The Office of the National Coordinator for Health Information Technology

2015 Edition Cures Update
§ 170.315(g)(10)
Standardized API for patient and population services

Testing Components:

Test Procedure Version 2.1 Last Updated 08-29-2022

Please consult the final rule entitled: *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* and the Interim Final Rule (IFR) *Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency,* for associated regulations and a detailed description of the certification criterion with which these testing steps are associated. Developers are encouraged to consult the Certification Companion Guide in tandem with the test procedure as these provide clarifications that may be useful for product development and testing.

Note: The order in which the test steps are listed reflects the sequence of the certification criterion and does not necessarily prescribe the order in which the test should take place.

Revision History

Version #	Description of Change	Version Date
1.0	Final Test Procedure	06-01-2020
1.1	Corrected typos. Corrected internal document references in Steps 12, 13, and 19 of "Authentication and Authorization for Patient and User Scopes." Corrected applicable launch scenarios in Step 13 of "Authentication and Authorization for Patient and User Scopes." Amended Step 10 of "Authentication and Authorization for Patient and User Scopes" by removing non-USCDI mapped US Core IG FHIR®® resources.	08-07-2020
1.2	Updated compliance date, regulation text, and standard for trial use (STU) 3 Release 3.1.1 at § 170.215(2), per the IFR, *Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency*.	11-02-2020
1.3	Added step for issuance of a refresh token to native apps that are capable of storing a refresh token (Step 21 of "Paragraph (g)(10)(v)(A) – Authentication and authorization for patient and user scopes").	12-16-2020

	Removed "PractitionerRole" and "RelatedPerson" from multiple patient services data support list (Step 8 of "Paragraph (g)(10)(i) – Data response").	
1.4	Updated test procedure step regarding "offline_access" scope, enabling health IT developer to demonstrate either support for the end-user to explicitly enable / disable the "offline_access" scope, or information communicating the application's request for the "offline_access" scope.	04-02-2021
1.5	Corrected typo in Step 5 of "Paragraph (g)(10)(v)(B) – Authentication and authorization for system scopes" to indicate that the "cache-control" header is sent by the application. Added step for health IT developer to demonstrate the public location of its certified API technology service base URLs that can be used by patients to access their Electronic Health Information.	05-12-2021
1.6	Updated Step 13 of "Paragraph (g)(10)(v)(A) – Authentication and authorization for patient and user scopes" to indicate that only the "launch" parameter, in EHR-Launch mode, is tested against the "launch" parameter provided in Step 8. Added a new Step 14 to this section to indicate how the "aud" parameter is tested. Corrected a typo in Step 22 of this section to indicate refresh tokens are granted to native applications capable of securing a refresh token.	XX-XX-2021
1.7	Updated "Missing Data" requirements in section "Data Response Checks for Single and Multiple Patients" to clarify that health IT developers must demonstrate that Health IT Modules support "Missing Data" according to the US Core IG, including for non-coded and coded data elements.	08-02-2021
1.8	Updated the link for § 170.215(a)(2) FHIR®® US Core Implementation Guide STU V3.1.1	11-03-21
1.9	Updated the Bulk Data IG references in "Standard(s) Referenced" from "HL7® FHIR®® Bulk Data Access (Flat FHIR®®) (V1.0.0:STU 1)" to the ONC-approved errata version "HL7® FHIR®® Bulk Data Access (Flat FHIR®®) (V1.0.1:STU 1)" that is now effective for testing.	12-08-21
2.0	Updated Testing Tool and Test Tool Documentation links.	04-06-2022
2.1	Removed Step 13, for Paragraph (g)(10)(v)(A) – "Authentication and authorization for patient and user scopes", which tested the response to an invalid "launch" parameter for EHR-Launch.	06-01-22
2.2	Updated to include the Standards Version Advancement Process (SVAP) Approved Standards for 2022. . Added unique identifiers (e.g., "APP-REG-1") to each test procedure step.	08-29-22

Regulation Text

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

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

(i) *Data response*.

(A) Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted at § 170.215(a)(2), including the mandatory capabilities described in "US Core Server CapabilityStatement," for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standard adopted in § 170.215(a)(1) and implementation specifications adopted at § 170.215(a)(2) and (a)(4), for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(ii) *Supported search operations*.

(A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(2), specifically the mandatory capabilities described in "US Core Server CapabilityStatement".

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

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

(iv) *Secure connection*.

(A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(a)(2) and (3).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(a)(4).

(v) *Authentication and authorization.*

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

(1) First time connections.

(i) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b).

(ii) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications capable of storing a client secret.

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

(2) Subsequent connections.

(i) Access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

(ii) 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 capable of storing a client secret.

(B) *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(a)(4) and the application must be issued a valid access token.

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

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued.

(viii) *Documentation*.

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

(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

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

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

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

Standard(s) Referenced

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

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

§ 170.215(a)(2) FHIR®® US Core Implementation Guide STU V3.1.1
§ 170.213 United States Core Data for Interoperability (USCDI)

Paragraph (g)(10)(i)(B)
§ 170.215(a)(1) HL7® Version 4.0.1 FHIR® Release 4, October 30, 2019
§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.1
§ 170.213 USCDI, Version 1
§ 170.215(a)(4) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.1:STU 1)

Paragraph (g)(10)(ii)(A)
§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.1

Paragraph (g)(10)(ii)(B)
§ 170.215(a)(4) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.1:STU 1)

Paragraph (g)(10)(iii)
None

Paragraph (g)(10)(iv)(A)
§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.1
§ 170.215(a)(3) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0

Paragraph (g)(10)(iv)(B)
§ 170.215(a)(4) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.1:STU 1)

Paragraph (g)(10)(v)(A)(1)
§ 170.215(a)(3) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0
§ 170.215(b) OpenID Connect Core 1.0 incorporating errata set 1

Paragraph (g)(10)(v)(A)(2)
§ 170.215(a)(3) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0

Paragraph (g)(10)(v)(B)
§ 170.215(a)(4) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.1: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

United States Core Data for Interoperability (USCDI), Version 2, July 2021

HL7® FHIR® US Core Implementation Guide STU 4.0.0, June 2021

HL7® FHIR® US Core Implementation Guide STU 5.0.1, June 2022

HL7® FHIR® SMART Application Launch Framework Implementation Guide Release 2.0.0, November 26, 2021

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

Required Tests

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

System Under Test	Test Lab Verification
Applies to all applicable base regulatory and SVAP standards **Application Registration**	*Applies to all applicable base regulatory and SVAP standards* **Application Registration**

System Under Test	Test Lab Verification
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).	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	Test Lab Verification
Applies to all applicable 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 the implementation specifications adopted in § 170.215(a)(2) and § 170.215(a)(3), including: • Using TLS version 1.2 or higher; and • Conformance to FHIR® Communications Security requirements.	*Applies to all applicable 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 the implementation specifications adopted in § 170.215(a)(2) and § 170.215(a)(3), 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	Test Lab Verification
Regulatory Standard: SMART 1.0.0 **Authentication and Authorization for Patient and User Scopes** 1. AUT-PAT-1: The health IT developer demonstrates the ability of the Health IT Module to support the following for "EHR-Launch," "Standalone-Launch," and "Both" ("EHR-Launch" and "Standalone-Launch") as specified in the implementation specification adopted in § 170.215(a)(3). 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(a)(3), 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(a)(3). 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(a)(3) and standard adopted in § 170.215(a)(1): • The ".well-known/smart-configuration.json" path; and • A FHIR® "CapabilityStatement".	*Regulatory Standard: SMART 1.0.0* **Authentication and Authorization for Patient and User Scopes** 1. AUT-PAT-1: The tester verifies the ability of the Health IT Module to support the following for "EHR-Launch," "Standalone-Launch," and "Both" ("EHR-Launch" and "Standalone-Launch") as specified in the implementation specification adopted in § 170.215(a)(3). 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(a)(3), 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(a)(3). 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(a)(3) and standard adopted in § 170.215(a)(1): • The ".well-known/smart-configuration.json" path; and • A FHIR® "CapabilityStatement". 6. AUT-PAT-6: [Both] The tester verifies the ability of the ".well-known/smart-configuration.json" path to support at least the

System Under Test	Test Lab Verification
6. AUT-PAT-6: [Both] The health IT developer demonstrates the ability of the ".well-known/smart-configuration.json" path to support at least the following as detailed in the implementation specification adopted in § 170.215(a)(3): • "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(a)(3) 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(a)(3), 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 as detailed in the implementation specification adopted in § 170.215(a)(3): • "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(a)(3) 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(a)(3), 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(a)(3) and standard adopted in § 170.215(b):

System Under Test	Test Lab Verification
following scopes and capabilities according to the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b): • "openid" (to support "sso-openid-connect" "SMART on FHIR® Core Capability"); • "FHIR®User" (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 the standard adopted in § 170.213	• "openid" (to support "sso-openid-connect" "SMART on FHIR® Core Capability"); • "FHIR®User" (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 the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2). If using US Core 3.1.1, 4.0.0, or 5.0.1, these resources include:

System Under Test	Test Lab Verification
and implementation specification adopted in § 170.215(a)(2). If using US Core 3.1.1, 4.0.0, or 5.0.1, these resources include: • "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device"; • "DiagnosticReport"; • "DocumentReference"; • "Goal"; • "Immunization"; • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Patient"; • "Procedure"; and • "Provenance". Additionally, the following resources must be supported if using US Core 5.0.1: • "Encounter"; • "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	• "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device"; • "DiagnosticReport"; • "DocumentReference"; • "Goal"; • "Immunization"; • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Patient"; • "Procedure"; and • "Provenance". Additionally, the following resources must be supported if using US Core 5.0.1: • "Encounter"; • "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

System Under Test	Test Lab Verification
or information communicating the application's request for the "offline_access" scope. 12. AUT-PAT-12: [Both] The health IT developer demonstrates the ability of the Health IT Module to deny an application's authorization request according to a patient's preferences selected in AUT-PAT-10, and AUT-PAT-11, of this section in accordance with the implementation specification adopted in § 170.215(a)(3). 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(a)(3), 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(a)(3): • "grant_type"; • "code"; • "redirect_uri"; • "client_id"; and	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(a)(3). 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(a)(3), 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(a)(3): • "grant_type"; • "code"; • "redirect_uri"; • "client_id"; and • Authorization header including "client_id" and "client_secret". 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

System Under Test	Test Lab Verification
• Authorization header including “client_id” and “client_secret”. 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(a)(3) and standard adopted in § 170.215(b), 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 5.0.1: • “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	implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b), 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 5.0.1: • “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(b), including: • All required fields populated according to implementation specification adopted in § 170.215(b); and

System Under Test	Test Lab Verification
well-known URI in accordance with the implementation specification adopted in § 170.215(b), including: • All required fields populated according to implementation specification adopted in § 170.215(b); 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(a)(3). 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-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 20. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 5.0.1: 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-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 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 the implementation specification adopted in § 170.215(a)(2). 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.	• 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(a)(3). 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-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 20. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 5.0.1: 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-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 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 the implementation specification adopted in § 170.215(a)(2). 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**

System Under Test	Test Lab Verification
Subsequent Connections: Authentication and Authorization for Patient and User Scopes 23. 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(a)(3). 24. 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(a)(3). *SVAP Version Approved: SMART 2.0.0* **Authentication and Authorization for Patient and User Scopes** 1. AUT-PAT-1: The health IT developer demonstrates the ability of the Health IT Module to support the following for "EHR-Launch," "Standalone-Launch," and "Both" ("EHR-Launch" and "Standalone-Launch") as specified in the implementation specification adopted in § 170.215(a)(3). 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(a)(3), including: • Launching the registered launch URL of the application; and • Passing the parameters: "iss" and "launch".	23. 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(a)(3). 24. 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(a)(3). *SVAP Version Approved: SMART 2.0.0* **Authentication and Authorization for Patient and User Scopes** 1. AUT-PAT-1: The tester verifies the ability of the Health IT Module to support the following for "EHR-Launch," "Standalone-Launch," and "Both" ("EHR-Launch" and "Standalone-Launch") as specified in the implementation specification adopted in § 170.215(a)(3). 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(a)(3), 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

System Under Test	Test Lab Verification
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(a)(3). 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.json" path as detailed in the implementation specification adopted in § 170.215(a)(3) 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.json" path to support at least the following as detailed in the implementation specification adopted in § 170.215(a)(3): • "authorization_endpoint"; • "token_endpoint"; • "capabilities" including support for "launch-ehr", "launch-standalone", "client-public", "client-confidential-symmetric", "sso-openid-connect", "context-banner", "context-style", "context-ehr-patient", "context-standalone-patient", "permission-offline", "permission-patient", "permission-user", "authorize-post", "permission-v2"; • "grant_types_supported" with support for "authorization_code" and "client_credentials"; and	mode detailed in the implementation specification adopted in § 170.215(a)(3). 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.json" path as detailed in the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(a)(1). 6. AUT-PAT-25: [Both] The tester verifies the ability of the ".well-known/smart-configuration.json" path to support at least the following as detailed in the implementation specification adopted in § 170.215(a)(3): • "authorization_endpoint"; • "token_endpoint"; • "capabilities" including support for "launch-ehr", "launch-standalone", "client-public", "client-confidential-symmetric", "sso-openid-connect", "context-banner", "context-style", "context-ehr-patient", "context-standalone-patient", "permission-offline", "permission-patient", "permission-user", "authorize-post", "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 5.0.1: • "context-ehr-encounter"

System Under Test	Test Lab Verification
• "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 5.0.1: • "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(a)(3), 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(a)(3). 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(a)(3) and standard adopted in § 170.215(b):	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(a)(3), 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(a)(3). 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(a)(3) and standard adopted in § 170.215(b): • "openid" (to support "sso-openid-connect" "SMART on FHIR® Capability"); • "FHIR®User" (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);

System Under Test	Test Lab Verification
• "openid" (to support "sso-openid-connect" "SMART on FHIR® Capability"); • "FHIR®User" (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"); and • User-level scopes (to support "permission-user" "SMART on FHIR® Capability"). • SMARTv2 scope syntax for patient-level and user-level scopes (to support "permission-v2" "SMART on FHIR® 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	• "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"); and • User-level scopes (to support "permission-user" "SMART on FHIR® Capability"). • SMARTv2 scope syntax for patient-level and user-level scopes (to support "permission-v2" "SMART on FHIR® 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 the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2).: If using US Core 3.1.1, 4.0.0, or 5.0.1, these resources include: • "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device";

System Under Test	Test Lab Verification
with the profiles specified in the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2). If using US Core 3.1.1, 4.0.0, or 5.0.1, these resources include: • "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device"; • "DiagnosticReport"; • "DocumentReference"; • "Goal"; • "Immunization"; • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Patient"; • "Procedure"; and • "Provenance". Additionally, the following resources must be supported if using US Core 5.0.1: • "Encounter"; • "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	• "DiagnosticReport"; • "DocumentReference"; • "Goal"; • "Immunization"; • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Patient"; • "Procedure"; and • "Provenance". Additionally, the following resources must be supported if using US Core 5.0.1: • "Encounter"; • "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(a)(3). 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

System Under Test	Test Lab Verification
or information communicating the application's request for the "offline_access" scope. 12. AUT-PAT-12: [Both] The health IT developer demonstrates the ability of the Health IT Module to deny an application's authorization request according to a patient's preferences selected in AUT-PAT-10, and AUT-PAT-11, of this section in accordance with the implementation specification adopted in § 170.215(a)(3). 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(a)(3). 14. AUT-PAT-13: [Both] The health IT developer demonstrates the ability of the Health IT Module to return an error response if the "aud" parameter provided by an application to the Health IT Module in AUT-PAT-8, is not a valid FHIR® resource server associated with the Health IT Module's authorization server. 15. AUT-PAT-14: [Both] The health IT developer demonstrates the ability of the Health IT Module to grant an application access to EHI by returning an authorization code to the application according to the implementation specification adopted in § 170.215(a)(3), 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(a)(3):	requests a clinical scope which is restricted to a single patient as detailed in the implementation specification adopted in § 170.215(a)(3). 14. AUT-PAT-13: [Both] The tester verifies the ability of the Health IT Module to return an error response if the "aud" parameter provided by an application to the Health IT Module in AUT-PAT-8, is not a valid FHIR® resource server associated with the Health IT Module's authorization server. 15. AUT-PAT-14: [Both] The tester verifies the ability of the Health IT Module to grant an application access to EHI by returning an authorization code to the application according to the implementation specification adopted in § 170.215(a)(3), 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(a)(3): • "grant_type"; • "code"; • "redirect_uri"; • "code_verifier"; • "client_id"; and • Authorization header including "client_id" and "client_secret". 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"

System Under Test	Test Lab Verification
• "grant_type"; • "code"; • "redirect_uri"; • "code_verifier"; • "client_id"; and • Authorization header including "client_id" and "client_secret". 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(a)(3). 18. AUT-PAT-16: [Both] The health IT developer demonstrates the ability of the Health IT Module to return a JSON object to applications according to the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b), 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");	value is supplied with an access token request according to the implementation specification adopted in § 170.215(a)(3). 18. AUT-PAT-16: [Both] The tester verifies the ability of the Health IT Module to return a JSON object to applications according to the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b), 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 5.0.1: • "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

System Under Test	Test Lab Verification
• "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 5.0.1: • "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(b), including: • All required fields populated according to implementation specification adopted in § 170.215(b); 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(a)(3). 21. AUT-PAT-19: [Both] The health IT developer demonstrates the ability of the Health IT Module to return a "Patient" FHIR® resource that matches the patient context provided in step AUT-PAT-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 22. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 5.0.1: 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	accordance with the implementation specification adopted in § 170.215(b), including: • All required fields populated according to implementation specification adopted in § 170.215(b); 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(a)(3). 21. AUT-PAT-19: [Both] The tester verifies the ability of the Health IT Module to return a "Patient" FHIR® resource that matches the patient context provided in step AUT-PAT-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 22. AUT-PAT-32: [EHR-Launch] The following must be supported if using US Core 5.0.1: 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-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 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 the implementation specification adopted in § 170.215(a)(2). 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.

System Under Test	Test Lab Verification
AUT-PAT-9 of this section according to the implementation specification adopted in § 170.215(a)(2). 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 the implementation specification adopted in § 170.215(a)(2). 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** 25. 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(a)(3). 26. 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(a)(3).	**Subsequent Connections: Authentication and Authorization for Patient and User Scopes** 25. 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(a)(3). 26. 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(a)(3).

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

System Under Test	Test Lab Verification
Applies to all applicable regulatory and SVAP standards	*Applies to all applicable regulatory and SVAP standards*

System Under Test	Test Lab Verification
Patient Authorization Revocation 1. 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, including a demonstration of the inability of the application with revoked access to receive patient EHI.	**Patient Authorization Revocation** 1. PAR-1: The tester verifies the ability of the Health IT Module to revoke access to an authorized application at a patient's direction, 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	Test Lab Verification
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 the implementation specification adopted in § 170.215(a)(4). 2. AUT-SYS-2: The health IT developer demonstrates the ability of the Health IT Module to support the following parameters according to the implementation specification adopted in § 170.215(a)(4): • "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 the implementation specification adopted in § 170.215(a)(4): • "alg" header;	*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 the implementation specification adopted in § 170.215(a)(4). 2. AUT-SYS-2: The tester verifies the ability of the Health IT Module to support the following parameters according to the implementation specification adopted in § 170.215(a)(4): • "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 the implementation specification adopted in § 170.215(a)(4): • "alg" header; • "kid" header; • "typ" header;

System Under Test	Test Lab Verification
• "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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4).	• "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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4), including the following property names:

System Under Test	Test Lab Verification
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 the implementation specification adopted in § 170.215(a)(4), 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 the implementation specification adopted in § 170.215(a)(4).	• "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 the implementation specification adopted in § 170.215(a)(4).

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

System Under Test	Test Lab Verification
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.	*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.

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

System Under Test	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 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 implementation specification adopted in § 170.215(a)(2). 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 the implementation specification adopted in § 170.215(a)(2), including demonstrating search support for "SHALL" operations and parameters for all the data included in the 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	*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 implementation specification adopted in § 170.215(a)(2). 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 the implementation specification adopted in § 170.215(a)(2), including demonstrating search support for "SHALL" operations and parameters for all the data included in the 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

System Under Test	Test Lab Verification
target "(_revIncludes: Provenance:target)" for all the FHIR® resources included in the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(a)(2). **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 implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4).	"(_revIncludes: Provenance:target)" for all the FHIR® resources included in the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(a)(2). **Supported Search Operations for Multiple Patients' Data** 4. 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 implementation specification adopted in § 170.215(a)(4). 5. 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 the implementation specification adopted in § 170.215(a)(4).

Paragraph (g)(10)(i) – Data response

System Under Test	Test Lab Verification
Applies to Regulatory Standard (USCDI v1 + US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 + US Core STU v4.0.0) **Data Response Checks for Single and Multiple Patients** 1. DAT-PAT-1: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-8, of this section respectively, the health IT developer demonstrates the ability of the	*Applies to Regulatory Standard (USCDI v1 + US Core STU v3.1.1) and SVAP Version Approved (USCDI v1 + US Core STU v4.0.0)* **Data Response Checks for Single and Multiple Patients** 1. DAT-PAT-1: For responses to data for single and multiple patients as described in steps DAT-PAT-7, and DAT-PAT-8, of this section respectively, the tester verifies the ability of the Health IT Module

System Under Test	Test Lab Verification
Health IT Module to respond to requests for data according to the implementation specification adopted in § 170.215(a)(2), 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 and implementation specification adopted in § 170.215(a)(2) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(a)(2). 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(a)(2).	to respond to requests for data according to the implementation specification adopted in § 170.215(a)(2), 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 and implementation specification adopted in § 170.215(a)(2) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(a)(2). 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(a)(2). 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

System Under Test	Test Lab Verification
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(a)(2). 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(a)(2), 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(a)(2) for all the data included in the standard adopted in § 170.213.	to support a "Medication" FHIR® resource according to the "Medication List Guidance" section of the implementation specification adopted in § 170.215(a)(2). 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(a)(2), 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(a)(2) for all the data included in the standard adopted in § 170.213. **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 the implementation specification adopted in § 170.215(a)(4) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in

System Under Test	Test Lab Verification
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 the implementation specification adopted in § 170.215(a)(4) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2).: • "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device"; • "DiagnosticReport"; • "DocumentReference"; • "Encounter"; • "Goal"; • "Immunization"; • "Location" (if supported); • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Organization"; • "Patient"; • "Practitioner" • "Procedure"; and • "Provenance".	§ 170.213 and implementation specification adopted in § 170.215(a)(2). • "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 the implementation specification adopted in § 170.215(a)(4). 10. DAT-PAT-10: The tester verifies the ability of the Health IT Module to support a successful data response according to the implementation adopted in § 170.215(a)(4).

System Under Test	Test Lab Verification
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 the implementation specification adopted in § 170.215(a)(4). 10. DAT-PAT-10: The health IT developer demonstrates the ability of the Health IT Module to support a successful data response according to the implementation adopted in § 170.215(a)(4). 11. DAT-PAT-11: The health IT developer demonstrates the ability of the Health IT Module to support a data response error according to the implementation adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 14. DAT-PAT-14: The health IT developer demonstrates the ability of the Health IT Module to support a file request according to the implementation specification adopted in § 170.215(a)(4), 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.	11. DAT-PAT-11: The tester verifies the ability of the Health IT Module to support a data response error according to the implementation adopted in § 170.215(a)(4). 12. DAT-PAT-12: The tester verifies the ability of the Health IT Module to support a bulk data delete request according to the implementation specification adopted in § 170.215(a)(4). 13. DAT-PAT-13: The tester verifies the ability of the Health IT Module to support a bulk data status request according to the implementation specification adopted in § 170.215(a)(4). 14. DAT-PAT-14: The tester verifies the ability of the Health IT Module to support a file request according to the implementation specification adopted in § 170.215(a)(4), 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. *SVAP Version Approved: USCDI v2 + US Core STU v5.0.1* **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(a)(2), 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	Test Lab Verification
SVAP Version Approved: USCDI v2 + US Core STU v5.0.1 **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(a)(2), 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 and implementation specification adopted in § 170.215(a)(2) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(a)(2).	• 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 and implementation specification adopted in § 170.215(a)(2) according to the "Basic Provenance Guidance" section of the implementation specification adopted in § 170.215(a)(2). 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(a)(2). 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(a)(2).

System Under Test	Test Lab Verification
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(a)(2). 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(a)(2). 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(a)(2), 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	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(a)(2), 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(a)(2) for all the data included in the standard adopted in § 170.213. **Response to Requests for Multiple Patients' Data** 8. DAT-PAT-16: The health IT developer verifies the ability of the Health IT Module to respond to requests for multiple patients' data according to the implementation specification adopted in § 170.215(a)(4) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2).

System Under Test	Test Lab Verification
for a single patient's data according to the "US Core Server CapabilityStatement" section of the implementation specification adopted in § 170.215(a)(2) for all the data included in the standard adopted in § 170.213. **Response to Requests for Multiple Patients' Data** 8. DAT-PAT-16: The health IT developer demonstrates the ability of the Health IT Module to respond to requests for multiple patients' data according to the implementation specification adopted in § 170.215(a)(4) for all of the FHIR® resources associated with the profiles and Data Elements specified in and according to the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2). • "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device"; • "DiagnosticReport"; • "DocumentReference"; • "Encounter"; • "Goal"; • "Immunization"; • "Location" (if supported); • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Organization";	• "AllergyIntolerance"; • "CarePlan"; • "CareTeam"; • "Condition"; • "Device"; • "DiagnosticReport"; • "DocumentReference"; • "Encounter"; • "Goal"; • "Immunization"; • "Location" (if supported); • "Medication" (if supported); • "MedicationRequest"; • "Observation"; • "Organization"; • "Patient"; • "Practitioner" • "Procedure"; and • "Provenance". • "PractitionerRole" (if supported); • "QuestionnaireReponse" (if supported); • "RelatedPerson"; 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 the implementation specification adopted in § 170.215(a)(4).

System Under Test	Test Lab Verification
• "Patient"; • "Practitioner" • "Procedure"; and • "Provenance". • "PractitionerRole" (if supported); • "QuestionnaireReponse" (if supported); • "RelatedPerson"; 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 the implementation specification adopted in § 170.215(a)(4). 10. DAT-PAT-10: The health IT developer demonstrates the ability of the Health IT Module to support a successful data response according to the implementation adopted in § 170.215(a)(4). 11. DAT-PAT-11: The health IT developer demonstrates the ability of the Health IT Module to support a data response error according to the implementation adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 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 the implementation specification adopted in § 170.215(a)(4). 14. DAT-PAT-14: The health IT developer demonstrates the ability of the Health IT Module to support a file request according to the	10. DAT-PAT-10: The tester verifies the ability of the Health IT Module to support a successful data response according to the implementation adopted in § 170.215(a)(4). 11. DAT-PAT-11: The tester verifies the ability of the Health IT Module to support a data response error according to the implementation adopted in § 170.215(a)(4). 12. DAT-PAT-12: The tester verifies the ability of the Health IT Module to support a bulk data delete request according to the implementation specification adopted in § 170.215(a)(4). 13. DAT-PAT-13: The tester verifies the ability of the Health IT Module to support a bulk data status request according to the implementation specification adopted in § 170.215(a)(4). 14. DAT-PAT-14: The tester verifies the ability of the Health IT Module to support a file request according to the implementation specification adopted in § 170.215(a)(4), 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	Test Lab Verification
implementation specification adopted in § 170.215(a)(4), 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.	

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

System Under Test	Test Lab Verification
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.	*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.

Testing tab

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 Instructions