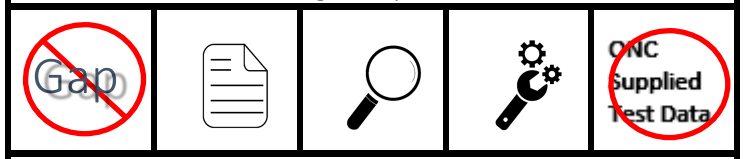
The Office of the National Coordinator for
Health Information Technology

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

Testing Components:



NPRM Draft

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

Revision History

Version #	Description of Change	Version Date
1.0	NPRM Draft	04-05-2019

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*. Respond to requests for data (based on an ID or other token) for each of the resources referenced by the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a)(2) and (3).

(ii) *Search support*. Respond to search requests for data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) *App registration*. Enable an application to register with the technology's "authorization server."

(iv) *Secure connection*. Establish a secure and trusted connection with an application that requests data in accordance with the standard adopted in § 170.215(a)(5).

(v) *Authentication and app authorization – 1st time connection*. The first time an application connects to request data the technology:

(A) *Authentication*. Demonstrates that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the standard adopted in § 170.215(b).

(B) *App authorization*. Demonstrates that a user can authorize applications to access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) and issue a refresh token that is valid for a period of at least 3 months.

(vi) *Authentication and app authorization – Subsequent connections*. Demonstrates that an application can access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months.

(vii) *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 an authorization server.

(B) The documentation used to meet paragraph (g)(10)(vii)(A) of this section must be available via a publicly accessible hyperlink.

Standard(s) Referenced

Paragraph (g)(10)(i)

§ 170.215(a)(1) Fast Healthcare Interoperability Resources (FHIR) Draft Standard for Trial Use (DSTU) 2 (v1.0.2-7202)
§ 170.215(a)(2) API Resource Collection in Health (ARCH) Version 1
§ 170.215(a)(3) Argonaut Data Query Implementation Guide Version 1.0.0

Paragraph (g)(10)(ii)

§ 170.215(a)(4) The Argonaut Data Query Implementation Guide Server

Paragraph (g)(10)(iv)

§ 170.215(a)(5) SMART Application Launch Framework Implementation Guide Release 1.0.0

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

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

Paragraph (g)(10)(v)(B)
§ 170.215(a)(5) SMART Application Launch Framework Implementation Guide Release 1.0.0

Paragraph (g)(10)(vi)
§ 170.215(a)(5) SMART Application Launch Framework Implementation Guide Release 1.0.0

Required Tests

Paragraph (g)(10)(iii) – App Registration (Discovery/Registration)
Paragraph (g)(10)(iv) – Secure Connection

System Under Test	Test Lab Verification
Conformance Discovery 1. The user demonstrates that the data exchange with the Health IT Module's FHIR server is trusted and secure. 2. The user demonstrates that the Health IT Module's FHIR server provides a conformance statement that specifies which FHIR interacts and resources are supports in accordance with the standard specified at § 170.215(a)(1) HL7 Fast Healthcare Interoperability Resources (FHIR®) DSTU Release 2. 3. The user demonstrates that the Health IT Module's FHIR server explicitly states the support for JSON representation format for FHIR resources in accordance with the standard specified at § 170.215(a)(4) Argonaut Data Query Implementation Guide Server. 4. The user demonstrates that the Health IT Module's FHIR server supports the automated discovery of OAuth2 endpoints in accordance with the standard specified at § 170.215(a)(5) Health Level 7 (HL7®) SMART App Authorization Implementation Guide Version 1.0.0 using the FHIR server Conformance Statement.	**Conformance Discovery** 1. The tester verified that Health IT Module's FHIR Server is secured by transport layer security (TLS) in accordance with the standard specified at § 170.215(a)(5). 2. The tester verifies that the Health IT Module provides a method to get the conformance statement from the FHIR server and that the FHIR server responses with a success status code and contains a valid DSTU Conformance resource as specified in § 170.215(a)(1). 3. The tester verifies that the conformance statement format field returned by the Health IT Module's FHIR server contains one of the following values: ○ json; ○ application/json; or ○ application/json+fhir. 4. The tester verifies that the capability statement returned as part of the Health IT Module's FHIR server conformance uses the Conformance.rest.security element to specify the:

System Under Test	Test Lab Verification
5. The user demonstrates that the Health IT Module's FHIR server supports the automated discovery of OAuth2 endpoints in accordance with the standard specified at § 170.215(a)(5) using a well-known Uniform Resource Identifiers (URIs) json file. 6. The user demonstrates that the Health IT Module's FHIR server's conformance statement declaration identifies the list of profiles, operations, and search parameters supported in accordance with the standard specified at § 170.215(a)(4). **App Registration** 7. The health IT developer supplies documentation describing the method used to provide a reliable secure authorization for FHIR resources needing to access authorized servers including any standards used, the methodology used to protect client registration endpoints (i.e. transport layer security), error reporting as it relates to FHIR resource registration, and whether the environment for the app is confidential (server-based application) or public (end-user device application).	○ URL to the OAuth2 authorization endpoint; and ○ URL to the OAuth2 token endpoint. 5. The tester verifies that a JSON document at the location formed by appending /.well-known/smart-configuration to their base URL is exposed and specifies the: ○ URL to the OAuth2 authorization endpoint; and ○ URL to the OAuth2 token endpoint 6. The tester verifies that Argonaut Data Query profiles supported are in accordance with the standard specified at § 170.215(a)(4) and are accurately identified as part of the Resource Conformance for each FHIR resource supported by the Health IT Module's FHIR server in accordance with the standard specified at § 170.215(a)(1). **App Registration** 7. The tester verifies that the identified documentation describes the method for the Health IT Module's app registration is in accordance with the standard specified at § 170.215(a)(5) and is complete by including, at a minimum, a description of: ○ A list of standards used to perform the App registration; ○ App confidentiality; ○ The transport security methodology; ○ The application environment; and ○ Error reporting.

Paragraph (g)(10)(v)(B) – App Authorization (Launch Sequence)
Paragraph (g)(10)(iv) – Secure Connection

System Under Test	Test Lab Verification
EHR Launch With User-Level Scope	**EHR Launch With User-Level Scope**

System Under Test	Test Lab Verification
1. The user demonstrates the ability of the Health IT Module to launch a user-level app from an established Health IT Module session and initiate a new session in accordance with the standard specified at § 170.215(a)(5) Health Level 7 (HL7®) SMART App Authorization Implementation Guide Version 1.0.0. 2. The user demonstrates the Health IT Module session launch returns the required parameters as specified at § 170.215(a)(5) including: ○ *Iss parameter* to identify the Health IT Module FHIR endpoint; and ○ *Launch parameter* to identify the specific EHR launch. 3. The user demonstrates that the OAuth *authorize* endpoint is trusted and secure in accordance to the standard specified at § 170.215(a)(5). 4. The user demonstrates the ability of the app, launched from within an established Health IT Module session, to initiate a query to the Health IT Module FHIR server to retrieve the OAuth 2.0 authorize and token endpoint URLs in accordance to the standard specified at § 170.215(a)(5). 5. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for authorization using the OAuth 2.0 endpoints and the information sent from the app as specified at § 170.215(a)(5): ○ *Response_ type parameter* fixed *code* value; ○ *Client_id* identifying the client; ○ *Redirect_uri* matching one of the client's pre-registered redirected URIs; ○ *Launch parameter* matching the launch value received from the Health IT Module; ○ *Scope parameter* indicating the user-level clinical data scope and	1. The tester verifies that the EHR launch has opened a new session pointing to the app's registered launch URL as specified in § 170.215(a)(5). 2. The tester verifies the EHR launch includes information in accordance with the standard specified at § 170.215(a)(5) and provides: ○ The ability of the app to identify the Health IT Module's FHIR endpoint; and ○ The ability for the Health IT Module context handle to be passed along as part of the launch URL. 3. The tester verifies that all sensitive information transmitted from the app to Health IT FHIR server is over a secure and trusted connection using Transport Layer Security (TLS) in accordance with the standard specified at § 170.215(a)(5). 4. The tester verifies that upon receiving launch notification the app can initiate a query to the Health IT Module FHIR server and receive a response with the OAuth 2.0 endpoint URLs' in accordance with the standard specified at § 170.215(a)(5). 5. The tester verifies the following information is returned from the Health IT Module Authorization server in response to the request for authorization in accordance with the standard specified at § 170.215(a)(5): ○ *Response_ type parameter code*; ○ *State parameter* contains the exact value sent from the client; and ○ *Scope parameter* minimally includes the Client_id, openid, fhirUser, and the user-level clinical data scope. Additionally, the scope must include read access. 6. The tester verifies that all sensitive information exchanged between

System Under Test	Test Lab Verification
OpenID Connect scope parameters as specified in § 170.215(b) OpenID Connect Core 1.0; ○ *State parameter* opaque value maintained between the request and the callback; and ○ *Aud parameter identifying the URL of the* Health IT Module FHIR resource server. 6. The user demonstrates that the OAuth *token* endpoint is trusted and secure in accordance to the standard specified at § 170.215(a)(5). 7. Negative Testing: The user demonstrates the ability of the Health IT Module Authorization server to return an error response due to a failed or invalid verification. 8. The user demonstrates the ability of the app to trade the authorization *code* in for an *access token* from the Health IT Module Authorization server's token endpoint URL as specified in the standard § 170.215(a)(5). 9. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for an access token with the body of the message specified in accordance with the standard specified at § 170.215(a)(5). 10. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for an access token with the header of the message specified in accordance with the standard specified at § 170.215(a)(5). 11. The user demonstrates the ability of the Health IT Module Authorization server's response to a request for an access token to include the launch context patient parameter in accordance with the standard specified at § 170.215(a)(5). 12. The user demonstrates the ability to retrieve a Patient resource in accordance with the standard specified at § 170.215(a)(1) HL7 Fast	the app and the Health IT Authorization server is over a secure and trusted connection using TLS in accordance with the standard specified at § 170.215(a)(5). 7. Negative Testing: The tester verifies that a Health IT Module Authorization server returns an error when supplied an invalid Refresh Token or a Client ID. 8. The tester verifies that the App can exchange the Authorization code from the Health IT Module Authorization server with an access token from the Health IT Module Authorization server's token endpoint URL as specified in § 170.215(a)(5). 9. The tester verifies the following information formatted as a json object is returned from the Health IT Module Authorization server upon the exchange the Authorization code in accordance with the standard specified at § 170.215(a)(5): ○ *Access code* issued by the authorized server*;* ○ *Token Type* fixed at bearer; ○ *Expiration lifetime* (in seconds); and ○ Authorized *Scope.* 10. The tester verifies the header information is returned from the Health IT Module Authorization server upon the exchange the Authorization code is in accordance with the standard specified at § 170.215(a)(5): ○ *HTTP "Cache-Control" response header field value is "no-store"*; and ○ "Pragma" response header field value is "*no-cache*". 11. The tester verifies the Health IT Module Authorization server returns the patient identifier sent by the EHR session as a launch context parameter in accordance with the standard specified at § 170.215(a)(5).

System Under Test	Test Lab Verification
Healthcare Interoperability Resources (FHIR®) DSTU Release 2. **<u>Standalone Launch With Patient-Level Scope</u>** 13. The user demonstrates that the OAuth *authorize* endpoint is trusted and secure in accordance to the standard specified at § 170.215(a)(5). 14. The user demonstrates the ability of the app, launched from outside the Health IT Module (e.g. a mobile phone or app icon), to initiate a query to the Health IT Module FHIR server to retrieve the OAuth 2.0 authorize and token endpoint URLs in accordance to the standard specified at § 170.215(a)(5). 15. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for authorization using the OAuth 2.0 endpoints and the information sent from the app as specified at § 170.215(a)(5): ○ *Response_ type parameter* fixed *code* value; ○ *Client_id* identifying the client; ○ *Redirect_uri* matching one of the client's pre-registered redirected URIs; ○ *Launch parameter* matching the launch value requested by the app (e.g. launch/patient, launch/user-id); ○ *Scope parameter* indicating the patient-level clinical data scope and OpenID Connect scope parameters as specified in § 170.215(b); ○ *State parameter* opaque value maintained between the request and the callback; and ○ *Aud parameter identifying the URL of the* Health IT Module FHIR resource server. 16. The user demonstrates that the OAuth *token* endpoint is trusted and	12. The tester verifies the response returned from the Health IT Module for the Patient resource is in accordance with the standard specified at § 170.215(a)(1). **<u>Standalone Launch With Patient-Level Scope</u>** 13. The tester verifies that all sensitive information transmitted from the Health IT Module Authorization server's OAuth *authorize* endpoint is over a secure and trusted connection using TLS. 14. The tester verifies that that the app can discover the Health IT Module authorization OAuth authorization and token endpoint URLs and receive a response from the Health IT Module Authorization server using the redirect URIs based upon its launch context requirements. 15. The tester verifies the following information is returned from the Health IT Module Authorization server in response to the request for authorization in accordance with the standard specified at § 170.215(a)(5): ○ *Response_ type parameter code*; ○ *State parameter* contains the exact value sent from the client; and ○ *Scope parameter* minimally includes the Client_id, openid, fhirUser, and the patient-level clinical data scope. Additionally, the scope must include read access. 16. The tester verifies that all sensitive information transmitted from the Health IT Module Authorization server's OAuth *authorize* endpoint is over a secure and trusted connection using TLS. 17. Negative Testing: The tester verifies that a Health IT Module Authorization server returns an error when supplied an invalid Refresh Token or a Client ID.

System Under Test	Test Lab Verification
secure in accordance to the standard specified at § 170.215(a)(5). 17. Negative Testing: The user demonstrates the ability of the Health IT Module Authorization server to return an error response due to a failed or invalid verification. 18. The user demonstrates the ability of the app to trade the authorization *code* in for an *access token* from the Health IT Module Authorization server's token endpoint URL as specified in the standard § 170.215(a)(5). 19. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for an access token with the body of the message specified in accordance with the standard specified at § 170.215(a)(5). 20. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for an access token with the header of the message specified in accordance with the standard specified at § 170.215(a)(5). 21. The user demonstrates the ability of the Health IT Module Authorization server's response to a request for an access token to include the launch context patient parameter in accordance with the standard specified at § 170.215(a)(5). 22. The user demonstrates the ability to retrieve a Patient resource in accordance with the standard specified at § 170.215(a)(1).	18. The tester verifies that the app can exchange the authorization code from the Health IT Module Authorization server with an access token from the Health IT Module Authorization server's token endpoint URL as specified in § 170.215(a)(5). 19. The tester verifies the following information formatted as a json object is returned from the Health IT Module Authorization server upon the exchange of the authorization code in accordance with the standard specified at § 170.215(a)(5): ○ *Access code* issued by the authorized server*;* ○ *Token Type* fixed at bearer; ○ *Expiration lifetime* (in seconds); and ○ Authorized *Scope.* 20. The tester verifies the header information is returned from the Health IT Module Authorization server upon the exchange of the Authorization code in accordance with the standard specified at § 170.215(a)(5): ○ *HTTP "Cache-Control" response header field value is "no-store"*; and ○ "Pragma" response header field value is "*no-cache*"*.* 21. The tester verifies the Health IT Module Authorization server returns the patient identifier sent by the App as a launch context parameter in accordance with the standard specified at § 170.215(a)(5). 22. The tester verifies the response returned from the Health IT Module is for the Patient resource in accordance with the standard specified at § 170.215(a)(1).

System Under Test	Test Lab Verification
Authentication Request 1. For each of the launch types performed in section (g)(10)(v)(B), the user demonstrates the ability of the Health IT Module Authorization server to authenticate according to the standard specified at § 170.215(b) OpenID Connect Core 1.0 by executing steps 2-7. 2. The user demonstrates the ID token provided in section (g)(10)(v)(B) during the launch is formatted in accordance with the standard specified at § 170.215(b) and that its content is correct. 3. The user demonstrates the ability of the Health IT Module Authorization server to retrieve the issuers' OpenID configuration in order to get to the JSON Web Key as specified in the standard at § 170.215(b). 4. The user demonstrates the ability of the Health IT Module Authorization server to retrieve the JSON Web Key using the" jwks_uri" property within the OpenID Configuration in accordance with the standard at § 170.215(b). 5. The user demonstrates the ability of the Health IT Module Authorization server to use the JSON Web Key to decode the ID token as specified in the standard at § 170.215(b). 6. The user demonstrates the ability of the Health IT Module Authorization server to verify the ID token information using the JSON Web Key Information as specified in the standard at § 170.215(b). 7. The user demonstrates the ability of the Health IT Module Authorization server to extract the fhirUser claim within the ID token as specified in the standard at § 170.215(b). **Resource Retrieval Protection** 8. The health IT developer supplies documentation that provides	**Authentication Request** 1. The tester verifies that the Health IT Module Authorization server can authenticate according to the standard specified at § 170.215(b) for both the EHR session and Standalone App by verifying steps 2-7 for each of the launch types. 2. The tester verifies that the format of the ID token provided in section (g)(10)(v)(B) during the launch is a valid jwt token in accordance with the standard specified at § 170.215(b) and that the ID token content is in accordance with the standard specified at § 170.215(b) and minimally includes the: ○ *Iss parameter* - the Issuer Identifier; ○ *Sub parameter* - Subject Identifier (a unique identifier not to be shared); ○ *Aud parameter* Client Identifier (who the ID token is intended for); ○ Exp (Expiration time) parameter – time after which the ID token will not be valid ○ *Iat – (Time of Issuing) parameter* – time the ID token was issued; and ○ ID token signature. 3. The tester verifies that the header and the payload information in the ID token is complete and accurate and is in accordance with the standard specified at § 170.215(b). As well as at a minimum, it contains the correct issuer properties containing a case sensitive URL. 4. The tester verifies that the Health IT Module Authorization server can fetch the JSON Web Key from the redirected uri specified in the OpenID configuration in accordance with standard at § 170.215(b). 5. The tester verifies that the Health IT Module Authorization server

System Under Test	Test Lab Verification
information on the lifetime of the access token. 9. The health IT developer supplies documentation describing the method used to protect the app from potential misbehaving or malicious values passed to its redirected URL, including any standards used and the methodology used.	can decrypt the ID token using the ID token's signature and the retrieved JSON Web Key public key as specified in the standard at § 170.215(b). 6. The tester verifies that the Health IT Module Authorization server can verify the integrity of the ID token claims, using the hash algorithm, as specified in the standard at § 170.215(b). 7. The tester verifies that the Health IT Module Authorization server can extract the fhirUser claim within the ID token and treat it as the URL of a FHIR resource as specified in the standard at § 170.215(b). **<u>Resource Retrieval Protection</u>** 8. The tester verifies that the identified documentation describes how the lifetime of the *access token* is managed and that the lifetime is less than 60 minutes. 9. The tester verifies that the identified documentation describes the method for protecting the app from potential misbehaving or malicious values passed to its redirected URL is in accordance with the standard specified at § 170.215(a)(5) and is complete by including, at a minimum, a description of: ○ The set of implementation standards; ○ The transport security methodology to ensure sensitive information is transmitted only to authenticated servers over TLS-secured channels; ○ The application environment (e.g. use of the *state* parameter, handling executable code, storage of persistent tokens); ○ Proof that app SHALL NOT execute any inputs; ○ Proof that app SHALL NOT forward values passed back to its redirect URL per the specification; ○ Proof that app SHALL NOT store bearer tokens in cookies that are

System Under Test	Test Lab Verification
	transmitted in the clear; and ○ Error reporting.

Paragraph (g)(10)(v)(B) – App Authorization (Refresh Token)
Paragraph (g)(10)(vi) – Authentication and App Authorization – Subsequent Connections (Token Refresh)
Paragraph (g)(10)(iv) – Secure Connection

System Under Test	Test Lab Verification
Refresh Tokens 1. For each of the launch types performed in section (g)(10)(v)(B), the user demonstrates the ability of the Health IT Module Authorization server to support a Refresh Token as specified in the standard § 170.215(a)(5) Health Level 7 (HL7®) SMART App Authorization Implementation Guide Version 1.0.0 by executing steps 2-8. 2. Negative Testing: Using the previously launched EHR session or the Standalone app in section (g)(10)(v)(B), the user demonstrates the ability of the Health IT Module Authorization server to return an error response when supplied an invalid Refresh Token or a Client ID as specified in the standard at § 170.215(a)(5). 3. The user demonstrates the ability of the Health IT Module to successfully exchange a new access token for a refresh token in accordance with the standard specified at § 170.215(a)(5). 4. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for a new access token with the body of the message specified in accordance with the standard specified at § 170.215(a)(5). 5. The user demonstrates the ability of the Health IT Module Authorization server to respond to the request for a new access token with the header of the message specified in accordance with	**Refresh Tokens** 1. The tester verifies that the Health IT Module Authorization server can support a Refresh Token as specified in the standard § 170.215(a)(5) for both the EHR session and Standalone App by verifying steps 2-8 for each of the launch types. 2. Negative Testing: The tester verifies that a Health IT Module Authorization server returns an error when supplied an invalid Refresh Token or a Client ID. 3. The tester verifies that the Health IT Module can successfully exchange a refresh token with a new access token and that the response grants authorization in accordance with the standard specified at § 170.215(a)(5). 4. The tester verifies the following information formatted as a json object is returned from the Health IT Module Authorization server upon the exchange the authorization code in accordance with the standard specified at § 170.215(a)(5): ○ *Access code* issued by the authorized server; ○ *Token Type* fixed at bearer; ○ *Expiration lifetime* (in seconds); and ○ Authorized *Scope.* 5. The tester verifies the header information is returned from the

System Under Test	Test Lab Verification
the standard specified at § 170.215(a)(5). 6. The user provides documentation describing the method used to expire a token. 7. The health IT developer supplies documentation about the Health IT Module's token refresh behavior. 8. The health IT developer demonstrates the ability to retrieve a Patient resource using the new access token in accordance with the standard specified in § 170.215(a)(1) HL7 Fast Healthcare Interoperability Resources (FHIR®) DSTU Release 2.	Health IT Module Authorization server upon the exchange the refresh token is in accordance with the standard specified at § 170.215(a)(5): ○ *HTTP "Cache-Control" response header field value is "no-store"*; and ○ "Pragma" response header field value is "*no-cache*". 6. The tester verifies that the identified documentation describes the method used to expire a token. 7. The tester verifies that the identified documentation describes how a token provided an app expires after a period of time and that the minimum period is 3 months. 8. The tester verifies the response returned from the Health IT Module is for a Patient resource in accordance with the standard specified at § 170.215(a)(1).

Paragraph (g)(10)(i) – Retrieve Clinical Data (Argonaut Profile Conformance – Read)
Paragraph (g)(10)(iv) – Secure Connection

System Under Test	Test Lab Verification
Response to Requests for Data for Patient Services 1. The health IT developer supplies documentation for each of the supported APIs (FHIR resources) implemented in accordance with the standards specified in § 170.215(a)(1) HL7 Fast Healthcare Interoperability Resources (FHIR®) DSTU Release 2, including required and optional resource interactions and/or capabilities supported. 2. Using a launched session from section (g)(10)(v)(A), for each of the supported APIs the user demonstrates the ability of the Health IT	**Response to Requests for Data for Patient Services** 1. The tester verifies that the identified documentation for the Health IT Module resources is specified in accordance with the standard specified in § 170.215(a)(1) and is complete and without omission. Additionally, the tester verifies that, at a minimum, the set of APIs includes all of the APIs specified in § 170.215(a)(2) which includes: ○ AllergyIntolerance; ○ CarePlan; ○ Condition;

System Under Test	Test Lab Verification
Module to respond with the requested clinical data for a single patient in accordance with the standard specified in § 170.215(a)(1). 3. Negative Test: The user demonstrates the ability of the Health IT Module to reject a request for a single patient request without proper authorization in accordance with the standard specified in § 170.215(a)(4) Argonaut Data Query Implementation Guide Server. **Response to Requests for Data for Population Services** 4. The health IT developer supplies documentation for supporting multiple patients (a.k.a. population services) APIs (FHIR resources) includes: ○ Required and optional resource interactions and/or capabilities supported; ○ Limitations on the amount of data which can be returned with a single request; ○ Mechanisms to throttle the information so the FHIR Server does not become overwhelmed; and ○ Performance expectations. 5. Using the session launched with a user-level scope in section (g)(10)(v)(A), for each of the supported population services APIs the user demonstrates the ability of the Health IT Module to respond with the requested clinical data for multiple patients (greater than one patient). 6. For one of the supported population services APIs, the user demonstrates the ability of the Health IT Module to respond with the requested clinical data for a population of at least 230 patients.	○ Device; ○ DiagnosticReport; ○ Goal; ○ Immunization; ○ Medication; ○ MedicationOrder; ○ MedicationStatement; ○ Observation; ○ Patient; ○ Procedure; ○ Provenance; and ○ DocumentReference. 2. The tester verifies that the app can retrieve all of the patient clinical data associated with each of the supported FHIR resources in accordance with the standard specified in § 170.215(a)(1): ○ Support json resource format for all interactions; and ○ Is accurate and without omission based upon the health IT developer's documentation for data return. 3. Negative Test: The tester verifies that the app is denied access to a single patient for an unauthorized request as specified at § 170.215(a)(4). **Response to Requests for Data for Population Services** 4. The tester verifies that the identified documentation for the Health IT Module resources is complete and without omission. Additionally, the tester verifies that: ○ At a minimum, the set of APIs includes support for all of the APIs specified in § 170.215(a)(2) as a population service;

System Under Test	Test Lab Verification
7. Negative Test: The user demonstrates the ability of the Health IT Module to reject a request for a population service request without proper authorization. **Retrieval of Data Elements for a Patient** 8. Using a launch session from section (g)(10)(v)(A), the user demonstrates the ability of the Health IT Module to respond with the requested clinical data for a single patient using the Patient resource in accordance in accordance with the standard specified in § 170.215(a)(1). 9. The user demonstrates the ability of the Health IT Module to access the patient address and patient telecom as part of the Patient Resource in accordance with the standard specified in § 170.215(a)(1). 10. The user demonstrates the ability of the Health IT Module to access all of the data elements associated with the API Resource Collection as specified in the standard at § 170.215(a)(2) API Resource Collection in Health (ARCH) Standard Version 1 for a single patient as an electronic patient record. **Retrieval of Data Elements for a Population Service** 11. Using the session launched with a user-level scope in section (g)(10)(v)(B), the user demonstrates the ability of the Health IT Module to access all of the data elements associated with the API Resource Collection as specified in the standard at § 170.215(a)(2) for multiple patients (more than one patient) as an electronic patient record for each patient.	○ The APIs defined for population services an aggregate of the information requested; ○ There is a discussion on how population data is supported both on the client and the server; and ○ There is a discussion on performance when dealing with population services. 5. The tester verifies that the app can retrieve all of the clinical data for the patients specified, for each of the supported FHIR resources, such that it: ○ Supports json resource format for all interactions; and ○ Is accurate and without omission based upon the health IT developer's documentation for data return. 6. The tester verifies that the app can retrieve all of the clinical data for the patients specified, for the specified FHIR resources, such that it: ○ Supports json resource format for all interactions; ○ Is accurate and without omission based upon the health IT developer's documentation for data return; ○ The request for patient information for population services is not performed on per patient case; and ○ The performance of the FHIR Server matches the expectation based upon the health IT developer documentation. 7. Negative Test: The tester verifies that the app is denied access to patients for an unauthorized request. **Retrieval of Data Elements for a Patient** 8. The tester verifies that the app can retrieve the clinical data associated with the patient as specified at § 170.215(a)(1) and that the clinical data returned:

System Under Test	Test Lab Verification
Provenance Resource 12. The user demonstrates the ability of the Health IT Module to support the provenance for an activity that created a version of a resource as specified in the standard at § 170.215(a)(1).	○ Supports json resource format; and ○ Is accurate and without omission based upon the health IT developer's documentation for data return. 9. The tester verifies that the app can access the patient address and patient telecom from the Health IT Module when accessing the Patient resource and that it is formatted according to the standard specified at § 170.215(a)(1). 10. The tester verifies that the app can retrieve all of the data elements associated with the electronic health record for a single patient from the Health IT Module and that it: ○ Includes all of the data elements for the FHIR resources specified in the standard at § 170.215(a)(2); ○ Includes the patient address and telecom information for the patient; and ○ Is accurate and without omission. **Retrieval of Data Elements for a Population Service** 11. The tester verifies that the app can retrieve all of the data elements associated with the electronic health record for multiple patients from the Health IT Module and for each of the patients it: ○ Includes all of the data elements for the FHIR resources specified in the standard at § 170.215(a)(2); ○ Includes the Patient Address and Telecom information for the patient; and ○ Is accurate and without omission. **Provenance Resource** 12. The tester verifies that the Health IT Module supports the provenance for an activity that created a version of a resource in

System Under Test	Test Lab Verification
	accordance with the standard specified at § 170.215(a)(1) and that, at a minimum, the following data elements are supported: ○ The author's time stamp (Provenance.recorded); and ○ The author and author's organization (Provenance.agent.actor).

Paragraph (g)(10)(ii) – Search Request (Argonaut Profile Conformance – Search)
Paragraph (g)(10)(iv) – Secure Connection

System Under Test	Test Lab Verification
Argonaut Data Query Server Support 1. The documentation provided in (g)(10)(i) is used to ensure the Health IT Module server data query support is in accordance with the standard specified at § 170.215(a)(4) Argonaut Data Query Implementation Guide Server. 2. The health IT developer shall identify the mechanism by which the Health IT Module declares its Argonaut Data Query Server capabilities as specified in § 170.215(a)(3) Argonaut Data Query Implementation Guide Version 1. **Response to Argonaut Data Query Requests for a Patient** 3. Using a launch session from section (g)(10)(v)(B), the user demonstrates the ability of the Health IT Module to return all of the data elements associated with each of the required search criteria (e.g. by date, code, category) as specified in § 170.215(a)(4) for each of the FHIR resources specified in § 170.215(a)(2) API Resource Collection in Health (ARCH) Standard Version 1. 4. The user demonstrates the ability of the Health IT Module to return the FHIR resource associated with a patient according to the standard specified in § 170.215(a)(4) for each of the required FHIR	**Argonaut Data Query Server Support** 1. The tester verifies that according to the identified documentation for the Health IT Module resources, the Health IT Module supports the Argonaut Data Query Patient resource profile and at least one additional resource profile from the list of Argonaut Data Query profiles as specified in § 170.215(a)(3) and that the Argonaut Data Query profile(s) supported as part of the FHIR Meta profile attribute (Meta.profile) for each instance. 2. The tester verifies that the Health IT Module accurately provides a Conformance identifying the list of profiles, operations, and search parameters supported in accordance to the standard specified at § 170.215(a)(3) using the mechanism provided by the health IT developer. **Response to Argonaut Data Query Requests** 3. The tester verifies that the Health IT Module can respond to a request for each of the required Argonaut Data Queries as specified in § 170.215(a)(3) and that the patient data returned: ○ Support json resource formats for all Argonaut Data Query interactions; and

System Under Test	Test Lab Verification
resources as specified in § 170.215(a)(2). **Response to Argonaut Data Query Requests for a Population Service** 5. Using the session launched with a user-level scope in section (g)(10)(v)(B), the user demonstrates the ability of the Health IT Module to return the FHIR resource associated with a population (greater than one patient) for each of the required FHIR resources as specified in § 170.215(a)(2). 6. The user demonstrates the ability of the Health IT Module to return the FHIR resource associated with a population (at least 230 patients) for one of the population services in accordance with the standard specified at § 170.215(a)(2).	○ Is accurate and without omission based upon the health IT developer's documentation for data return. 4. The tester verifies that the Health IT Module can respond to a request for a FHIR resource associated with a patient for each of the required FHIR resources as specified at in § 170.215(a)(2) and that the patient data returned: ○ Supports json resource formats for all Argonaut Data Query interactions; and ○ Is accurate and without omission based upon the health IT developer's documentation for data return. **Response to Argonaut Data Query Requests for a Population Service** 5. The tester verifies that the Health IT Module can respond to a request for a FHIR resource associated with a population for each of the required FHIR resources as specified in § 170.215(a)(2) and that the patient data returned: ○ Supports json resource formats for all Argonaut Data Query interactions; ○ The request for patient information for population services is not performed on per patient case; and ○ Is accurate and without omission based upon the health IT developer's documentation for data return. 6. The tester verifies that the Health IT Module can respond to a request for a FHIR resource associated with a population for each of the required FHIR resources as specified in § 170.215(a)(2) and that the patient data returned: ○ Supports json resource formats for all Argonaut Data Query interactions; ○ Is accurate and without omission based upon the health IT

System Under Test	Test Lab Verification
	developer's documentation for data return; and ○ The performance of the FHIR Server matches the expectation based upon the health IT developer documentation.

Paragraph (g)(10)(vii)(A) – Documentation of API

System Under Test	Test Lab Verification
1. The health IT developer supplies documentation describing the API, with the intended audience of developers, and includes at a minimum: ○ API syntax; ○ Function names; ○ Required and optional parameters and their data types; ○ Return variables and their types/structures; and ○ Exceptions and exception handling methods and their returns. 2. The health IT developer supplies accompanying documentation describing the Health IT Module's API implementation requirements, with the intended audience of developers, which must include: ○ The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s). 3. The health IT developer supplies accompanying documentation describing all of the technical requirements and attributes necessary for an application to be registered with an authorized server.	1. The tester verifies that the identified documentation for the Health IT Module's API definition is accurate and without omission and that it matches the version of the software release. 2. The tester verifies that the identified documentation for interfacing with the Health IT Module's API (including both the software components and the configuration) is accurate and without omission and that it matches the version of the software release. 3. The tester verifies that the identified documentation necessary for an application to register with an authorized server is accurate and without omission and that it matches the version of the software release.

Paragraph (g)(10)(vii)(B) – Hyperlink to Documentation

System Under Test	Test Lab Verification
The documentation used to meet paragraph (g)(10)(vii)(A) of this	The tester verifies that the supplied documentation is publicly accessible

System Under Test	Test Lab Verification
section must be available via a publicly accessible hyperlink.	by hyperlink.

Testing tab

Testing Tool

Inferno

Test Tool Documentation

Inferno User's Guide