Standardized API for patient and population services

- Certification Companion Guide (CCG)
- Test Procedure

Updated on 11-26-2024

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.

1. *Data response*.
    1. 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.
    2. 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.
2. *Supported search operations*.
    1. 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."
    2. Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).
3. *Application registration*. Enable an application to register with the Health IT Module's "authorization server."

4. *Secure connection*.
    1. 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).
    2. 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).
5. *Authentication and authorization.*
    1. *Authentication and authorization for patient and user scopes.*
        1. *First time connections.*
            1. 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).
            2. 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).
            3. 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*.
            1. 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.
            2. A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).
    2. *Authentication and authorization for system scopes.* Authentication and authorization must occur during 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.
6. *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.
7. *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).

8. *Documentation*.
    1. 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.
    2. 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)

§ 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)

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)

None

Paragraph (g)(10)(vii)

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
- Applications supported through certified health IT
- Use of FHIR in apps through certified health IT
- 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 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
1.3	Updated tests for SVAP 2024 adopted standards.	11-13-2024
1.4	• Corrected test step IDs and references for Paragraph (g)(10)(v)(A) for SMART App Launch 2.0.0 and 2.2.0, adding test IDs AUT-PAT-33, AUT-PAT-34, AUT-PAT-35, AUT-PAT-36, and AUT-PAT-37 • Corrected test step IDs and references for Paragraph (g)(10)(i), section “Data Response Checks for Single and Multiple Patients” for US Core 6.1.0 and 7.0.0, adding test ID DAT-PAT-18 • Corrected missing references to US Core 7.0.0 for test steps AUT-PAT-32 and AUT-PAT-35	11-26-2024

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.

1. *Data response*.
    1. 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.
    2. 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.
2. *Supported search operations*.
    1. 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."
    2. Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).
3. *Application registration*. Enable an application to register with the Health IT Module's "authorization server."
4. *Secure connection*.
    1. 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).
    2. 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).

5. *Authentication and authorization.*
    1. *Authentication and authorization for patient and user scopes.*
        1. *First time connections.*
            1. 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).
            2. 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).
            3. 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*.
            1. 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.
            2. A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).
    2. *Authentication and authorization for system scopes.* Authentication and authorization must occur during 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.
6. *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.
7. *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).

8. *Documentation*.
    1. 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.
    2. 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)

§ 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)

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)

None

Paragraph (g)(10)(vii)

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
- Applications supported through certified health IT
- Use of FHIR in apps through certified health IT
- 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.

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

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 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
1.3	Updated tests for SVAP 2024 adopted standards.	11-13-2024

Version #	Description of Change	Version Date
1.4	• Corrected test step IDs and references for Paragraph (g)(10)(v)(A) for SMART App Launch 2.0.0 and 2.2.0, adding test IDs AUT-PAT-33, AUT-PAT-34, AUT-PAT-35, AUT-PAT-36, and AUT-PAT-37 • Corrected test step IDs and references for Paragraph (g)(10)(i), section “Data Response Checks for Single and Multiple Patients” for US Core 6.1.0 and 7.0.0, adding test ID DAT-PAT-18 • Corrected missing references to US Core 7.0.0 for test steps AUT-PAT-32 and AUT-PAT-35	11-26-2024

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

SVAP

Paragraph (g)(10) – (Conditional – For Modules with Existing Certification to (g)(10))

System Under Test

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.

System Under Test	ONC-ACB Verification
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.	**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).

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).

Paragraph (g)(10)(iv) – Secure connection

System Under Test

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.

System Under Test

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.

Paragraph (g)(10)(v)(A) – Authentication and authorization for patient and user scopes

System Under Test

Expires on January 1, 2026: SMART App Launch 1.0.0
Note: US Core 7.0.0 must be tested with SMART App Launch 2.0.0 or above.

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);
- "launch/patient" (to support "context-standalone-patient" "SMART on FHIR® Core Capability" for Standalone-Launch mode only);
- "launch" (for EHR-Launch mode only);
- "offline_access" (to support "permission-offline" "SMART on FHIR® Core Capability");
- 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-33, 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”;
- “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”).

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)
Note: Use this section if testing SMART App Launch 2.2.0.

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)(2).
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)(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 or 7.0.0:

"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”);
- 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 or 7.0.0, 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-33: [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, 6.1.0, or 7.0.0 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 or 7.0.0:

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

The following resources must also be supported if using US Core 7.0.0:

"Location"

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-34: [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-33, 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-37: [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-26, 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
- “state”.

16. AUT-PAT-30: [Both] The health IT developer demonstrates 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”;
- “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-35: [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 or 7.0.0: “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-36: [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-35 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 or 7.0.0: 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-35 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 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 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)(2).

Test Lab Verification

Expires on January 1, 2026: SMART App Launch 1.0.0
Note: US Core 7.0.0 must be tested with SMART App Launch 2.0.0 or above.

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);
- “offline_access” (to support “permission-offline” “SMART on FHIR® Core Capability”);
- 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 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 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”).

16. 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)(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 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)***
Note: Use this section if testing SMART App Launch 2.2.0.

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)(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”.

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)(2).
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-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 or 7.0.0:

"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 or 7.0.0, 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-33: [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 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, 6.1.0, or 7.0.0 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 or 7.0.0:

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

The following resources must also be supported if using US Core 7.0.0:

"Location"

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-34: [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-33, 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-37: [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-26, 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”;

- “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 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-35: [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 or 7.0.0:

“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-36: [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-35 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 or 7.0.0: 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-35 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).

System Under Test	Test Lab Verification
Expires on January 1, 2026: SMART App Launch 1.0.0 *Note: US Core 7.0.0 must be tested with SMART App Launch 2.0.0 or above.*	**Expires on January 1, 2026: SMART App Launch 1.0.0** *Note: US Core 7.0.0 must be tested with SMART App Launch 2.0.0 or above.*
Authentication and Authorization for Patient and User Scopes	**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).	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).

System Under Test

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

Test Lab Verification

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”).

System Under Test

- “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);

Test Lab Verification

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);

System Under Test

- “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);
- “offline_access” (to support “permission-offline” “SMART on FHIR® Core Capability”);
- 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”;

Test Lab Verification

- “launch/patient” (to support “context-standalone-patient” “SMART on FHIR® Core Capability” for Standalone-Launch mode only);
- “launch” (for EHR-Launch mode only);
- “offline_access” (to support “permission-offline” “SMART on FHIR® Core Capability”);
- 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 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 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”.

System Under Test

- “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-33, 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.

Test Lab Verification

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”.

System Under Test

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”;
- “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”).

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”;

Test Lab Verification

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”).

16. 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)(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 or 6.1.0:

System Under Test

- “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).

Test Lab Verification

“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).

System Under Test

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

Test Lab Verification

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)***
Note: Use this section if testing SMART App Launch 2.2.0.

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)(2).

System Under Test

and 4.0.0 expire on January 1, 2026)
Note: Use this section if testing SMART App Launch 2.2.0.

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)(2).
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)(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).

Test Lab Verification

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".

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)(2).
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-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";

System Under Test

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 or 7.0.0:

"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"

Test Lab Verification

- "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 or 7.0.0:

"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).

System Under Test

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");
- 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"

Test Lab Verification

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"

System Under Test

- 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 or 7.0.0, 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-33: [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, 6.1.0, or 7.0.0 these resources include:

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

Test Lab Verification

- 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 or 7.0.0, 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-33: [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 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, 6.1.0, or 7.0.0 these resources include:

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

System Under Test

- “Patient”;
- “Procedure”; and
- “Provenance”.

The following resources must also be supported if using US Core 6.1.0 or 7.0.0:

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

The following resources must also be supported if using US Core 7.0.0:

"Location"

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-34: [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-33, 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).

Test Lab Verification

- “Patient”;
- “Procedure”; and
- “Provenance”.

The following resources must also be supported if using US Core 6.1.0 or 7.0.0:

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

The following resources must also be supported if using US Core 7.0.0:

"Location"

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-34: [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-33, 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).

System Under Test

14. AUT-PAT-37: [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-26, 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
    - “state”.

16. AUT-PAT-30: [Both] The health IT developer demonstrates 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”;
    - “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”)

Test Lab Verification

14. AUT-PAT-37: [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-26, 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”;
    - “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”)

System Under Test

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-35: [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 or 7.0.0: “encounter” (to support "context-ehr-encounter" “SMART on FHIR® Capability”)

Test Lab Verification

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-35: [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 or 7.0.0:

“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:

System Under Test

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-36: [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-35 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 or 7.0.0: 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-35 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).

Test Lab Verification

- 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-36: [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-35 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 or 7.0.0: 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-35 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

System Under Test

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 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 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)(2).

Test Lab Verification

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).

Paragraph (g)(10)(vi) – Patient authorization revocation

System Under Test

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.

System Under Test	Test Lab Verification
Applies to all applicable regulatory and SVAP standards	*Applies to all applicable regulatory and SVAP standards*
Patient Authorization Revocation	**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.	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.

Paragraph (g)(10)(v)(B) – Authentication and authorization for system scopes

System Under Test

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).

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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).

System Under Test

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):

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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”.

System Under Test

- “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).

Test Lab Verification

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).

System Under Test

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).

Test Lab Verification

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).

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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).

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).

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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).

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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).

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.

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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.

System Under Test

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).

Test Lab Verification

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

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).

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).

Paragraph (g)(10)(i) – Data response

System Under Test

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 and US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 and 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® 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”;
- “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 and US Core STU v6.1.0
Note: Use this section if testing USCDI v4 and US Core 7.0.0.

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-18: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-17, 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.

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(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).
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 or using US Core 7.0.0);
- “Medication” (if supported);
- “MedicationDispense”
- “MedicationRequest”;
- “Observation”;
- “Organization”;
- “Patient”;
- “Practitioner”
- “Procedure”;
- “Provenance”;
- “PractitionerRole” (if supported);
- “QuestionnaireReponse” (if supported);
- “RelatedPerson”;
- “Specimen”; and
- “ServiceRequest”

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.

Test Lab Verification

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 and US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 and 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";
- "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 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 and US Core STU v6.1.0
Note: Use this section if testing USCDI v4 and US Core 7.0.0.

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-18: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-17, 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).
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)(ii).
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 or using US Core 7.0.0);
- "Medication" (if supported);
- "MedicationDispense"
- "MedicationRequest";
- "Observation";
- "Organization";
- "Patient";
- "Practitioner"
- "Procedure";
- "Provenance";
- "PractitionerRole" (if supported);
- "QuestionnaireReponse" (if supported);
- "RelatedPerson";
- "Specimen"; and
- "ServiceRequest"

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.

System Under Test

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 and US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 and 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:

Test Lab Verification

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 and US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 and 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:

System Under Test

- 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).

Test Lab Verification

- 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).

System Under Test

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® 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):

Test Lab Verification

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):

System Under Test

- “AllergyIntolerance”;
- “CarePlan”;
- “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).

Test Lab Verification

- “AllergyIntolerance”;
- “CarePlan”;
- “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 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).

System Under Test

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 and US Core STU v6.1.0
Note: Use this section if testing USCDI v4 and US Core 7.0.0.

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-18: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-17, 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

Test Lab Verification

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 and US Core STU v6.1.0
Note: Use this section if testing USCDI v4 and US Core 7.0.0.

Data Response Checks for Single and Multiple Patients

1. DAT-PAT-18: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-17, 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.

System Under Test

- 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(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).
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.

Test Lab Verification

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).
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)(ii).
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

System Under Test

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";

Test Lab Verification

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 or using US Core 7.0.0);
- "Medication" (if supported);
- "MedicationDispense"
- "MedicationRequest";
- "Observation";

System Under Test

- “Location” (if supported or using US Core 7.0.0);
- “Medication” (if supported);
- “MedicationDispense”
- “MedicationRequest”;
- “Observation”;
- “Organization”;
- “Patient”;
- “Practitioner”
- “Procedure”;
- “Provenance”;
- “PractitionerRole” (if supported);
- “QuestionnaireReponse” (if supported);
- “RelatedPerson”;
- “Specimen”; and
- “ServiceRequest”

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).

Test Lab Verification

- “Organization”;
- “Patient”;
- “Practitioner”
- “Procedure”;
- “Provenance”;
- “PractitionerRole” (if supported);
- “QuestionnaireReponse” (if supported);
- “RelatedPerson”;
- “Specimen”; and
- “ServiceRequest”

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.

System Under Test

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.

Test Lab Verification

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.

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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.

System Under Test	Test Lab Verification

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.

Test Lab Verification

Applies to all applicable regulatory and SVAP standards

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.

Updated on 03-27-2025

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.

1. *Data response*.
    1. 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.
    2. 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.
2. *Supported search operations*.
    1. 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."
    2. Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).
3. *Application registration*. Enable an application to register with the Health IT Module's "authorization server."
4. *Secure connection*.
    1. 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).
    2. 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).

5. *Authentication and authorization.*
    1. *Authentication and authorization for patient and user scopes.*
        1. *First time connections.*
            1. 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).
            2. 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).
            3. 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*.
            1. 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.
            2. A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).
    2. *Authentication and authorization for system scopes.* Authentication and authorization must occur during 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.
6. *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.
7. *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).

8. *Documentation*.
    1. 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.
    2. 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)

§ 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)

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)

None

Paragraph (g)(10)(vii)

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
- Applications supported through certified health IT
- Use of FHIR in apps through certified health IT
- 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 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
1.3	Updated tests for SVAP 2024 adopted standards.	11-13-2024
1.4	• Corrected test step IDs and references for Paragraph (g)(10)(v)(A) for SMART App Launch 2.0.0 and 2.2.0, adding test IDs AUT-PAT-33, AUT-PAT-34, AUT-PAT-35, AUT-PAT-36, and AUT-PAT-37 • Corrected test step IDs and references for Paragraph (g)(10)(i), section “Data Response Checks for Single and Multiple Patients” for US Core 6.1.0 and 7.0.0, adding test ID DAT-PAT-18 • Corrected missing references to US Core 7.0.0 for test steps AUT-PAT-32 and AUT-PAT-35	11-26-2024

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.

1. *Data response*.
    1. 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.
    2. 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.
2. *Supported search operations*.
    1. 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."
    2. Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(d).
3. *Application registration*. Enable an application to register with the Health IT Module's "authorization server."
4. *Secure connection*.
    1. 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).
    2. 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).

5. *Authentication and authorization.*
    1. *Authentication and authorization for patient and user scopes.*
        1. *First time connections.*
            1. 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).
            2. 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).
            3. 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*.
            1. 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.
            2. A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).
    2. *Authentication and authorization for system scopes.* Authentication and authorization must occur during 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.
6. *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.
7. *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).

8. *Documentation*.
    1. 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.
    2. 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)

§ 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)

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)

None

Paragraph (g)(10)(vii)

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
- Applications supported through certified health IT
- Use of FHIR in apps through certified health IT
- 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 paragraph (g)(10)(vi) are required by March 11, 2024. • Revised clarification for paragraph (g)(10)(i)(A) for US Core 6.1.0 and USCDI v3 to indicate that for the “Practitioner” US Core IG profile only the “read” type interaction must be supported.	05-16-2024
1.2	Updated a typo in 170.215(d)(1) standard referenced to reflect the correct version cited in regulation as V1.0.0.	07-22-2024
1.3	• For Paragraph (g)(10)(i)(A), added a clarification in alignment with US Core 'Patch' Process ticket FHIR-45319. • For Paragraph (g)(10)(v)(A)(1), added new clarification regarding support for authorization requests simultaneously including both SMART v1 and SMART v2 scopes, and revised and added clarifications regarding support for granular SMART v2 scopes defined using “Finer-grained resource constraints using search parameters”.	08-05-2024
1.4	Standards Referenced updated to reflect the 2024 Approved SVAP Standards.	08-19-2024

Version #	Description of Change	Version Date
1.5	• Applicable to the entire criterion: Added clarifications regarding US Core “patches” and “additional guidance” approved by the HL7 Cross-Group Projects Work Group. • For Paragraph (g)(10)(i)(A), added clarifications for US Core “patches” FHIR-43355 and FHIR-44693.	08-30-2024
1.6	For Paragraph (g)(10)(i)(A), added clarification for US Core “patch” FHIR-46240.	11-05-2024
1.7	Updated clarifications for SVAP 2024 adopted standards.	11-13-2024
1.8	• Updated link for § 170.215(c)(2) HL7® SMART App Launch Implementation Guide Release 2.0.0 under Standard(s) Referenced • For entire criterion, added clarification regarding compliance with EO 14168 and OPM guidance	03-27-2025

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

Certification Companion Guide: Standardized API for patient and population services

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

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

Base EHR Definition	Real World Testing	Insights Condition	SVAP	Requires Updates
Included	Yes	Yes	Yes	Yes

Certification Requirements

Technical Explanations and Clarifications

Applies to Entire Criterion

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT Modules are not required to support patient-facing API-enabled “read” services for multiple patients for the purposes of this certification criterion.
- The clinical note text included in any of the notes described in the “Clinical Notes Guidance” section of a US Core Implementation Guide (IG) adopted in § 170.215(b)(1) must be represented in a “plain text” form, and it would be unacceptable for the note text to be converted to another file or format (e.g., .docx, PDF) when it is provided as part of an API response. The intent of this policy is to prohibit Health IT Modules from converting clinical notes from a “machine readable” format to a non-“machine readable” format (e.g., PDF). Clinical note text that originates from outside Health IT Modules should be exchanged using its original format. Additionally, “plain text” does not necessarily mean the FHIR® “contentType” “text/plain.”
- The US Core IG Profile “StructureDefinition-us-core-patient” element “name.suffix” is required for testing and certification in the Certification Program to meet the USCDI requirement to support the “Patient Demographics” Data Class: “Suffix” Data Element.
- A Health IT Module must support at least one Choice or Reference for US Core IG “must support” elements with multiple Choices or References, respectively.
- A Health IT Module must be conformant to the US Core IG for all Choices and References included in its standardized API, and cannot misrepresent Choices via the standardized API (e.g. a Health IT Module cannot transform “integer” values to “string” values).

- A health IT developer must document which US Core IG Choices and References are supported by their Health IT Module via public technical documentation to meet the requirements at § 170.315(g)(10)(viii) and the transparency conditions at § 170.404(a)(2).
- Information originating from the (g)(10)-certified Health IT Module must conform to the requirements included in the criterion, but legacy information and information from outside systems is not required to be mapped to the USCDI "Applicable Standards" and the US Core IG terminologies and value sets. However, health IT developers are encouraged to exceed the minimum requirements described in § 170.315(g)(10) to support the mapping of legacy information to the terminologies and value sets included in the USCDI and US Core IG where possible.
- In order to mitigate potential interoperability errors and inconsistent implementation of the Fast Healthcare Interoperability Resources (FHIR®) Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1) standard, ONC assesses, approves, and incorporates corrections (errata) as part of required certification and testing to this criterion. Compliance with the following errata is necessary because the errata implements technical corrections and clarifications to the FHIR® Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1) standard. There is a 90-day delay from the time the CCG has been updated with the ONC-approved errata to when compliance with the errata will be required to pass testing. Similarly, there will be an 18-month delay before a finding of an erratum's absence in a Certified Health IT Module during surveillance would constitute a non-conformity under the Certification Program.

    Version: FHIR® Bulk Data Access (Flat FHIR®) (v1.0.1: STU 1). Effective for testing on October 25, 2021. Surveillance compliance date on January 27, 2023.
- Through the US Core Patch Process, the HL7® Cross-Group Projects Work Group (CGP WG) approves US Core "patches", which are corrections for issues with the US Core implementation guide (US Core IG). US Core "patches" include corrections for issues such as ambiguous requirements and requirements incompatible with real world deployment. Similar to US Core "patches" are US Core "additional guidance". US Core "additional guidance" approved by the CGP WG indicates guidance included in a newer version of the US Core IG as being relevant to a previous version of the US Core IG. Though US Core "patches" and "additional guidance" are not required for certification purposes (unless indicated in the Certification Companion Guide), health IT developers may optionally implement US Core "additional guidance" in their Health IT Module and still be conformant with § 170.315(g)(10) criterion requirements.
- More information regarding the US Core Patch Process and US Core "patches" and "additional guidance" approved by the CGP WG is available on the HL7® Confluence pages of US Core 'Patch' Process and Approved Patches and Additional Guidance.

- Consistent with Executive Order (EO) 14168 and OPM guidance, Health IT Modules certifying and/or currently certified to certification criteria that cross-reference the USCDI standard at 45 CFR 170.213 are only required to demonstrate the capability to categorize data on individuals for the sex data element in accordance with the following SNOMED CT® codes:
    - 248152002 |Female (finding)| and
    - 248153007 |Male (finding)|
- Further, these Health IT Modules are no longer required to support the following USCDI data elements for purposes of certification:
    - Sexual orientation in USCDI version 4;
    - Gender identity in USCDI version 4;
    - Sex parameter for clinical use in USCDI version 5;
    - Name to use in USCDI version 5;
    - Pronouns in USCDI version 5.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standards US Core 4.0.0 (expires on January 1, 2026):

The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-40299, approved patching the US Core Patient Profile in US Core 3.1.1 and US Core 4.0.0. The USCDI data element “Patient Demographics: Previous Name” must be supported by including the capability to set the US Core Patient Profile element “Patient.name.use” to “old” or provide an end date in “Patient.name.period” element or support both. Additionally, the USCDI data element “Patient Demographics: Previous Address” must be supported by including the capability to set the US Core Patient Profile “Patient.address.use” element to “old” or provide an end date in “Patient.address.period” element or support both. Also, support for the US Core Patient Profile “Patient.address.period” element is not required for purposes of testing and certification.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT Modules are not required to support patient-facing API-enabled “read” services for multiple patients for the purposes of this certification criterion.

- The clinical note text included in any of the notes described in the "Clinical Notes Guidance" section of a US Core Implementation Guide (IG) adopted in § 170.215(b)(1) must be represented in a "plain text" form, and it would be unacceptable for the note text to be converted to another file or format (e.g., .docx, PDF) when it is provided as part of an API response. The intent of this policy is to prohibit Health IT Modules from converting clinical notes from a "machine readable" format to a non-"machine readable" format (e.g., PDF). Clinical note text that originates from outside Health IT Modules should be exchanged using its original format. Additionally, "plain text" does not necessarily mean the FHIR® "contentType" "text/plain."
- The US Core IG Profile "StructureDefinition-us-core-patient" element "name.suffix" is required for testing and certification in the Certification Program to meet the USCDI requirement to support the "Patient Demographics" Data Class: "Suffix" Data Element.
- A Health IT Module must support at least one Choice or Reference for US Core IG "must support" elements with multiple Choices or References, respectively.
- A Health IT Module must be conformant to the US Core IG for all Choices and References included in its standardized API, and cannot misrepresent Choices via the standardized API (e.g. a Health IT Module cannot transform "integer" values to "string" values).
- A health IT developer must document which US Core IG Choices and References are supported by their Health IT Module via public technical documentation to meet the requirements at § 170.315(g)(10)(viii) and the transparency conditions at § 170.404(a)(2).
- Information originating from the (g)(10)-certified Health IT Module must conform to the requirements included in the criterion, but legacy information and information from outside systems is not required to be mapped to the USCDI "Applicable Standards" and the US Core IG terminologies and value sets. However, health IT developers are encouraged to exceed the minimum requirements described in § 170.315(g)(10) to support the mapping of legacy information to the terminologies and value sets included in the USCDI and US Core IG where possible.
- In order to mitigate potential interoperability errors and inconsistent implementation of the Fast Healthcare Interoperability Resources (FHIR®) Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1) standard, ONC assesses, approves, and incorporates corrections (errata) as part of required certification and testing to this criterion. Compliance with the following errata is necessary because the errata implements technical corrections and clarifications to the FHIR® Bulk Data Access (Flat FHIR®) (v1.0.0: STU 1) standard. There is a 90-day delay from the time the CCG has been updated with the ONC-approved errata to when compliance with the errata will be required to pass testing. Similarly, there will be an 18-month delay before a finding of an erratum's absence in a Certified Health IT Module during surveillance would constitute a non-conformity under the Certification Program.

    Version: FHIR® Bulk Data Access (Flat FHIR®) (v1.0.1: STU 1). Effective for testing on October 25, 2021. Surveillance compliance date on January 27, 2023.

- Through the US Core Patch Process, the HL7® Cross-Group Projects Work Group (CGP WG) approves US Core “patches”, which are corrections for issues with the US Core implementation guide (US Core IG). US Core “patches” include corrections for issues such as ambiguous requirements and requirements incompatible with real world deployment. Similar to US Core “patches” are US Core “additional guidance”. US Core “additional guidance” approved by the CGP WG indicates guidance included in a newer version of the US Core IG as being relevant to a previous version of the US Core IG. Though US Core “patches” and “additional guidance” are not required for certification purposes (unless indicated in the Certification Companion Guide), health IT developers may optionally implement US Core “additional guidance” in their Health IT Module and still be conformant with § 170.315(g)(10) criterion requirements.
- More information regarding the US Core Patch Process and US Core “patches” and “additional guidance” approved by the CGP WG is available on the HL7® Confluence pages of US Core 'Patch' Process and Approved Patches and Additional Guidance.
- Consistent with Executive Order (EO) 14168 and OPM guidance, Health IT Modules certifying and/or currently certified to certification criteria that cross-reference the USCDI standard at 45 CFR 170.213 are only required to demonstrate the capability to categorize data on individuals for the sex data element in accordance with the following SNOMED CT® codes:
  - 248152002 |Female (finding)| and
  - 248153007 |Male (finding)|
- Further, these Health IT Modules are no longer required to support the following USCDI data elements for purposes of certification:
  - Sexual orientation in USCDI version 4;
  - Gender identity in USCDI version 4;
  - Sex parameter for clinical use in USCDI version 5;
  - Name to use in USCDI version 5;
  - Pronouns in USCDI version 5.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standards US Core 4.0.0 (expires on January 1, 2026):

The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-40299, approved patching the US Core Patient Profile in US Core 3.1.1 and US Core 4.0.0. The USCDI data element “Patient Demographics: Previous Name” must be supported by including the capability to set the US Core Patient Profile element “Patient.name.use” to “old” or provide an end date in “Patient.name.period” element or support both. Additionally, the USCDI data element “Patient Demographics: Previous Address” must be supported by including the capability to set the US Core Patient Profile “Patient.address.use” element to “old” or provide an end date in “Patient.address.period” element or support both. Also, support for the US Core Patient Profile “Patient.address.period” element is not required for purposes of testing and certification.

Paragraph (g)(10)(i)(A) Data response – single patient

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- All data elements and operations indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported and are in-scope for testing.
- Health IT Modules must support provenance according to the "Basic Provenance Guidance" section of the US Core IG.
- For purposes of ONC Health IT Certification, health IT developers that always provide HL7® FHIR® "observation" values are not required to demonstrate Health IT Module support for "dataAbsentReason" elements. These include "dataAbsentReason" elements contained in the US Core implementation guide profiles and FHIR® Vital Sign profiles that build on the HL7® FHIR® "observation" and its derived profiles including HL7® FHIR® "observation-vitalsigns", and HL7® FHIR® "observation-oxygensat", including "component.dataAbsentReason" elements. However, health IT developers are still required to adhere to and demonstrate Health IT Module support for the "Missing Data" section of the US Core implementation guide.
- For purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the "USCoreFetchDocumentReferences" ($docref) US Core IG operation.

Applies to USCDI v1 and US Core 3.1.1 (expires on January 1, 2026)

The HL7® Cross-Group Projects work group, through the US Core 'Patch' Process ticket FHIR-28393, approved patching US Core 3.1.1 to remove "must support" from the "DocumentReference.custodian" data element. For the purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the "custodian" data element in the "DocumentReference" US Core 3.1.1 IG Profile.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standard US Core 4.0.0 (expires on January 1, 2026):

- For “Encounter,” “Organization,” and “Practitioner,” US Core IG profiles, only the “read” type interaction must be supported and will be included in testing and certification. For the “Location” FHIR® resource, Health IT Modules must either demonstrate support for the “read” type interaction or demonstrate support for providing the “Location” and FHIR® resource references as a contained resource. The “search” type interactions for these profiles and resource are not in scope for testing and certification. Health IT Modules must support these US Core IG profiles / FHIR® resource because they are included as “must support” data elements in US Core IG profiles required by the United States Core Data for Interoperability (USCDI).
- Health IT Modules must support provenance according to the “Basic Provenance Guidance” section of the US Core IG.

Applies to USCDI v3 and US Core 6.1.0 (required by December 31, 2025):

- The HL7® Cross-Group Projects workgroup approved the US Core 'Patch' Process ticket FHIR-45319 for US Core 6.1.0. In alignment with that issued guidance, the Health IT Module must support all four codes from the US Core Screening Assessment Observation Category ValueSet for the US Core Observation Screening Assessment Profile for “Observation.category:screening-assessment”. Additionally, the Health IT Module must support the “sdoh” code from the US Core Screening Assessment Condition Category ValueSet for the US Core Condition Problems and Health Concerns Profile for “Condition.category:screening-assessment”.
- For the “Organization” and "Practitioner" US Core IG profile, only the “read” type interaction must be supported and will be included in testing and certification. For the “Location” FHIR® resource, Health IT Modules must either demonstrate support for the “read” type interaction or demonstrate support for providing the “Location” FHIR® resource reference as a contained resource. The “search” type interactions for these profiles and resource are not in scope for testing and certification. Health IT Modules must support these US Core IG profiles / FHIR® resource because they are included as “must support” data elements in US Core IG profiles required by the United States Core Data for Interoperability (USCDI).
- For purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the “QuestionnaireResponse” US Core IG profile.
- The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-43355, approved patching the US Core Smoking Status Observation Profile in US Core 6.1.0. For purposes of certification, the clinically relevant time/time-period for observation for the US Core Smoking Status Observation Profile may be supported using either Observation.effectiveDateTime or Observation.effectivePeriod data elements, where Observation.effectivePeriod has the “Period” type.

- The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-44693, approved patching the US Core Practitioner Profile in US Core 6.1.0. For purposes of certification, Practitioner.address from the US Core Practitioner Profile is not required to be supported if the Health IT Module supports the US Core PractitionerRole Profile.
- The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-46240, approved patching the US Core DiagnosticReport Profile for Report and Note Exchange in US Core 6.1.0. For purposes of certification, DiagnosticReport.media and DiagnosticReport.media.link from the US Core DiagnosticReport Profile for Report and Note Exchange are not required to be supported.

Applies to SVAP approved standards USCDI v4 and US Core 7.0.0:

- For the “Organization” and “Practitioner” US Core IG profiles, only the “read” type interaction must be supported and will be included in testing and certification. The “search” type interactions for these profiles are not in scope for testing and certification. Health IT Modules must support these US Core IG profiles because they are included as “must support” data elements in US Core IG profiles required by the United States Core Data for Interoperability (USCDI).
- For purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the “QuestionnaireResponse” US Core IG profile.

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- All data elements and operations indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported and are in-scope for testing.
- Health IT Modules must support provenance according to the “Basic Provenance Guidance” section of the US Core IG.

- For purposes of ONC Health IT Certification, health IT developers that always provide HL7® FHIR® “observation” values are not required to demonstrate Health IT Module support for “dataAbsentReason” elements. These include “dataAbsentReason” elements contained in the US Core implementation guide profiles and FHIR® Vital Sign profiles that build on the HL7® FHIR® “observation” and its derived profiles including HL7® FHIR® “observation-vitalsigns”, and HL7® FHIR® “observation-oxygensat”, including “component.dataAbsentReason” elements. However, health IT developers are still required to adhere to and demonstrate Health IT Module support for the “Missing Data” section of the US Core implementation guide.
- For purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the “USCoreFetchDocumentReferences” ($docref) US Core IG operation.

Applies to USCDI v1 and US Core 3.1.1 (expires on January 1, 2026)

The HL7® Cross-Group Projects work group, through the US Core 'Patch' Process ticket FHIR-28393, approved patching US Core 3.1.1 to remove "must support" from the "DocumentReference.custodian" data element. For the purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the “custodian” data element in the “DocumentReference” US Core 3.1.1 IG Profile.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standard US Core 4.0.0 (expires on January 1, 2026):

- For “Encounter,” “Organization,” and “Practitioner,” US Core IG profiles, only the “read” type interaction must be supported and will be included in testing and certification. For the “Location” FHIR® resource, Health IT Modules must either demonstrate support for the “read” type interaction or demonstrate support for providing the “Location” and FHIR® resource references as a contained resource. The “search” type interactions for these profiles and resource are not in scope for testing and certification. Health IT Modules must support these US Core IG profiles / FHIR® resource because they are included as “must support” data elements in US Core IG profiles required by the United States Core Data for Interoperability (USCDI).
- Health IT Modules must support provenance according to the “Basic Provenance Guidance” section of the US Core IG.

Applies to USCDI v3 and US Core 6.1.0 (required by December 31, 2025):

- The HL7® Cross-Group Projects workgroup approved the US Core 'Patch' Process ticket FHIR-45319 for US Core 6.1.0. In alignment with that issued guidance, the Health IT Module must support all four codes from the US Core Screening Assessment Observation Category ValueSet for the US Core Observation Screening Assessment Profile for “Observation.category:screening-assessment”. Additionally, the Health IT Module must support the “sdoh” code from the US Core Screening Assessment Condition Category ValueSet for the US Core Condition Problems and Health Concerns Profile for “Condition.category:screening-assessment”.

- For the “Organization” and "Practitioner" US Core IG profile, only the “read” type interaction must be supported and will be included in testing and certification. For the “Location” FHIR® resource, Health IT Modules must either demonstrate support for the “read” type interaction or demonstrate support for providing the “Location” FHIR® resource reference as a contained resource. The “search” type interactions for these profiles and resource are not in scope for testing and certification. Health IT Modules must support these US Core IG profiles / FHIR® resource because they are included as “must support” data elements in US Core IG profiles required by the United States Core Data for Interoperability (USCDI).
- For purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the “QuestionnaireResponse” US Core IG profile.
- The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-43355, approved patching the US Core Smoking Status Observation Profile in US Core 6.1.0. For purposes of certification, the clinically relevant time/time-period for observation for the US Core Smoking Status Observation Profile may be supported using either Observation.effectiveDateTime or Observation.effectivePeriod data elements, where Observation.effectivePeriod has the “Period” type.
- The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-44693, approved patching the US Core Practitioner Profile in US Core 6.1.0. For purposes of certification, Practitioner.address from the US Core Practitioner Profile is not required to be supported if the Health IT Module supports the US Core PractitionerRole Profile.
- The HL7® Cross-Group Projects workgroup, through the US Core 'Patch' Process ticket FHIR-46240, approved patching the US Core DiagnosticReport Profile for Report and Note Exchange in US Core 6.1.0. For purposes of certification, DiagnosticReport.media and DiagnosticReport.media.link from the US Core DiagnosticReport Profile for Report and Note Exchange are not required to be supported.

Applies to SVAP approved standards USCDI v4 and US Core 7.0.0:

- For the “Organization” and “Practitioner” US Core IG profiles, only the “read” type interaction must be supported and will be included in testing and certification. The “search” type interactions for these profiles are not in scope for testing and certification. Health IT Modules must support these US Core IG profiles because they are included as “must support” data elements in US Core IG profiles required by the United States Core Data for Interoperability (USCDI).
- For purposes of testing and certification, health IT developers are not required to demonstrate Health IT Module support for the “QuestionnaireResponse” US Core IG profile.

Paragraph (g)(10)(i)(B) Data response – multiple patients

Technical outcome – 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 corresponding standard adopted in § 170.213. All data

elements indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT Modules may support scopes using either the system wildcard scope syntax or a list of -system resource scopes- to enable the export of multiple patients’ data as a group.
- During testing and certification for multiple patient services, Health IT Modules must demonstrate support for “Encounter,” “Organization,” and “Practitioner” US Core IG FHIR® Profiles.
- Health IT Modules must support provenance according to the “Basic Provenance Guidance” section of the US Core IG.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standards US Core 4.0.0 (expires on January 1, 2026) and USCDI v3 and US Core 6.1.0 (required by December 31, 2025):

Health IT Modules must demonstrate support for the “Location” FHIR® resource by either by providing this resource as part of the multiple patient services response, or by including it as a contained resource as part of the multiple patient services response.

Technical outcome – 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 corresponding standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT Modules may support scopes using either the system wildcard scope syntax or a list of -system resource scopes- to enable the export of multiple patients' data as a group.
- During testing and certification for multiple patient services, Health IT Modules must demonstrate support for "Encounter," "Organization," and "Practitioner" US Core IG FHIR® Profiles.
- Health IT Modules must support provenance according to the "Basic Provenance Guidance" section of the US Core IG.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standards US Core 4.0.0 (expires on January 1, 2026) and USCDI v3 and US Core 6.1.0 (required by December 31, 2025):

> Health IT Modules must demonstrate support for the "Location" FHIR® resource by either by providing this resource as part of the multiple patient services response, or by including it as a contained resource as part of the multiple patient services response.

Paragraph (g)(10)(ii)(A) Supported search operations – single patient

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported and are in scope for testing.
- The § 170.315(g)(10) certification criterion requires Health IT Modules to support API-enabled "read" services for single and multiple patients. "Read" services include those that allow authenticated and authorized third-party applications to view EHI through a secure API. These services specifically exclude "write" capabilities, where authenticated and authorized third-party applications would be able to create or modify EHI through a secure API.

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported and are in scope for testing.
- The § 170.315(g)(10) certification criterion requires Health IT Modules to support API-enabled "read" services for single and multiple patients. "Read" services include those that allow authenticated and authorized third-party applications to view EHI through a secure API. These services specifically exclude "write" capabilities, where authenticated and authorized third-party applications would be able to create or modify EHI through a secure API.

Paragraph (g)(10)(ii)(B) Supported search operations - multiple patients

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

No additional clarifications.

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

No additional clarifications.

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

Technical outcome – Enable an application to register with the Health IT Module's "authorization server."

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT presented for testing and certification must support app registration regardless of the scope of patient search utilized by the application (e.g., single or multiple).
- This certification criterion requires a health IT developer, as finalized in the Condition of Certification requirements, to demonstrate its registration process, but does not require conformance to a standard.
- The third-party application registration process that a health IT developer must meet under this criterion is not a form of review or “vetting” for purposes of this criterion.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standard US Core 4.0.0 (expires on January 1, 2026):

For demonstration of the SMART IG "Standalone Launch" steps, health IT developers are permitted to scope US Core IG resources that do not exist in either the standard adopted at § 170.213(a) (USCDI v1) or the "Compartment Patient" section of the standard adopted at § 170.215(a)(1) (HL7® FHIR® Release 4.0.1) as either patient/[Resource] or user/[Resource]. These resources include “Encounter,” “Device,” “Location,” “Medication,” “Organization,” “Practitioner,” and “PractitionerRole.” Health IT developers must document their supported scopes according to the technical documentation requirements at § 170.315(g)(10)(viii)(A) and § 170.404(a)(2).

Applies to USCDI v3 and US Core 6.1.0 (required by December 31, 2025):

For demonstration of the SMART IG “Standalone Launch” steps, health IT developers are permitted to scope US Core IG resources that do not exist in either the standard adopted at § 170.213(b) (USCDI v3) or the “Compartment Patient” section of the standard adopted at § 170.215(a)(1) (HL7® FHIR® Release 4.0.1) as either patient/[Resource] or user/[Resource]. These resources include “Device,” “Location,” “Medication,” “Organization,” “Practitioner,” and “PractitionerRole.” Health IT developers must document their supported scopes according to the technical documentation requirements at § 170.315(g)(10)(viii)(A) and § 170.404(a)(2).

Applies to SVAP approved standards USCDI v4 and US Core 7.0.0:

For demonstration of the SMART IG “Standalone Launch” steps, health IT developers are permitted to scope US Core IG resources that do not exist in either USCDI v4 or the “Compartment Patient” section of the standard adopted at § 170.215(a)(1) (HL7® FHIR® Release 4.0.1) as either patient/[Resource] or user/[Resource]. These resources include “Device,” “Medication,” “Organization,” “Practitioner,” and “PractitionerRole.” Health IT developers must document their supported scopes according to the technical documentation requirements at § 170.315(g)(10)(viii)(A) and § 170.404(a)(2).

Technical outcome – Enable an application to register with the Health IT Module's "authorization server."

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT presented for testing and certification must support app registration regardless of the scope of patient search utilized by the application (e.g., single or multiple).
- This certification criterion requires a health IT developer, as finalized in the Condition of Certification requirements, to demonstrate its registration process, but does not require conformance to a standard.
- The third-party application registration process that a health IT developer must meet under this criterion is not a form of review or "vetting" for purposes of this criterion.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standard US Core 4.0.0 (expires on January 1, 2026):

> For demonstration of the SMART IG "Standalone Launch" steps, health IT developers are permitted to scope US Core IG resources that do not exist in either the standard adopted at § 170.213(a) (USCDI v1) or the "Compartment Patient" section of the standard adopted at § 170.215(a)(1) (HL7® FHIR® Release 4.0.1) as either patient/[Resource] or user/[Resource]. These resources include "Encounter," "Device," "Location," "Medication," "Organization," "Practitioner," and "PractitionerRole." Health IT developers must document their supported scopes according to the technical documentation requirements at § 170.315(g)(10)(viii)(A) and § 170.404(a)(2).

Applies to USCDI v3 and US Core 6.1.0 (required by December 31, 2025):

> For demonstration of the SMART IG "Standalone Launch" steps, health IT developers are permitted to scope US Core IG resources that do not exist in either the standard adopted at § 170.213(b) (USCDI v3) or the "Compartment Patient" section of the standard adopted at § 170.215(a)(1) (HL7® FHIR® Release 4.0.1) as either patient/[Resource] or user/[Resource]. These resources include "Device," "Location," "Medication," "Organization," "Practitioner," and "PractitionerRole." Health IT developers must document their supported scopes according to the technical documentation requirements at § 170.315(g)(10)(viii)(A) and § 170.404(a)(2).

Applies to SVAP approved standards USCDI v4 and US Core 7.0.0:

> For demonstration of the SMART IG "Standalone Launch" steps, health IT developers are permitted to scope US Core IG resources that do not exist in either USCDI v4 or the "Compartment Patient" section of the standard adopted at § 170.215(a)(1) (HL7® FHIR® Release 4.0.1) as either patient/[Resource] or user/[Resource]. These resources include "Device," "Medication," "Organization," "Practitioner," and "PractitionerRole." Health IT developers must document their supported scopes according to the technical documentation requirements at § 170.315(g)(10)(viii)(A) and § 170.404(a)(2).

Paragraph (g)(10)(iv) Secure connection

Technical outcome - (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 an implementation specification adopted in § 170.215(d).

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- TLS version 1.2 or above must be enforced for the appropriate connections.
- Health IT developers are encouraged but not required to follow TLS Best Current Practice (BCP 195) for TLS version enforcement, referenced in section 6.1.0.3 of the HL7® 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, October 30, 2019, which recommends TLS 1.2 or above to be used for all production data exchange and limits support for lower versions of TLS. To meet ONC Certification requirements, Health IT developers must document how the Health IT Module enforces TLS version 1.2 or above to meet the API documentation requirements at § 170.315(g)(10)(viii) and API Transparency Conditions at 45 CFR 170.404(a)(2).

Technical outcome - (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 an implementation specification adopted in § 170.215(d).

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- TLS version 1.2 or above must be enforced for the appropriate connections.
- Health IT developers are encouraged but not required to follow TLS Best Current Practice (BCP 195) for TLS version enforcement, referenced in section 6.1.0.3 of the HL7® 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, October 30, 2019, which recommends TLS 1.2 or above to be used for all production data exchange and limits support for lower versions of TLS. To meet ONC Certification requirements, Health IT developers must document how the Health IT Module enforces TLS version 1.2 or above to meet the API documentation requirements at § 170.315(g)(10)(viii) and API Transparency Conditions at 45 CFR 170.404(a)(2).

Paragraph (g)(10)(v)(A)(*1*) Authentication and authorization – Authentication and authorization for patient and user scopes – First time connections

Technical outcome – For first time connections, authentication and authorization must occur during the process of granting access to patient data in accordance with an implementation specification adopted in § 170.215(c) and standard adopted in § 170.215(e)(1). Additionally, 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). Finally, 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.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT Modules will be explicitly tested for US Core IG operations using authentication and authorization tokens acquired via the process described in an implementation specification adopted in § 170.215(c).
- Only the relevant parts of the OpenID Connect Core 1.0 including errata set 1 adopted in § 170.215(e)(1) that are also included in an implementation specification adopted in § 170.215(c) will be in-scope for testing and certification.
- Although Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on FHIR® resource-level scopes, Health IT Modules are not prohibited from presenting authorization scopes in a more user-friendly format (e.g. grouping resources under categories, renaming the scopes for easier comprehension by the end-user, using more granular scopes), as long as the ability for patients to authorize applications based on resource-level scopes is available, if requested by the patient.
- For § 170.315(g)(10) criterion requirements at § 170.315(g)(10)(v)(A) regarding authorization for patient and user scopes, we clarify wildcard scopes as defined in the implementation specifications at § 170.215(c) are not required to be supported.
- Health IT Modules will only be tested for the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" "Capability Sets" described in an implementation specification adopted at § 170.215(c).
- Since the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" "Capability Sets" do not include "context-standalone-encounter" ONC will not test Health IT Modules for support for the "context-standalone-encounter" SMART on FHIR® Capability described in an implementation specification adopted at § 170.215(c).
- Implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of the information blocking provisions.
- As part of the requirements at § 170.315(g)(10)(v)(A)(1)(iii), health IT developers must publish the method(s) by which their Health IT Modules support the secure issuance of an initial refresh token to native applications according to the technical documentation requirements at § 170.315(g)(10)(viii) and transparency conditions at § 170.404(a)(2).

- Application developer affirmations to health IT developers regarding the ability of their applications to secure a refresh token, a client secret, or both, must be treated in a good faith manner consistent with the provisions established in the openness and pro-competitive conditions at § 170.404(a)(4).
- Health IT developers can determine the method(s) they use to support interactions with native applications and clarify that health IT developers are not required to support all methods third-party application developers seek to use.
- ONC recognizes there may be some ambiguity in the HL7® SMART Application Launch Framework Implementation Guide (incorporated by reference at § 170.215(c)) in its guidance for supporting native applications, in particular, in providing references to best practices, strategies, and examples such as “OAuth 2.0 for Native Apps: 8.5. Client Authentication”, “OAuth 2.0 Dynamic Client Registration Protocol”, and “universal redirect_uris” without a standardized solution. ONC provides flexibility for how the health IT developer implements the HL7® SMART Application Launch Framework implementation specification, as long as the Certified Health IT Module supports for first time connections the issuance of three-month refresh tokens to native applications capable of securing a refresh token.
- The paragraph at § 170.215(c) requires health IT developers to support the SMART Application Launch Framework Implementation Guide (SMART IG) “SMART [on FHIR®] Core Capabilities,” including “permission-offline,” which grants support for refresh tokens. The implementation specifications adopted in § 170.215(c) require that patients have the ability to explicitly enable the “offline_access” scope during authorization. If the “offline_access” scope is not enabled by patients, patients will be required to re-authenticate and re-authorize an application's access to their EHI after the application's access token expires. However, the ability of a patient to explicitly enable the “offline_access” scope during authorization is not described in the implementation specification. ONC clarifies that health IT developers must support the ability for patients to be provided information about an application’s request for persistent access prior to the patient sharing their health information, in order to enable patients to make an informed decision during authorization. Examples include, but are not limited to a health IT developer allowing patients to granularly grant “offline-access” scopes during authorization or clearly providing this information as a notice during authorization. The critical requirement is that patients are empowered to deny authorization for offline access.
- The SMART capabilities in § 170.215(c) are explicitly required for testing and certification because these capabilities are otherwise indicated as optional in the implementation specification.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standard US Core 4.0.0 (expires on January 1, 2026):

Since "Encounter" is not a USCDI v1 data class or data element, ONC will not test Health IT Modules for support for "context-ehr-encounter" SMART on FHIR® Core Capabilities described in an implementation specification adopted at § 170.215(c).

Applies to SMART App Launch Framework 1.0.0 (expires on January 1, 2026):

- As part of the “permission-patient” “SMART on FHIR® Core Capability” in § 170.215(c), Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their electronic health information (EHI) based on FHIR® resource-level scopes. Specifically, this means patients would need to have the ability to authorize access to their EHI at the individual FHIR® resource level, from one specific FHIR® resource (e.g., “Immunization”) up to all FHIR® resources necessary to implement a standard adopted in § 170.213 and corresponding implementation specification adopted in § 170.215(b)(1).
- As described in the ONC Cures Act Final Rule, we encourage implementers to adhere to industry best practices to mitigate Cross-Site Request Forgery (CSRF) and other known security threats (85 FR 25742). Proof Key for Code Exchange (PKCE) (Internet Engineering Task Force Request for Comments 7636) is an industry standard that can help mitigate CSRF and other known security threats. The ONC Health IT Certification Program will support the optional use of PKCE during authentication and authorization testing. Health IT developers that implement and require the use of PKCE should include documentation for their PKCE implementation as part of the API Documentation requirement at 45 CFR 170.315(g)(10)(viii) and API Transparency Conditions at 45 CFR 170.404(a)(2).

Applies to SMART App Launch 2.0.0 (required by December 31, 2025) and SVAP approved standard SMART App Launch 2.2.0:

- For certification purposes, a Health IT Module is not required to support authorization requests nor responses including a combination of SMART v1 and SMART v2 scopes. For example, an authorization request including simultaneously the SMART v1 scope of “patient/Observation.read” and the SMART v2 scope of “patient/Condition.rs” is not required to be supported.
- A Health IT Module may optionally support the "fhirContext" launch context parameter defined in the SMART App Launch 2.0.0 implementation guide. If the "fhirContext" parameter is supported, the Health IT Module must conform to the requirements for the parameter detailed in the SMART App Launch implementation guide.

- We clarify the following SMART App Launch capabilities must be supported as part of fulfilling the authentication and authorization requirements at § 170.315(g)(10)(v)(A) when certifying using the implementation specification at § 170.215(c)(2):
    - To support patient access for standalone apps, the Health IT Module must support:
        - the capabilities of "launch-standalone" and "context-standalone-patient"; and
        - the capabilities in subsections "Authorization Methods", "Client Types", "Single Sign-on", and "Permissions" except the "permission-online" and "permission-user" capabilities
    - To support clinician access for EHR launch, the Health IT Module must support:
        - the capabilities of "launch-ehr", "context-banner", "context-style", "context-ehr-patient", and "context-ehr-encounter" (if supporting USCDI v2 or v3); and
        - the capabilities in subsections "Authorization Methods", "Client Types", "Single Sign-on", and "Permissions" except the "permission-online" capability
- As finalized in the HTI-1 Final Rule (89 FR 1294), Health IT Modules are required to support SMART App Launch "Finer-grained resource constraints using search parameters" for the “category” parameter for the Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern, and the Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs. We defer to the implementation guides referenced at § 170.215(b)(1) and § 170.215(c) for specific implementation guidance for this requirement. In the context of the US Core 6.1.0 implementation guide, the Observation sub-resources of Clinical Test and SDOH may have scopes supported as follows:
    - support for scopes for the Observation sub-resource Clinical Test using the "procedure" code from the US Core Clinical Result Observation Category value set.
    - support for scopes for the Observation sub-resource SDOH using the "sdoh" code from the US Core Category code system.
- The US Core 7.0.0 IG includes requirements for how scopes for the Condition and Observation resources must be supported, including requirements in the “SMART on FHIR Obligations and Capabilities” section as well as Condition and Observation profiles sections.
- For certification and testing purposes the Health IT Module must demonstrate support for patients and users to authorize an app to receive patient data using scopes with “Finer-grained resource constraints using search parameters” for the sub-resources specified in the HTI-1 Final Rule. We require a Health IT Module to support a patient’s ability to provide authorization at the individual sub-resource scope level.

- Although Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on individual FHIR resource level and individual sub-resource level scopes, Health IT Modules are not prohibited from presenting authorization scopes in a more user-friendly format (e.g. grouping scopes under categories, renaming the scopes for easier comprehension by the end-user), as long as the ability for patients to authorize applications based on individual resource level and individual sub-resource level scopes is available, if requested by the patient.
- As part of supporting the SMART App Launch "permission-v2" capability for the purposes of certification, if an app requests authorization for a resource level scope for the "Condition" or "Observation" resources, then for patient authorization purposes a Health IT Module must support presentation of the required sub-resource scopes to the patient for authorization. Specifically, sub-resource scopes must be presented for patient authorization as follows:
    - "Condition" sub-resource scopes "Encounter Diagnosis", "Problem List", and "Health Concern" if a "Condition" resource level scope is requested
    - "Observation" sub-resource scopes "Clinical Test", "Laboratory", "Social History", "SDOH", "Survey", and "Vital Signs" if an "Observation" resource level scope is requested
- For purposes of certification to the § 170.315(g)(10) criterion, a Health IT Module is not required to support for authorization purposes presentation of sub-resource scopes to the user during clinician access for EHR launch.

Technical outcome – For first time connections, authentication and authorization must occur during the process of granting access to patient data in accordance with an implementation specification adopted in § 170.215(c) and standard adopted in § 170.215(e)(1). Additionally, 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). Finally, 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.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT Modules will be explicitly tested for US Core IG operations using authentication and authorization tokens acquired via the process described in an implementation specification adopted in § 170.215(c).
- Only the relevant parts of the OpenID Connect Core 1.0 including errata set 1 adopted in § 170.215(e)(1) that are also included in an implementation specification adopted in § 170.215(c) will be in-scope for testing and certification.

- Although Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on FHIR® resource-level scopes, Health IT Modules are not prohibited from presenting authorization scopes in a more user-friendly format (e.g. grouping resources under categories, renaming the scopes for easier comprehension by the end-user, using more granular scopes), as long as the ability for patients to authorize applications based on resource-level scopes is available, if requested by the patient.
- For § 170.315(g)(10) criterion requirements at § 170.315(g)(10)(v)(A) regarding authorization for patient and user scopes, we clarify wildcard scopes as defined in the implementation specifications at § 170.215(c) are not required to be supported.
- Health IT Modules will only be tested for the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" "Capability Sets" described in an implementation specification adopted at § 170.215(c).
- Since the "Patient Access for Standalone Apps" and "Clinician Access for EHR Launch" "Capability Sets" do not include "context-standalone-encounter" ONC will not test Health IT Modules for support for the "context-standalone-encounter" SMART on FHIR® Capability described in an implementation specification adopted at § 170.215(c).
- Implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of the information blocking provisions.
- As part of the requirements at § 170.315(g)(10)(v)(A)(1)(iii), health IT developers must publish the method(s) by which their Health IT Modules support the secure issuance of an initial refresh token to native applications according to the technical documentation requirements at § 170.315(g)(10)(viii) and transparency conditions at § 170.404(a)(2).
- Application developer affirmations to health IT developers regarding the ability of their applications to secure a refresh token, a client secret, or both, must be treated in a good faith manner consistent with the provisions established in the openness and pro-competitive conditions at § 170.404(a)(4).
- Health IT developers can determine the method(s) they use to support interactions with native applications and clarify that health IT developers are not required to support all methods third-party application developers seek to use.
- ONC recognizes there may be some ambiguity in the HL7® SMART Application Launch Framework Implementation Guide (incorporated by reference at § 170.215(c)) in its guidance for supporting native applications, in particular, in providing references to best practices, strategies, and examples such as "OAuth 2.0 for Native Apps: 8.5. Client Authentication", "OAuth 2.0 Dynamic Client Registration Protocol", and "universal redirect_uris" without a standardized solution. ONC provides flexibility for how the health IT developer implements the HL7® SMART Application Launch Framework implementation specification, as long as the Certified Health IT Module supports for first time connections the issuance of three-month refresh tokens to native applications capable of securing a refresh token.

- The paragraph at § 170.215(c) requires health IT developers to support the SMART Application Launch Framework Implementation Guide (SMART IG) "SMART [on FHIR®] Core Capabilities," including "permission-offline," which grants support for refresh tokens. The implementation specifications adopted in § 170.215(c) require that patients have the ability to explicitly enable the "offline_access" scope during authorization. If the "offline_access" scope is not enabled by patients, patients will be required to re-authenticate and re-authorize an application's access to their EHI after the application's access token expires. However, the ability of a patient to explicitly enable the "offline_access" scope during authorization is not described in the implementation specification. ONC clarifies that health IT developers must support the ability for patients to be provided information about an application's request for persistent access prior to the patient sharing their health information, in order to enable patients to make an informed decision during authorization. Examples include, but are not limited to a health IT developer allowing patients to granularly grant "offline-access" scopes during authorization or clearly providing this information as a notice during authorization. The critical requirement is that patients are empowered to deny authorization for offline access.
- The SMART capabilities in § 170.215(c) are explicitly required for testing and certification because these capabilities are otherwise indicated as optional in the implementation specification.

Applies to USCDI v1 and US Core 3.1.1 and SVAP approved standard US Core 4.0.0 (expires on January 1, 2026):

Since "Encounter" is not a USCDI v1 data class or data element, ONC will not test Health IT Modules for support for "context-ehr-encounter" SMART on FHIR® Core Capabilities described in an implementation specification adopted at § 170.215(c).

Applies to SMART App Launch Framework 1.0.0 (expires on January 1, 2026):

- As part of the "permission-patient" "SMART on FHIR® Core Capability" in § 170.215(c), Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their electronic health information (EHI) based on FHIR® resource-level scopes. Specifically, this means patients would need to have the ability to authorize access to their EHI at the individual FHIR® resource level, from one specific FHIR® resource (e.g., "Immunization") up to all FHIR® resources necessary to implement a standard adopted in § 170.213 and corresponding implementation specification adopted in § 170.215(b)(1).
- As described in the ONC Cures Act Final Rule, we encourage implementers to adhere to industry best practices to mitigate Cross-Site Request Forgery (CSRF) and other known security threats (85 FR 25742). Proof Key for Code Exchange (PKCE) (Internet Engineering Task Force Request for Comments 7636) is an industry standard that can help mitigate CSRF and other known security threats. The ONC Health IT Certification Program will support the optional use of PKCE during authentication and authorization testing. Health IT developers that implement and require the use of PKCE should include documentation for their PKCE implementation as part of the API Documentation requirement at 45 CFR 170.315(g)(10)(viii) and API Transparency Conditions at 45 CFR 170.404(a)(2).

Applies to SMART App Launch 2.0.0 (required by December 31, 2025) and SVAP approved standard SMART App Launch 2.2.0:

- For certification purposes, a Health IT Module is not required to support authorization requests nor responses including a combination of SMART v1 and SMART v2 scopes. For example, an authorization request including simultaneously the SMART v1 scope of “patient/Observation.read” and the SMART v2 scope of “patient/Condition.rs” is not required to be supported.
- A Health IT Module may optionally support the "fhirContext" launch context parameter defined in the SMART App Launch 2.0.0 implementation guide. If the "fhirContext" parameter is supported, the Health IT Module must conform to the requirements for the parameter detailed in the SMART App Launch implementation guide.
- We clarify the following SMART App Launch capabilities must be supported as part of fulfilling the authentication and authorization requirements at § 170.315(g)(10)(v)(A) when certifying using the implementation specification at § 170.215(c)(2):
    - To support patient access for standalone apps, the Health IT Module must support:
        - the capabilities of "launch-standalone" and "context-standalone-patient"; and
        - the capabilities in subsections "Authorization Methods", "Client Types", "Single Sign-on", and "Permissions" except the "permission-online" and "permission-user" capabilities
    - To support clinician access for EHR launch, the Health IT Module must support:
        - the capabilities of "launch-ehr", "context-banner", "context-style", "context-ehr-patient", and "context-ehr-encounter" (if supporting USCDI v2 or v3); and
        - the capabilities in subsections "Authorization Methods", "Client Types", "Single Sign-on", and "Permissions" except the "permission-online" capability
- As finalized in the HTI-1 Final Rule (89 FR 1294), Health IT Modules are required to support SMART App Launch "Finer-grained resource constraints using search parameters" for the “category” parameter for the Condition resource with Condition sub-resources Encounter Diagnosis, Problem List, and Health Concern, and the Observation resource with Observation sub-resources Clinical Test, Laboratory, Social History, SDOH, Survey, and Vital Signs. We defer to the implementation guides referenced at § 170.215(b)(1) and § 170.215(c) for specific implementation guidance for this requirement. In the context of the US Core 6.1.0 implementation guide, the Observation sub-resources of Clinical Test and SDOH may have scopes supported as follows:
    - support for scopes for the Observation sub-resource Clinical Test using the "procedure" code from the US Core Clinical Result Observation Category value set.
    - support for scopes for the Observation sub-resource SDOH using the "sdoh" code from the US Core Category code system.
- The US Core 7.0.0 IG includes requirements for how scopes for the Condition and Observation resources must be supported, including requirements in the “SMART on FHIR Obligations and Capabilities” section as well as Condition and Observation profiles sections.

- For certification and testing purposes the Health IT Module must demonstrate support for patients and users to authorize an app to receive patient data using scopes with “Finer-grained resource constraints using search parameters” for the sub-resources specified in the HTI-1 Final Rule. We require a Health IT Module to support a patient’s ability to provide authorization at the individual sub-resource scope level.
- Although Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on individual FHIR resource level and individual sub-resource level scopes, Health IT Modules are not prohibited from presenting authorization scopes in a more user-friendly format (e.g. grouping scopes under categories, renaming the scopes for easier comprehension by the end-user), as long as the ability for patients to authorize applications based on individual resource level and individual sub-resource level scopes is available, if requested by the patient.
- As part of supporting the SMART App Launch “permission-v2” capability for the purposes of certification, if an app requests authorization for a resource level scope for the “Condition” or “Observation” resources, then for patient authorization purposes a Health IT Module must support presentation of the required sub-resource scopes to the patient for authorization. Specifically, sub-resource scopes must be presented for patient authorization as follows:
    - “Condition” sub-resource scopes “Encounter Diagnosis”, “Problem List”, and “Health Concern” if a “Condition” resource level scope is requested
    - “Observation” sub-resource scopes “Clinical Test”, “Laboratory”, “Social History”, “SDOH”, “Survey”, and “Vital Signs” if an “Observation” resource level scope is requested
- For purposes of certification to the § 170.315(g)(10) criterion, a Health IT Module is not required to support for authorization purposes presentation of sub-resource scopes to the user during clinician access for EHR launch.

Paragraph (g)(10)(v)(A)(*2*) Authentication and authorization – Authentication and authorization for patient user scopes – Subsequent connections

Technical outcome – For subsequent connections, access must be granted to patient data in accordance with an implementation specification adopted in§ 170.215(c) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application. Additionally, a Health IT Module’s authorization server must issue a refresh token valid for a new period of no less than three months to applications using the “confidential app” profile according to an implementation specification adopted in § 170.215(c).

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

For subsequent connections of applications capable of storing a client secret, Health IT Modules are required to issue a refresh token valid for a new period of no shorter than three months per the API certification criterion requirement finalized in § 170.315(g)(10)(v)(A)(2)(ii).

Technical outcome – For subsequent connections, access must be granted to patient data in accordance with an implementation specification adopted in§ 170.215(c) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application. Additionally, a Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications using the "confidential app" profile according to an implementation specification adopted in § 170.215(c).

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

For subsequent connections of applications capable of storing a client secret, Health IT Modules are required to issue a refresh token valid for a new period of no shorter than three months per the API certification criterion requirement finalized in § 170.315(g)(10)(v)(A)(2)(ii).

Paragraph (g)(10)(v)(B) Authentication and authorization – Authentication and authorization for system scopes

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

Health IT Modules may use access control schemes other than OAuth 2.0 for controlling access to the file server, such as capability URLs. The HL7® FHIR®-I Work Group has documented expectations for the use of capability URLs with the Bulk Data Access IG on the HL7® confluence website. For purposes of Certification testing, Health IT Modules will be tested for the ability to share bulk data files either using OAuth 2.0 bearer tokens or via capability URLs accessible without preconditions or additional steps.

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

Health IT Modules may use access control schemes other than OAuth 2.0 for controlling access to the file server, such as capability URLs. The HL7® FHIR®-I Work Group has documented expectations for the use of capability URLs with the Bulk Data Access IG on the HL7® confluence website. For purposes of Certification testing, Health IT Modules will be tested for the ability to share bulk data files either using OAuth 2.0 bearer tokens or via capability URLs accessible without preconditions or additional steps.

Paragraph (g)(10)(vi) Patient authorization revocation

Technical outcome – 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 one hour of the request.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- This is a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop.
- Patients are expected to have the ability to revoke an authorized application's access to their EHI at any time.
- For authorization revocation, Health IT Modules presented for certification are permitted to allow short-lived access tokens to expire in lieu of immediate access token revocation. ONC recommends health IT developers limit the lifetime of access tokens to one hour or less as recommended in the implementation specifications adopted at § 170.215(c). For purposes of testing and certification, Health IT Modules will be tested for patient authorization revocation occurring within one hour of the request.

Technical outcome – 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 one hour of the request.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- This is a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop.
- Patients are expected to have the ability to revoke an authorized application's access to their EHI at any time.
- For authorization revocation, Health IT Modules presented for certification are permitted to allow short-lived access tokens to expire in lieu of immediate access token revocation. ONC recommends health IT developers limit the lifetime of access tokens to one hour or less as recommended in the implementation specifications adopted at § 170.215(c). For purposes of testing and certification, Health IT Modules will be tested for patient authorization revocation occurring within one hour of the request.

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

Technical outcome – 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).

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

Health IT Developers must update their § 170.315(g)(10)-certified Health IT Modules to support token introspection as defined in the SMART App Launch 2.0.0 or 2.2.0 implementation specification, and provide such updated Certified Health IT Modules to their customers by December 31, 2025.

Technical outcome – 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).

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

> Health IT Developers must update their § 170.315(g)(10)-certified Health IT Modules to support token introspection as defined in the SMART App Launch 2.0.0 or 2.2.0 implementation specification, and provide such updated Certified Health IT Modules to their customers by December 31, 2025.

Paragraph (g)(10)(viii)(A) Documentation – minimum requirements

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT developers are not required to re-publish documentation from the adopted standards and implementation specifications. However, health IT developers must publish documentation that goes beyond the adopted standards and implementation specifications.
- Health IT developers are expected to disclose any additional data their § 170.315(g)(10)-certified Health IT Module supports in the context of the adopted standards and implementation specifications.

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

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

- Health IT developers are not required to re-publish documentation from the adopted standards and implementation specifications. However, health IT developers must publish documentation that goes beyond the adopted standards and implementation specifications.
- Health IT developers are expected to disclose any additional data their § 170.315(g)(10)-certified Health IT Module supports in the context of the adopted standards and implementation specifications.

Paragraph (g)(10)(viii)(B) Documentation – public access

Technical outcome – 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.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

No additional clarifications.

Technical outcome – 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.

Clarifications:

Applies to all applicable base regulatory and SVAP standards:

No additional clarifications.