the ability of the Health IT Module to return an "Encounter" FHIR® resource that matches the encounter context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
21. AUT-PAT-20: [Both] The tester verifies the ability of the Health IT Module to grant an access token when a refresh token is supplied according to an implementation specification adopted in § 170.215(b)(1).
22. AUT-PAT-21: [Both] The tester verifies the ability of the Health IT Module to grant a refresh token valid for a period of no less than three months to native applications capable of securing a refresh token.

Subsequent Connections: Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-22: The tester verifies the ability of the Health IT Module to issue a refresh token valid for a new period of no shorter than three months without requiring re-authentication and re-authorization when a valid refresh token is supplied by the application according to the implementation specification adopted in § 170.215(c)(1).
2. AUT-PAT-23: The tester verifies the ability of the Health IT Module to return an error response when supplied an invalid refresh token as specified in the implementation specification adopted in § 170.215(c)(1).

Required by December 31, 2025: SMART App Launch 2.0.0 (Note: US Core 3.1.1 and 4.0.0 expire on January 1, 2026)

Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-1: The tester verifies the ability of the Health IT Module to support the following for "EHR-Launch," "Standalone-Launch," and "Both" ("EHR-Launch" and "Standalone-Launch") as specified in the implementation specification adopted in § 170.215(c)(2).
2. AUT-PAT-2: [EHR-Launch] The tester verifies the ability of the Health IT Module to initiate a "launch sequence" using the "launch-ehr" "SMART on FHIR® Core Capability" SMART EHR Launch mode detailed in the implementation specification adopted in § 170.215(c)(2), including:
    - Launching the registered launch URL of the application; and
    - Passing the parameters: "iss" and "launch".

HealthIT.gov

client profile.

5. AUT-PAT-24: [Both] The tester verifies the ability of the Health IT Module to support a ".well-known/smart-configuration" path as detailed in the implementation specification adopted in § 170.215(c)(2) and standard adopted in § 170.215(a)(1).
6. AUT-PAT-25: [Both] The tester verifies the ability of the ".well-known/smart-configuration" path to support at least the following as detailed in the implementation specification adopted in § 170.215(c)(2):

- "authorization_endpoint";
- "token_endpoint";
- "capabilities" including support for "launch-ehr", "launch-standalone", "authorize-post", "client-public", "client-confidential-symmetric", "client-confidential-asymmetric", "sso-openid-connect", "context-banner", "context-style", "context-ehr-patient", "context-standalone-patient", "permission-offline", "permission-patient", "permission-user", "permission-v1", "permission-v2";
- "grant_types_supported" with support for "authorization_code" and "client_credentials"; and
- "code_challenge_methods_supported" with support for "S256" and shall not include support for "plain"

Additionally, the following "capabilities" must be supported if using US Core 6.1.0:

- "context-ehr-encounter"

7. AUT-PAT-26: [Both] The tester verifies the ability of the Health IT Module to receive an authorization request according to the implementation specification adopted in § 170.215(c)(2), including support for the following parameters:

- "response_type";
- "client_id";
- "redirect_uri";
- "launch" (for EHR-Launch mode only);
- "scope";
- "state";
- "aud";
- "code_challenge"; and
- "code_challenge_method"

8. AUT-PAT-27: [Both] The tester verifies the ability of the Health IT Module's Authorization Server to support the use of the HTTP GET and POST methods at the Authorization Endpoint as detailed in the implementation specification adopted in § 170.215(c)(2).
9. AUT-PAT-28: [Both] The tester verifies the ability of the Health IT Module to support the receipt of the following scopes and capabilities according to the implementation specification adopted in § 170.215(c)(2) and standard adopted in § 170.215(e)(1):

- "openid" (to support "sso-openid-connect" "SMART on FHIR® Capability");
- "fhirUser" (to support "sso-openid-connect" "SMART on FHIR® Capability");
- "need_patient_banner" (to support "context-banner" "SMART on FHIR® Capability" for EHR-Launch mode only);
- "smart_style_url" (to support "context-style" "SMART on FHIR® Capability" for EHR-Launch mode only);
- "launch/patient" (to support "context-standalone-patient" "SMART on FHIR® Capability" for Standalone-Launch mode only);
- "launch" (for EHR-Launch mode only);
- "offline_access" (to support "permission-offline" "SMART on FHIR® Capability");
- Patient-level scopes (to support "permission-patient" and "SMART on FHIR® Capability");
- User-level scopes (to support "permission-user" "SMART on FHIR® Capability"); and
- SMART v1 scope syntax for patient-level and user-level scopes to support the "permission-v1" "SMART on FHIR® Capability"
- SMART v2 scope syntax for patient-level and user-level scopes to support the "permission-v2" "SMART on FHIR® Capability". If using US Core 6.1.0, this includes support for finer-grained resource constraints using search parameters according to section 3.0.2.3 of the implementation specification at § 170.215(c)(2) for the "category" parameter for the following resources: (1) Condition resource with Condition sub-resources Encounter

HealthIT.gov

end-user to authorize an application to receive EHI based on FHIR® resource-level scopes for all of the FHIR resources associated with the profiles specified in a standard adopted in § 170.213 and the corresponding implementation specification adopted in § 170.215(b)(1).

If using US Core 3.1.1, 4.0.0, or 6.1.0 these resources include:

- “AllergyIntolerance”;
- “CarePlan”;
- “CareTeam”;
- “Condition”;
- “Device”;
- “DiagnosticReport”;
- “DocumentReference”;
- “Goal”;
- “Immunization”;
- “Medication” (if supported);
- “MedicationRequest”;
- “Observation”;
- “Patient”;
- “Procedure”; and
- “Provenance”.

The following resources must also be supported if using US Core 6.1.0:

- “Encounter”
- “Coverage”
- “Specimen”
- “MedicationDispense”
- “RelatedPerson”; and
- “ServiceRequest”

11. AUT-PAT-11: [Both] The tester verifies the ability of the Health IT Module to evaluate the authorization request and request end-user input, if applicable (required for patient-facing applications), including either the ability for the end-user to explicitly enable / disable the “offline_access” scope or information communicating the application’s request for the “offline_access” scope.
12. AUT-PAT-12: [Both] The tester verifies the ability of the Health IT Module to deny an application’s authorization request according to a patient’s preferences selected in AUT-PAT-10, and AUT-PAT-11, of this section in accordance with the implementation specification adopted in § 170.215(c)(2).
13. AUT-PAT-29: [EHR-Launch] The tester verifies the ability of the Health IT Module to establish a patient in context if an application requests a clinical scope which is restricted to a single patient as detailed in the implementation specification adopted in § 170.215(c)(2).
14. AUT-PAT-13: [Both] The tester verifies the ability of the Health IT Module to return an error response if the "aud" parameter provided by an application to the Health IT Module in AUT-PAT-8, is not a valid FHIR® resource server associated with the Health IT Module's authorization server.
15. AUT-PAT-14: [Both] The tester verifies the ability of the Health IT Module to grant an application access to EHI by returning an authorization code to the application according to the implementation specification adopted in § 170.215(c)(2), including the following parameters:

- “code”; and
- “state”.

16. AUT-PAT-30: [Both] The tester verifies the ability of the Health IT Module to receive the following access token request parameters from an application according to the implementation specification adopted in § 170.215(c)(2):

- “grant_type”;
- “code”;

HealthIT.gov

symmetric" "SMART on FHIR® Capability"); and
- Authentication JSON Web Token (to support "client-confidential-asymmetric" "SMART on FHIR® Capability")

17. AUT-PAT-31: [Both] The tester verifies the ability of the Health IT Module to return an error response if an invalid "code_verifier" value is supplied with an access token request according to the implementation specification adopted in § 170.215(c)(2).
18. AUT-PAT-16: [Both] The tester verifies the ability of the Health IT Module to return a JSON object to applications according to the implementation specification adopted in § 170.215(c)(2) and standard adopted in § 170.215(e)(1), including the following:
- "access_token";
- "token_type";
- "scope";
- "id_token";
- "refresh_token" (valid for a period of no shorter than three months);
- HTTP "Cache-Control" response header field with a value of "no-store";
- HTTP "Pragma" response header field with a value of "no-cache";
- "patient" (to support "context-ehr-patient" and "context-standalone-patient" "SMART on FHIR® Core Capabilities");
- "need_patient_banner" (to support "context-banner" "SMART on FHIR® Core Capability" for EHR-Launch mode only); and
- "smart_style_url" (to support "context-style" "SMART on FHIR® Core Capability" for EHR-Launch mode only).

Additionally, the following must be supported if using US Core 6.1.0:

- "encounter" (to support "context-ehr-encounter" "SMART on FHIR® Capability")

19. AUT-PAT-17: [Both] The tester verifies the ability of the Health IT Module to provide an OpenID Connect well-known URI in accordance with the implementation specification adopted in § 170.215(e)(1), including:
- All required fields populated according to implementation specification adopted in § 170.215(e)(1); and
- Valid JWKS populated according to implementation specification can be retrieved via JWKS URI.

20. AUT-PAT-18: [Both] The tester verifies the ability of the Health IT Module to deny an application's authorization request in accordance with the implementation specification adopted in § 170.215(c)(2).
21. AUT-PAT-19: [Both] The tester verifies the ability of the Health IT Module to return a "Patient" FHIR® resource that matches the patient context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
22. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 6.1.0: The tester verifies the ability of the Health IT Module to return an "Encounter" FHIR® resource that matches the encounter context provided in step AUT-PAT-16 of this section according to an implementation specification adopted in § 170.215(b)(1).
23. AUT-PAT-20: [Both] The tester verifies the ability of the Health IT Module to grant an access token when a refresh token is supplied according to an implementation specification adopted in § 170.215(b)(1).
24. AUT-PAT-21: [Both] The tester verifies the ability of the Health IT Module to grant a refresh token valid for a period of no less than three months to native applications capable of securing a refresh token.

Subsequent Connections: Authentication and Authorization for Patient and User Scopes

1. AUT-PAT-22: The tester verifies the ability of the Health IT Module to issue a refresh token valid for a new period of no shorter than three months without requiring re-authentication and re-authorization when a valid refresh token is supplied by the application according to the implementation specification adopted in § 170.215(c)(2).
2. AUT-PAT-23: The tester verifies the ability of the Health IT Module to return an error response when supplied an invalid refresh token as specified in the implementation specification adopted in § 170.215(c)(2).

HealthIT.gov

Applies to all applicable regulatory and SVAP standards

Patient Authorization Revocation

PAR-1: The health IT developer demonstrates the ability of the Health IT Module to revoke access to an authorized application at a patient's direction within 1 hour of the revocation request, including a demonstration of the inability of the application with revoked access to receive patient EHI.

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

Patient Authorization Revocation

PAR-1: The tester verifies the ability of the Health IT Module to revoke access to an authorized application at a patient's direction within 1 hour of the revocation request, including a demonstration of the inability of the application with revoked access to receive patient EHI.

HealthIT.gov

Applies to all applicable regulatory and SVAP standards

Authentication and Authorization for System Scopes

1. AUT-SYS-1: The health IT developer demonstrates the ability of the Health IT Module to support OAuth 2.0 client credentials grant flow in accordance with an implementation specification adopted in § 170.215(d).
2. AUT-SYS-2: The health IT developer demonstrates the ability of the Health IT Module to support the following parameters according to an implementation specification adopted in § 170.215(d):
   - “scope”;
   - “grant_type”;
   - “client_assertion_type”; and
   - “client_assertion”.
3. AUT-SYS-3: The health IT developer demonstrates the ability of the Health IT Module to support the following JSON Web Token (JWT) Headers and Claims according to an implementation specification adopted in § 170.215(d):
   - “alg” header;
   - “kid” header;
   - “typ” header;
   - “iss” claim;
   - “sub” claim;
   - “aud” claim;
   - “exp” claim; and
   - “jti” claim.
4. AUT-SYS-4: The health IT developer demonstrates the ability of the Health IT Module to receive and process the JSON Web Key (JWK) Set via a TLS-protected URL to support authorization for system scopes in § 170.315(g)(10)(v)(B).
5. AUT-SYS-5: The health IT developer demonstrates that the Health IT Module does not cache a JWK Set received via a TLS-protected URL for longer than the “cache-control” header sent by an application indicates.
6. AUT-SYS-6: The health IT developer demonstrates the ability of the Health IT Module to validate an application’s JWT, including its JSON Web Signatures, according to an implementation specification adopted in § 170.215(d).
7. AUT-SYS-7: The health IT developer demonstrates the ability of the Health IT Module to respond with an “invalid_client” error for errors encountered during the authentication process according to an implementation specification adopted in § 170.215(d).
8. AUT-SYS-8: The health IT developer demonstrates the ability of the Health IT Module to assure the scope granted based on the scope requested by an application is no greater than the pre-authorized scope for multiple patients according to an implementation specification adopted in § 170.215(d).
9. AUT-SYS-9: The health IT developer demonstrates the ability of the Health IT Module to issue an access token to an application as a JSON object in accordance with an implementation specification adopted in § 170.215(d), including the following property names:
   - “access_token”;
   - “token_type”;
   - “expires_in”; and
   - “scope”.
10. AUT-SYS-10: The health IT developer demonstrates the ability of the Health IT Module to respond to errors using the appropriate error messages as specified in an implementation specification adopted in § 170.215(d).

HealthIT.gov

Authentication and Authorization for System Scopes

1. AUT-SYS-1: The tester verifies the ability of the Health IT Module to support OAuth 2.0 client credentials grant flow in accordance with an implementation specification adopted in § 170.215(d).
2. AUT-SYS-2: The tester verifies the ability of the Health IT Module to support the following parameters according to an implementation specification adopted in § 170.215(d):
   - "scope";
   - "grant_type";
   - "client_assertion_type"; and
   - "client_assertion".
3. AUT-SYS-3: The tester verifies the ability of the Health IT Module to support the following JSON Web Token (JWT) Headers and Claims according to an implementation specification adopted in § 170.215(d):
   - "alg" header;
   - "kid" header;
   - "typ" header;
   - "iss" claim;
   - "sub" claim;
   - "aud" claim;
   - "exp" claim; and
   - "jti" claim.
4. AUT-SYS-4: The tester verifies the ability of the Health IT Module to receive and process the JWK structure via a TLS-protected URL to support authorization for system scopes in § 170.315(g)(10)(v)(B).
5. AUT-SYS-5: The tester verifies the Health IT Module does not cache a JWK Set received via a TLS-protected URL for longer than the "cache-control" header sent by an application indicates.
6. AUT-SYS-6: The tester verifies the ability of the Health IT Module to validate an application's JWT, including its JSON Web Signatures, according to an implementation specification adopted in § 170.215(d).
7. AUT-SYS-7: The tester verifies the ability of the Health IT Module to respond with an "invalid_client" error for errors encountered during the authentication process according to an implementation specification adopted in § 170.215(d).
8. AUT-SYS-8: The tester verifies the ability of the Health IT Module to assure the scope granted based on the scope requested by an application is no greater than the pre-authorized scope for multiple patients according to an implementation specification adopted in § 170.215(d).
9. AUT-SYS-9: The tester verifies the ability of the Health IT Module to issue an access token to an application as a JSON object in accordance with an implementation specification adopted in § 170.215(d), including the following property names:
   - "access_token";
   - "token_type";
   - "expires_in"; and
   - "scope".
10. AUT-SYS-10: The tester verifies the ability of the Health IT Module to respond to errors using the appropriate error messages as specified in an implementation specification adopted in § 170.215(d).

Paragraph (g)(10)(vii) – Token introspection

System Under Test

Applies to all applicable regulatory and SVAP standards

Token Introspection

1. TOK-INTRO-1: The health IT developer demonstrates the ability of the Health IT Module to receive and validate a token it has issued in accordance with an implementation specification in § 170.215(c).

HealthIT.gov

Token Introspection

1. TOK-INTRO-1: The tester verifies the ability of the Health IT Module to receive and validate a token it has issued in accordance with an implementation specification in § 170.215(c).

Paragraph (g)(10)(ii) – Supported search operations

System Under Test

Applies to all applicable regulatory and SVAP standards

Supported Search Operations for a Single Patient's Data

1. SH-PAT-1: The health IT developer demonstrates the ability of the Health IT Module to support the "capabilities" interaction as specified in the standard adopted in § 170.215(a)(1), including support for a "CapabilityStatement" as specified in the standard adopted in § 170.215(a)(1) and an implementation specification adopted in § 170.215(b)(1).
2. SH-PAT-2: The health IT developer demonstrates the ability of the Health IT Module to respond to requests for a single patient's data consistent with the search criteria detailed in the "US Core Server CapabilityStatement" section of an implementation specification adopted in § 170.215(b)(1), including demonstrating search support for "SHALL" operations and parameters for all the data included in the corresponding standard adopted in § 170.213.
3. SH-PAT-3: The health IT developer demonstrates the ability of the Health IT Module to support a resource search for the provenance target "(_revIncludes: Provenance:target)" for all the FHIR® resources included in a standard adopted in § 170.213 and the corresponding implementation specification adopted in § 170.215(b)(1) according to the "Basic Provenance Guidance" section of an implementation specification adopted in § 170.215(b)(1).

Supported Search Operations for Multiple Patients' Data

4. SH-PAT-4: The health IT developer demonstrates the ability of the Health IT Module to support the "capabilities" interaction as specified in the standard adopted in § 170.215(a)(1), including support for a "CapabilityStatement" as specified in the standard adopted in § 170.215(a)(1) and an implementation specification adopted in § 170.215(d).
5. SH-PAT-5: The health IT developer demonstrates the ability of the Health IT Module to support requests for multiple patients' data as a group using the "group-export" operation as detailed in an implementation specification adopted in § 170.215(d).

HealthIT.gov

Supported Search Operations for a Single Patient's Data

1. SH-PAT-1: The tester verifies the ability of the Health IT Module to support the "capabilities" interaction as specified in the standard adopted in § 170.215(a)(1), including support for a "CapabilityStatement" as specified in the standard adopted in § 170.215(a)(1) and an implementation specification adopted in § 170.215(b)(1).
2. SH-PAT-2: The tester verifies the ability of the Health IT Module to respond to requests for a single patient's data consistent with the search criteria detailed in the "US Core Server CapabilityStatement" section of an implementation specification adopted in § 170.215(b)(1), including demonstrating search support for "SHALL" operations and parameters for all the data included in the corresponding standard adopted in § 170.213.
3. SH-PAT-3: The tester verifies the ability of the Health IT Module to support a resource search for the provenance target "(_revIncludes: Provenance:target)" for all the FHIR® resources included in a standard adopted in § 170.213 and the corresponding implementation specification adopted in § 170.215(b)(1) according to the "Basic Provenance Guidance" section of an implementation specification adopted in § 170.215(b)(1).

Supported Search Operations for Multiple Patients' Data

1. SH-PAT-4: The tester verifies the ability of the Health IT Module to support the "capabilities" interaction as specified in the standard adopted in § 170.215(a)(1), including support for a "CapabilityStatement" as specified in the standard adopted in § 170.215(a)(1) and an implementation specification adopted in § 170.215(d).
2. SH-PAT-5: The tester verifies the ability of the Health IT Module to support requests for multiple patients' data as a group using the "group-export" operation as detailed in an implementation specification adopted in § 170.215(d).

HealthIT.gov

All of the following test steps for Paragraph (g)(10)(i) – "Data response" apply to both Bulk Data Access v1.0.1 and Bulk Data Access v2.0.0

Expires on January 1, 2026: (USCDI v1 + US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 + US Core STU v4.0.0)

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-1: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-8, of this section respectively, the health IT developer demonstrates the ability of the Health IT Module to respond to requests for data according to the implementation specification adopted in § 170.215(b)(1)(i), including the following steps.
2. DAT-PAT-2: The health IT developer demonstrates the ability of the Health IT Module to respond with data that meet the following conditions:
   - All data elements indicated with a cardinality of one or greater and / or "must support" are included;
   - Content is structurally correct;
   - All invariant rules are met;
   - All data elements with required "ValueSet" bindings contain codes within the bound "ValueSet";
   - All information is accurate and without omission; and
   - All references within the resources can be resolved and validated, as applicable, according to steps DAT-PAT-2, DAT-PAT-3, DAT-PAT-4, DAT-PAT-5, and DAT-PAT-6, of this section.
3. DAT-PAT-3: The health IT developer demonstrates the ability of the Health IT Module to support a "Provenance" FHIR® resource for all the FHIR® resources included in the standard adopted in § 170.213(a) and implementation specification adopted in § 170.215(b)(1)(i) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(b)(1)(i).
4. DAT-PAT-4: The health IT developer demonstrates the ability of the Health IT Module to support a "DocumentReference" and/or "DiagnosticReport" FHIR® resource for each of the "Clinical Notes" and "Diagnostic Reports" included in and according to the "Clinical Notes Guidance" section of the implementation specification adopted in § 170.215(b)(1)(i).
5. DAT-PAT-5: If supported, and for responses to data for a single patient only, the health IT developer demonstrates the ability of the Health IT Module to support a "Medication" FHIR® resource according to the "Medication List Guidance" section of the implementation specification adopted in § 170.215(b)(1)(i).
6. DAT-PAT-6: The health IT developer demonstrates the ability of the Health IT Module to support "Missing Data" according to the implementation specification adopted in § 170. 215(b)(1)(i), including:
   - For non-coded data elements; and
   - For coded data elements, including support for the "DataAbsentReason" Code System.

Note: We require the health IT developers to demonstrate support for the tests above for both responses to requests for a single patient's data and responses to requests for multiple patients' data because we make no assumption regarding the re-use of technical infrastructure for "read" services for single and multiple patients in Health IT Modules.

Response to Requests for a Single Patient's Data

7. DAT-PAT-7: The health IT developer demonstrates the ability of the Health IT Module to return all of the data associated with requests for a single patient's data according to the "US Core Server CapabilityStatement" section of the implementation specification adopted in § 170.215(b)(1)(i) for all the data included in the standard adopted in § 170.213(a).

Response to Requests for Multiple Patients' Data

8. DAT-PAT-8: The health IT developer demonstrates the ability of the Health IT Module to respond to requests for multiple patients' data according to an implementation specification adopted in § 170.215(d) for all of the FHIR®

- “CareTeam”;
- “Condition”;
- “Device”;
- “DiagnosticReport”;
- “DocumentReference”;
- “Encounter”;
- “Goal”;
- “Immunization”;
- “Location” (if supported);
- “Medication” (if supported);
- “MedicationRequest”;
- “Observation”;
- “Organization”;
- “Patient”;
- “Practitioner”
- “Procedure”; and
- “Provenance”.

9. DAT-PAT-9: The health IT developer demonstrates the ability of the Health IT Module to limit the data returned to only those FHIR® resources for which the client is authorized according to an implementation specification adopted in § 170.215(d).
10. DAT-PAT-10: The health IT developer demonstrates the ability of the Health IT Module to support a successful data response according to an implementation adopted in § 170.215(d).
11. DAT-PAT-11: The health IT developer demonstrates the ability of the Health IT Module to support a data response error according to an implementation adopted in § 170.215(d).
12. DAT-PAT-12: The health IT developer demonstrates the ability of the Health IT Module to support a bulk data delete request according to an implementation specification adopted in § 170.215(d).
13. DAT-PAT-13: The health IT developer demonstrates the ability of the Health IT Module to support a bulk data status request according to an implementation specification adopted in § 170.215(d).
14. DAT-PAT-14: The health IT developer demonstrates the ability of the Health IT Module to support a file request according to an implementation specification adopted in § 170.215(d), including support for the “ndjson” format for files provided.
15. DAT-PAT-15: The health IT developer demonstrates that the information provided as part of this data response includes data for patients in the group identifier provided during the “group-export” request.

Required by December 31, 2025: USCDI v3 + US Core STU v6.1.0

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-1: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-8, of this section respectively, the health IT developer demonstrates the ability of the Health IT Module to respond to requests for data according to the implementation specification adopted in § 170.215(b)(1)(ii), including the following steps.
2. DAT-PAT-2: The health IT developer demonstrates the ability of the Health IT Module to respond with data that meet the following conditions:

- All data elements indicated with a cardinality of one or greater and / or “must support” are included;
- Content is structurally correct;
- All invariant rules are met;
- All data elements with required “ValueSet” bindings contain codes within the bound “ValueSet”;
- All information is accurate and without omission; and
- All references within the resources can be resolved and validated, as applicable, according to steps DAT-PAT-2, DAT-PAT-3, DAT-PAT-4, DAT-PAT-5, and DAT-PAT-6, of this section.

HealthIT.gov

4. DAT-PAT-4: The health IT developer demonstrates the ability of the Health IT Module to support a "DocumentReference" and/or "DiagnosticReport" FHIR® resource for each of the "Clinical Notes" and "Diagnostic Reports" included in and according to the "Clinical Notes Guidance" section of the implementation specification adopted in § 170.215(b)(1)(ii).
5. DAT-PAT-5: If supported, and for responses to data for a single patient only, the health IT developer demonstrates the ability of the Health IT Module to support a "Medication" FHIR® resource according to the "Medication List Guidance" section of the implementation specification adopted in § 170.215(b)(1)(ii).
6. DAT-PAT-6: The health IT developer demonstrates the ability of the Health IT Module to support "Missing Data" according to the implementation specification adopted in § 170. 215(b)(1)(ii), including:

- For non-coded data elements; and
- For coded data elements, including support for the "DataAbsentReason" Code System.

Note: We require the health IT developers to demonstrate support for the tests above for both responses to requests for a single patient's data and responses to requests for multiple patients' data because we make no assumption regarding the re-use of technical infrastructure for "read" services for single and multiple patients in Health IT Modules.

Response to Requests for Single Patients' Data

7. DAT-PAT-7: The health IT developer demonstrates the ability of the Health IT Module to return all of the data associated with requests for a single patient's data according to the "US Core Server CapabilityStatement" section of the implementation specification adopted in § 170.215(b)(1)(ii) for all the data included in the standard adopted in § 170.213(b).

Response to Requests for Multiple Patients' Data

8. DAT-PAT-17: The health IT developer demonstrates the ability of the Health IT Module to respond to requests for multiple patients' data according to an implementation specification adopted in § 170.215(d) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in § 170.213(b) and implementation specification adopted in § 170.215(b)(1)(ii).

- "AllergyIntolerance";
- "CarePlan";
- "CareTeam";
- "Condition";
- "Coverage"
- "Device";
- "DiagnosticReport";
- "DocumentReference";
- "Encounter";
- "Goal";
- "Immunization";
- "Location" (if supported);
- "Medication" (if supported);
- "MedicationDispense"
- "MedicationRequest";
- "Observation";
- "Organization";
- "Patient";
- "Practitioner"
- "Procedure";
- "Provenance";
- "PractitionerRole" (if supported);
- "QuestionnaireReponse" (if supported);

HealthIT.gov

only those FHIR® resources for which the client is authorized according to an implementation specification adopted in § 170.215(d).

10. DAT-PAT-10: The health IT developer demonstrates the ability of the Health IT Module to support a successful data response according to an implementation adopted in § 170.215(d).
11. DAT-PAT-11: The health IT developer demonstrates the ability of the Health IT Module to support a data response error according to an implementation adopted in § 170.215(d).
12. DAT-PAT-12: The health IT developer demonstrates the ability of the Health IT Module to support a bulk data delete request according to an implementation specification adopted in § 170.215(d).
13. DAT-PAT-13: The health IT developer demonstrates the ability of the Health IT Module to support a bulk data status request according to an implementation specification adopted in § 170.215(d).
14. DAT-PAT-14: The health IT developer demonstrates the ability of the Health IT Module to support a file request according to an implementation specification adopted in § 170.215(d), including support for the “ndjson” format for files provided.
15. DAT-PAT-15: The health IT developer demonstrates that the information provided as part of this data response includes data for patients in the group identifier provided during the “group-export” request.

HealthIT.gov

Access v2.0.0

Expires on January 1, 2026: (USCDI v1 + US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 + US Core STU v4.0.0)

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-1: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-8, of this section respectively, the tester verifies the ability of the Health IT Module to respond to requests for data according to the implementation specification adopted in § 170.215(b)(1)(i), including the following steps.
2. DAT-PAT-2: The tester verifies the ability of the Health IT Module to respond with data that meet the following conditions:
   - All data elements indicated with a cardinality of one or greater and / or "must support" are included;
   - Content is structurally correct;
   - All invariant rules are met;
   - All data elements with required "ValueSet" bindings contain codes within the bound "ValueSet";
   - All information is accurate and without omission; and
   - All references within the resources can be resolved and validated, as applicable, according to steps DAT-PAT-2, DAT-PAT-3, DAT-PAT-4, DAT-PAT-5, and DAT-PAT-6, of this section.
3. DAT-PAT-3: The tester verifies the ability of the Health IT Module to support a "Provenance" FHIR® resource for all the FHIR® resources included in the standard adopted in § 170.213(a) and implementation specification adopted in § 170.215(b)(1)(i) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(b)(1)(i).
4. DAT-PAT-4: The tester verifies the ability of the Health IT Module to support a "DocumentReference" and/or "DiagnosticReport" FHIR® resource for each of the "Clinical Notes" and "Diagnostic Reports" included in and according to the "Clinical Notes Guidance" section of the implementation specification adopted in § 170.215(b)(1)(i).
5. DAT-PAT-5: If supported, and for responses to data for a single patient only, the tester verifies the ability of the Health IT Module to support a "Medication" FHIR® resource according to the "Medication List Guidance" section of the implementation specification adopted in § 170.215(b)(1)(i).
6. DAT-PAT-6: The tester verifies the ability of the Health IT Module to support "Missing Data" according to the implementation specification adopted in § 170. 215(b)(1)(i), including:
   - For non-coded data elements; and
   - For coded data elements, including support for the "DataAbsentReason" Code System.

Note: We require the tester to verify support for the tests above for both responses to requests for a single patient's data and responses to requests for multiple patients' data because we make no assumption regarding the re-use of technical infrastructure for "read" services for single and multiple patients in Health IT Modules.

Response to Requests for a Single Patient's Data

7. DAT-PAT-7: The tester verifies the ability of the Health IT Module to return all of the data associated with requests for a single patient's data according to the "US Core Server CapabilityStatement" section of the implementation specification adopted in § 170.215(b)(1)(i) for all the data included in the standard adopted in § 170.213(a).

Response to Requests for Multiple Patients' Data

8. DAT-PAT-8: The tester verifies the ability of the Health IT Module to respond to requests for multiple patients' data according to an implementation specification adopted in § 170.215(d) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in § 170.213(a) and implementation specification adopted in § 170.215(b)(1)(i):
   - "AllergyIntolerance";
   - "CarePlan";

HealthIT.gov

- “DocumentReference”;
- “Encounter”;
- “Goal”;
- “Immunization”;
- “Location” (if supported);
- “Medication” (if supported);
- “MedicationRequest”;
- “Observation”;
- “Organization”;
- “Patient”;
- “Practitioner”
- “Procedure”; and
- “Provenance”.

9. DAT-PAT-9: The tester verifies the ability of the Health IT Module to limit the data returned to only those FHIR® resources for which the client is authorized according to an implementation specification adopted in § 170.215(d).
10. DAT-PAT-10: The tester verifies the ability of the Health IT Module to support a successful data response according to an implementation adopted in § 170.215(d).
11. DAT-PAT-11: The tester verifies the ability of the Health IT Module to support a data response error according to an implementation adopted in § 170.215(d).
12. DAT-PAT-12: The tester verifies the ability of the Health IT Module to support a bulk data delete request according to an implementation specification adopted in § 170.215(d).
13. DAT-PAT-13: The tester verifies the ability of the Health IT Module to support a bulk data status request according to an implementation specification adopted in § 170.215(d).
14. DAT-PAT-14: The tester verifies the ability of the Health IT Module to support a file request according to an implementation specification adopted in § 170.215(d), including support for the “ndjson” format for files provided.
15. DAT-PAT-15: The tester verifies the information provided as part of this data response includes data for patients in the group identifier provided during the “group-export” request.

Required by December 31, 2025: USCDI v3 + US Core STU v6.1.0

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-1: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-8, of this section respectively, the tester verifies the ability of the Health IT Module to respond to requests for data according to the implementation specification adopted in § 170.215(b)(1)(ii), including the following steps.
2. DAT-PAT-2: The tester verifies the ability of the Health IT Module to respond with data that meet the following conditions:

- All data elements indicated with a cardinality of one or greater and / or “must support” are included;
- Content is structurally correct;
- All invariant rules are met;
- All data elements with required “ValueSet” bindings contain codes within the bound “ValueSet”;
- All information is accurate and without omission; and
- All references within the resources can be resolved and validated, as applicable, according to steps DAT-PAT-2, DAT-PAT-3, DAT-PAT-4, DAT-PAT-5, and DAT-PAT-6, of this section.

3. DAT-PAT-3: The tester verifies the ability of the Health IT Module to support a “Provenance” FHIR® resource for all the FHIR® resources included in the standard adopted in § 170.213(b) and implementation specification adopted in § 170.215(b)(1)(ii) according to the “Basic Provenance Guidance” section of the implementation specification adopted in § 170.215(b)(1)(ii).

HealthIT.gov

5. DAT-PAT-5: If supported, and for responses to data for a single patient only, the tester verifies the ability of the Health IT Module to support a "Medication" FHIR® resource according to the "Medication List Guidance" section of the implementation specification adopted in § 170.215(b)(1)(ii).
6. DAT-PAT-6: The tester verifies the ability of the Health IT Module to support "Missing Data" according to the implementation specification adopted in § 170. 215(b)(1)(ii), including:
   - For non-coded data elements; and
   - For coded data elements, including support for the "DataAbsentReason" Code System.

Note: We require the health IT developers to demonstrate support for the tests above for both responses to requests for a single patient's data and responses to requests for multiple patients' data because we make no assumption regarding the re-use of technical infrastructure for "read" services for single and multiple patients in Health IT Modules.

Response to Requests for Single Patients' Data

7. DAT-PAT-7: The tester verifies the ability of the Health IT Module to return all of the data associated with requests for a single patient's data according to the "US Core Server CapabilityStatement" section of the implementation specification adopted in § 170.215(b)(1)(ii) for all the data included in the standard adopted in § 170.213(b).

Response to Requests for Multiple Patients' Data

8. DAT-PAT-17: The health IT developer verifies the ability of the Health IT Module to respond to requests for multiple patients' data according to an implementation specification adopted in § 170.215(d) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in § 170.213(b) and implementation specification adopted in § 170.215(b)(1)(ii).
   - "AllergyIntolerance";
   - "CarePlan";
   - "CareTeam";
   - "Condition";
   - "Coverage"
   - "Device";
   - "DiagnosticReport";
   - "DocumentReference";
   - "Encounter";
   - "Goal";
   - "Immunization";
   - "Location" (if supported);
   - "Medication" (if supported);
   - "MedicationDispense"
   - "MedicationRequest";
   - "Observation";
   - "Organization";
   - "Patient";
   - "Practitioner"
   - "Procedure";
   - "Provenance";
   - "PractitionerRole" (if supported);
   - "QuestionnaireReponse" (if supported);
   - "RelatedPerson";
   - "Specimen"; and
   - "ServiceRequest"

HealthIT.gov

according to an implementation adopted in § 170.215(d).

11. DAT-PAT-11: The tester verifies the ability of the Health IT Module to support a data response error according to an implementation adopted in § 170.215(d).
12. DAT-PAT-12: The tester verifies the ability of the Health IT Module to support a bulk data delete request according to an implementation specification adopted in § 170.215(d).
13. DAT-PAT-13: The tester verifies the ability of the Health IT Module to support a bulk data status request according to an implementation specification adopted in § 170.215(d).
14. DAT-PAT-14: The tester verifies the ability of the Health IT Module to support a file request according to an implementation specification adopted in § 170.215(d), including support for the “ndjson” format for files provided.
15. DAT-PAT-15: The tester verifies the information provided as part of this data response includes data for patients in the group identifier provided during the “group-export” request.

Paragraph (g)(10)(viii) – Documentation

System Under Test

Applies to all applicable regulatory and SVAP standards

API Documentation Requirements

1. API-DOC-1: The health IT developer supplies documentation describing the API(s) of the Health IT Module and includes at a minimum:
   - API syntax;
   - Function names;
   - Required and optional parameters supported and their data types;
   - Return variables and their types/structures;
   - Exceptions and exception handling methods and their returns;
   - Mandatory software components;
   - Mandatory software configurations; and
   - All technical requirements and attributes necessary for registration.
2. API-DOC-2: The health IT developer demonstrates that the documentation described in step API-DOC-1, of this section is available via a publicly accessible hyperlink that does not require preconditions or additional steps to access.
3. API-DOC-3: To fulfill the API Maintenance of Certification requirement at § 170.404(b)(2), the health IT developer demonstrates the public location of its certified API technology service base URLs and related organization details.

HealthIT.gov

API Documentation Requirements

1. API-DOC-1: The tester verifies the documentation supplied by the health IT developer describing the API(s) of the Health IT Module includes at a minimum:
   - API syntax;
   - Function names;
   - Required and optional parameters supported and their data types;
   - Return variables and their types/structures;
   - Exceptions and exception handling methods and their returns;
   - Mandatory software components;
   - Mandatory software configurations; and
   - All technical requirements and attributes necessary for registration.
2. API-DOC-2: The tester verifies the documentation described in step API-DOC-1, of this section is available via a publicly accessible hyperlink that does not require preconditions or additional steps to access.
3. API-DOC-3: To fulfill the API Maintenance of Certification requirement at § 170.404(b)(2), the tester verifies the public location of the health IT developer's certified API technology service base URLs and related organization details.

Content last reviewed on August 30, 2024