






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

Please consult the final rule entitled: *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* for associated regulations and a detailed description of the certification criterion with which these testing steps are associated.

Revision History

Version #	Description of Change	Version Date
1.0	2015 Edition Cures Update Test Procedure	XX-XX-2020

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 at § 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 and implementation specifications adopted at § 170.215(a)(1), (a)(2), and (a)(4), respectively, 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 § 170.215(a)(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 a single patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard § 170.215(b).
 - (ii.) An application capable of storing a client secret must be issued a refresh token valid for a period of no less than three months.
 - (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.) An application capable of storing a client secret must be issued a new refresh token valid for new period of no less than three months.
 - (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 V3.1.0](#)

§ 170.213 [United States Core Data for Interoperability \(USCDI\)](#)

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

§ 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 V3.1.0](#)

§ 170.213 [United States Core Data for Interoperability \(USCDI\)](#)

§ 170.215(a)(4) [HL7® FHIR Bulk Data Access \(Flat FHIR\) \(V1.0.0:STU 1\)](#)

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

§ 170.215(a)(2) [FHIR® US Core Implementation Guide STU V3.1.0](#)

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

§ 170.215(a)(4) [HL7® FHIR® Bulk Data Access \(Flat FHIR®\) \(V1.0.0:STU 1\)](#)

Paragraph (g)(10)(iii)

None

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

§ 170.215(a)(2) [FHIR® US Core Implementation Guide STU V3.1.0](#)

§ 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 \(Flat FHIR\) \(V1.0.0:STU 1\)](#)

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 \(Flat FHIR\) \(V1.0.0:STU 1\)](#)

Paragraph (g)(10)(vi)

None

Paragraph (g)(10)(vii)

None

Paragraph (g)(10)(viii)

None

Required Tests

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

System Under Test	Test Lab Verification
<p><u>Application Registration</u></p> <ol style="list-style-type: none"> 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. 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). 	<p><u>Application Registration</u></p> <ol style="list-style-type: none"> 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. 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
<p><u>Secure Connection</u></p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • Using TLS version 1.2 or higher; and • Conformance to FHIR Communications Security requirements. 	<p><u>Secure Connection</u></p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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
<p><u>Authentication and Authorization for Patient and User Scopes</u></p> <ol style="list-style-type: none"> 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. [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: <ul style="list-style-type: none"> • Launching the registered launch URL of the application; and • Passing the parameters: “iss” and “launch”. 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. [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): <ul style="list-style-type: none"> • The “.well-known/smart-configuration.json” path; and • A FHIR “CapabilityStatement”. 5. [Both] The health IT developer demonstrates the ability of the “.well-known/smart-configuration.json” path to support at least 	<p><u>Authentication and Authorization for Patient and User Scopes</u></p> <ol style="list-style-type: none"> 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. [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: <ul style="list-style-type: none"> • Launching the registered launch URL of the application; and • Passing the parameters: “iss” and “launch”. 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. [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): <ul style="list-style-type: none"> • The “.well-known/smart-configuration.json” path; and • A FHIR “CapabilityStatement”. 5. [Both] The tester verifies the ability of the “.well-known/smart-configuration.json” path to support at least the following as

System Under Test	Test Lab Verification
<p>the following as detailed in the implementation specification adopted in § 170.215(a)(3):</p> <ul style="list-style-type: none"> • “authorization_endpoint”; • “token_endpoint”; and • “capabilities” (including support for all the “SMART on FHIR Core Capabilities”). <p>6. [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:</p> <ul style="list-style-type: none"> • “authorize”; and • “token”. <p>7. [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:</p> <ul style="list-style-type: none"> • “response_type”; • “client_id”; • “redirect_uri”; • “launch” (for EHR-Launch mode only); • “scope”; • “state”; and • “aud”. <p>8. [Both] The health IT developer demonstrates 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):</p>	<p>detailed in the implementation specification adopted in § 170.215(a)(3):</p> <ul style="list-style-type: none"> • “authorization_endpoint”; • “token_endpoint”; and • “capabilities” (including support for all the “SMART on FHIR Core Capabilities”). <p>6. [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:</p> <ul style="list-style-type: none"> • “authorize”; and • “token”. <p>7. [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:</p> <ul style="list-style-type: none"> • “response_type”; • “client_id”; • “redirect_uri”; • “launch” (for EHR-Launch mode only); • “scope”; • “state”; and • “aud”. <p>8. [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):</p>

System Under Test	Test Lab Verification
<ul style="list-style-type: none"> • “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”). <p>9. [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 Electronic Health Information (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), including:</p> <ul style="list-style-type: none"> • “AllergyIntolerance”; 	<ul style="list-style-type: none"> • “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”). <p>9. [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), including:</p> <ul style="list-style-type: none"> • “AllergyIntolerance”; • “CarePlan”;

System Under Test	Test Lab Verification
<ul style="list-style-type: none"> • “CarePlan”; • “CareTeam”; • “Condition”; • “Device”; • “DiagnosticReport”; • “DocumentReference”; • “Encounter”; • “Goal”; • “Immunization”; • “Location”; • “Medication” (if supported); • “MedicationRequest”; • “Observation”; • “Organization”; • “Practitioner”; • “PractitionerRole”; • “Procedure”; and • “Provenance”. <p>10. [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 step 9 of this section in accordance with the implementation specification adopted in § 170.215(a)(3).</p> <p>11. [Both] The health IT developer demonstrates the ability of 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 explicitly enable the</p>	<ul style="list-style-type: none"> • “CareTeam”; • “Condition”; • “Device”; • “DiagnosticReport”; • “DocumentReference”; • “Encounter”; • “Goal”; • “Immunization”; • “Location”; • “Medication” (if supported); • “MedicationRequest”; • “Observation”; • “Organization”; • “Practitioner”; • “PractitionerRole”; • “Procedure”; and • “Provenance”. <p>10. [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 step 9 of this section in accordance with the implementation specification adopted in § 170.215(a)(3).</p> <p>11. [Both] The tester verifies the ability of 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 explicitly enable the “offline_access” scope according to the implementation specification adopted in § 170.215(a)(3).</p>

System Under Test	Test Lab Verification
<p>“offline_access” scope according to the implementation specification adopted in § 170.215(a)(3).</p> <p>12. [EHR-Launch] The health IT developer demonstrates the ability of the Health IT Module to return an error response if the following parameters provided by an application to the Health IT Module in step 7 of this section do not match the parameters originally provided to an application by the Health IT Module in step 2 of this section according to the implementation specification adopted in § 170.215(a)(3):</p> <ul style="list-style-type: none"> • “launch”; and • “aud”. <p>13. [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:</p> <ul style="list-style-type: none"> • “code”; and • “state”. <p>14. [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):</p> <ul style="list-style-type: none"> • “grant_type”; • “code”; • “redirect_uri”; • “client_id”; and • Authorization header including “client_id” and “client_secret”. 	<p>12. [EHR-Launch] The tester verifies the ability of the Health IT Module to return an error response if the following parameters provided by an application to the Health IT Module in step 7 of this section do not match the parameters originally provided to an application by the Health IT Module in step 2 of this section according to the implementation specification adopted in § 170.215(a)(3):</p> <ul style="list-style-type: none"> • “launch”; and • “aud”. <p>13. [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:</p> <ul style="list-style-type: none"> • “code”; and • “state”. <p>14. [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):</p> <ul style="list-style-type: none"> • “grant_type”; • “code”; • “redirect_uri”; • “client_id”; and • Authorization header including “client_id” and “client_secret”. <p>15. [Both] The tester verifies the ability of the Health IT Module to return a JSON object to applications according to the</p>

System Under Test	Test Lab Verification
<p>15. [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:</p> <ul style="list-style-type: none"> • “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). <p>16. [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).</p> <p>17. [Standalone-Launch] 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 8 of this section</p>	<p>implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b), including the following:</p> <ul style="list-style-type: none"> • “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). <p>16. [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).</p> <p>17. [Standalone-Launch] The tester verifies the ability of the Health IT Module to return a “Patient” FHIR resource that matches the patient context provided in step 8 of this section according to the implementation specification adopted in § 170.215(a)(2).</p>

System Under Test	Test Lab Verification
<p>according to the implementation specification adopted in § 170.215(a)(2).</p> <p>18. [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).</p> <p><u>Subsequent Connections: Authentication and Authorization for Patient and User Scopes</u></p> <p>19. The health IT developer demonstrates the ability of the Health IT Module to issue a new refresh token valid for a 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).</p> <p>20. 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).</p>	<p>18. [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).</p> <p><u>Subsequent Connections: Authentication and Authorization for Patient and User Scopes</u></p> <p>19. The tester verifies the ability of the Health IT Module to issue a new refresh token valid for a 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).</p> <p>20. 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).</p>

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

System Under Test	Test Lab Verification
<p><u>Patient Authorization Revocation</u></p> <p>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</p>	<p><u>Patient Authorization Revocation</u></p> <p>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.</p>

System Under Test	Test Lab Verification
application with revoked access to receive patient Electronic Health Information (EHI).	

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

System Under Test	Test Lab Verification
<p><u>Authentication and Authorization for System Scopes</u></p> <ol style="list-style-type: none"> 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). 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): <ul style="list-style-type: none"> “scope”; “grant_type”; “client_assertion_type”; and “client_assertion”. 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): <ul style="list-style-type: none"> “alg” header; “kid” header; “typ” header; “iss” claim; “sub” claim; 	<p><u>Authentication and Authorization for System Scopes</u></p> <ol style="list-style-type: none"> 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). 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): <ul style="list-style-type: none"> “scope”; “grant_type”; “client_assertion_type”; and “client_assertion”. 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): <ul style="list-style-type: none"> “alg” header; “kid” header; “typ” header; “iss” claim; “sub” claim;

System Under Test	Test Lab Verification
<ul style="list-style-type: none"> • “aud” claim; • “exp” claim; and • “jti” claim. <ol style="list-style-type: none"> 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. 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 received by an application indicates. 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. 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. The health IT developer demonstrates the ability of the Health IT Module to assure 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. 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: 	<ul style="list-style-type: none"> • “aud” claim; • “exp” claim; and • “jti” claim. <ol style="list-style-type: none"> 4. The tester verifies the ability of the Health IT Module to receive and process the JSON Web Key (JWK) structure via a TLS-protected URL to support authorization for system scopes in § 170.315(g)(10)(v)(B). 5. The tester verifies that the Health IT Module does not cache a JWK Set received via a TLS-protected URL for longer than the “cache-control” header received by an application indicates. 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. 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. The tester verifies the ability of the Health IT Module to assure 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. 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
<ul style="list-style-type: none"> • “access_token”; • “token_type”; • “expires_in”; and • “scope”. <p>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).</p>	<ul style="list-style-type: none"> • “access_token”; • “token_type”; • “expires_in”; and • “scope”. <p>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).</p>

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

System Under Test	Test Lab Verification
<p><u>Token Introspection</u></p> <ol style="list-style-type: none"> 1. The health IT developer demonstrates the ability of the Health IT Module to receive and validate a token it has issued. 	<p><u>Token Introspection</u></p> <ol style="list-style-type: none"> 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
<p><u>Supported Search Operations for a Single Patient’s Data</u></p> <ol style="list-style-type: none"> 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. 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. 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 	<p><u>Supported Search Operations for a Single Patient’s Data</u></p> <ol style="list-style-type: none"> 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. 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. 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 the

System Under Test	Test Lab Verification
<p>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).</p> <p><u>Supported Search Operations for Multiple Patients’ Data</u></p> <ol style="list-style-type: none"> 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). 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). 	<p>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).</p> <p><u>Supported Search Operations for Multiple Patients’ Data</u></p> <ol style="list-style-type: none"> 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). 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
<p><u>Data Response Checks for Single and Multiple Patients</u></p> <ol style="list-style-type: none"> For responses to data for single and multiple patients as described in steps 7 and 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. 	<p><u>Data Response Checks for Single and Multiple Patients</u></p> <ol style="list-style-type: none"> For responses to data for single and multiple patients as described in steps 7 and 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.

System Under Test	Test Lab Verification
<p>2. The health IT developer demonstrates the ability of the Health IT Module to respond with data that meet the following conditions:</p> <ul style="list-style-type: none"> • 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 2-6 of this section. <p>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).</p> <p>4. The health IT developer demonstrates the ability of the Health IT Module to support a “DocumentReference” FHIR resource for each of the “Clinical Notes” and “Diagnostic Reports” included in the “Clinical Notes Guidance” section of the implementation specification adopted in § 170.215(a)(2).</p> <p>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).</p>	<p>2. The tester verifies the ability of the Health IT Module to respond with data that meet the following conditions:</p> <ul style="list-style-type: none"> • 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 2-6 of this section. <p>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).</p> <p>4. The tester verifies the ability of the Health IT Module to support a “DocumentReference” FHIR resource for each of the “Clinical Notes” and “Diagnostic Reports” included in the “Clinical Notes Guidance” section of the implementation specification adopted in § 170.215(a)(2).</p> <p>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).</p>

System Under Test	Test Lab Verification
<p>6. The health IT developer demonstrates the ability of the Health IT Module to support “DataAbsentReason” as specified in the implementation specification adopted in § 170. 215(a)(2), including:</p> <ul style="list-style-type: none"> • “DataAbsentReason” Extension; and • “DataAbsentReason” Code System. <p>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.</p> <p><u>Response to Requests for a Single Patient’s Data</u></p> <p>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.</p> <p><u>Response to Requests for Multiple Patients’ Data</u></p> <p>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</p>	<p>6. The tester verifies the ability of the Health IT Module to support “DataAbsentReason” as specified in the implementation specification adopted in § 170. 215(a)(2), including:</p> <ul style="list-style-type: none"> • “DataAbsentReason” Extension; and • “DataAbsentReason” Code System. <p>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.</p> <p><u>Response to Requests for a Single Patient’s Data</u></p> <p>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.</p> <p><u>Response to Requests for Multiple Patients’ Data</u></p> <p>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 § 170.213</p>

System Under Test	Test Lab Verification
<p>standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2), including the following FHIR resources:</p> <ul style="list-style-type: none"> • “AllergyIntolerance”; • “CarePlan”; • “CareTeam”; • “Condition”; • “Device”; • “DiagnosticReport”; • “DocumentReference”; • “Encounter”; • “Goal”; • “Immunization”; • “Location”; • “Medication” (if supported); • “MedicationRequest”; • “Observation”; • “Organization”; • “Practitioner”; • “PractitionerRole”; • “Procedure”; and • “Provenance”. <p>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).</p> <p>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).</p>	<p>and implementation specification adopted in § 170.215(a)(2), including the following FHIR resources:</p> <ul style="list-style-type: none"> • “AllergyIntolerance”; • “CarePlan”; • “CareTeam”; • “Condition”; • “Device”; • “DiagnosticReport”; • “DocumentReference”; • “Encounter”; • “Goal”; • “Immunization”; • “Location”; • “Medication” (if supported); • “MedicationRequest”; • “Observation”; • “Organization”; • “Practitioner”; • “PractitionerRole”; • “Procedure”; and • “Provenance”. <p>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).</p> <p>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).</p>

System Under Test	Test Lab Verification
<p>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).</p> <p>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).</p> <p>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).</p> <p>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.</p> <p>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.</p>	<p>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).</p> <p>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).</p> <p>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).</p> <p>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.</p> <p>15. The tester verifies that the information provided as part of this data response includes data for patients in the group identifier provided during the “group-export” request.</p>

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

System Under Test	Test Lab Verification
<p><u>API Documentation Requirements</u></p> <ol style="list-style-type: none"> The health IT developer supplies documentation describing the API(s) of the Health IT Module and includes at a minimum: <ul style="list-style-type: none"> 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. The health IT developer demonstrates that the documentation described in step 1 of this section is available via a publicly accessible hyperlink that does not require preconditions or additional steps to access. 	<p><u>API Documentation Requirements</u></p> <ol style="list-style-type: none"> The tester verifies that the documentation supplied by the health IT developer describing the API(s) of the Health IT Module includes at a minimum: <ul style="list-style-type: none"> 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. The tester verifies that the documentation described in step 1 of this section is available via a publicly accessible hyperlink that does not require preconditions or additional steps to access.

Testing tab

Testing Tool

[Inferno](#)

Test Tool Documentation

[Inferno User's Guide](#)