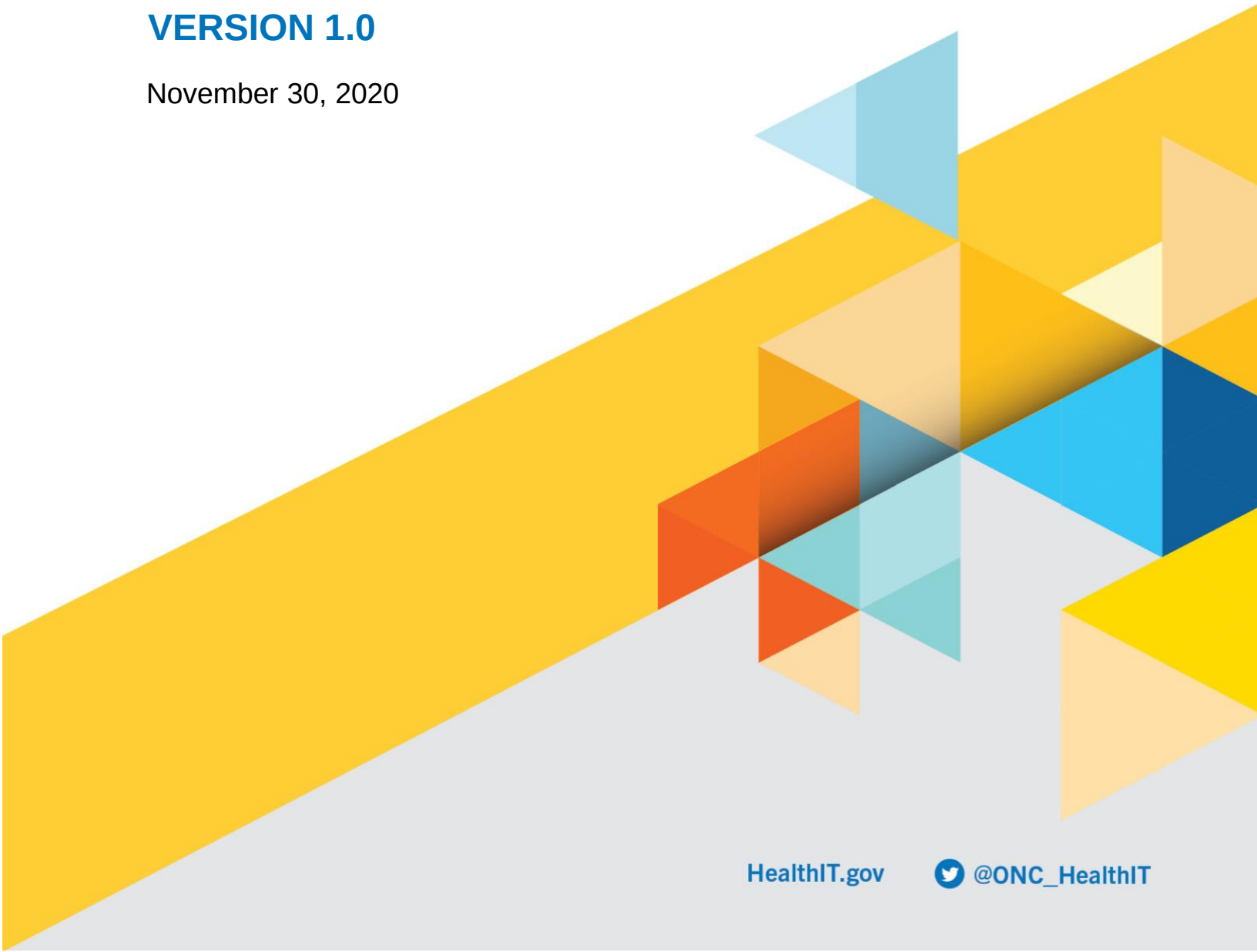
The Office of the National Coordinator for Health Information Technology

Application Programming Interfaces (API) Resource Guide

VERSION 1.0

November 30, 2020



HealthIT.gov @ONC_HealthIT

Table of Contents

Version History

Version #	Description of Change	Version Date
1.0	Initial Publication	November 30, 2020

Foreward

The 21st Century Cures Act (Section 4002) establishes a condition of certification that requires health IT developers to publish application programming interfaces (APIs) that allow "health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law." The Cures Act's API Condition of Certification requirement also states that a developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws."`

As part of the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Cures Act Final Rule), ONC has finalized a certification criterion for APIs for single and multiple patient services at § 170.315(g)(10) to replace the certification criterion at § 170.315(g)(8). Additionally, ONC has finalized API Conditions and Maintenance of Certification requirements at § 170.404 that apply to health IT developers certified to criteria § 170.315(g)(7), § 170.315(g)(8), § 170.315(g)(9), and § 170.315(g)(10).

This document accompanies the Certification Companion Guide (CCG) and Test Procedure for the Standardized API for patient and population services certification criterion finalized at § 170.315(g)(10) and the CCG for API Conditions and Maintenance of Certification requirements finalized at § 170.404.

I. How to Use this Resource Guide

This informative document supplements other public documentation available to help health IT developers certify to the API criteria in the ONC Health IT Certification Program and meet the requirements under the API Conditions and Maintenance of Certification. At the highest level, this document mirrors the organization of paragraphs in the Code of Federal Regulations, including headers for "§ 170.315(g)(10) Standardized API Certification Criterion" (the FHIR-based standardized API), "§ 170.404 Conditions and Maintenance of Certification" (the broader API behavior requirements), and sub-paragraphs. It also contains standalone sections for topics that generate a lot of questions, like "Real World Testing of APIs" and "Standards Version Advancement Process and APIs." Efforts have been made to make this document easily navigable, searchable, and consumable. If you have recommendations to improve this document, please submit an inquiry to the Health IT Feedback and Inquiry Portal.

This document is intended to provide clarifications to assist developers to implement applicable provisions contained in 45 CFR part 170. In developing and implementing APIs and other health IT, developers should remain mindful of the information blocking privisions of the ONC Cures Act Final Rule contained in 45 CFR part 171. This document does not supersede existing statutory or regulatory requirements. The use of the term "Health IT Module(s)" or "certified Health IT Module(s)" in this document refers to Health IT Modules certified through the ONC Health IT Certification Program.

This document encompasses clarifications from the § 170.315(g)(10) Certification Companion Guide (CCG) and § 170.404 CCG. Within each regulation paragraph, there is a section titled "Clarifications Included in [name of CCG]," which includes clarifications from the respective CCG, and "Additional Clarifications to the [name of CCG]," which includes additional clarifications not included in the respective CCG.

II. Helpful Links

These are helpful links for the standardized API criterion and API Conditions and Maintenance of Certification requirements.

A. REFERENCE DOCUMENT LINKS

- § 170.315(g)(10) Certification Companion Guide (CCG)
- § 170.315(g)(10) Test Procedure
- § 170.404 Certification Companion Guide (CCG)

B. TESTING TOOL LINKS

1. Inferno Program Edition

- Inferno Program Edition Online Demonstration Instance
- Inferno Program Edition Installation and Deployment Instructions

C. RULES AND REGULATION LINKS

1. Cures Act Final Rule

- § 170.315(g)(10) Preamble
- § 170.315(g)(10) Regulation text
- § 170.404 Preamble
- § 170.404 Regulation text

2. Interim Final Rule with Comment Period

- § 170.315(g)(10) Preamble
- § 170.315(g)(10) Regulation text
- § 170.404 Preamble
- § 170.404 Regulation text

3. Code of Federal Regulations

- § 170.315(g)(10) Standardized API for patient and population services
- § 170.404 Application Programming Interfaces

D. LINKS TO STANDARDS ADOPTED

- § 170.213: United States Core Data for Interoperability (USCDI)
- § 170.215(a)(1): Health Level 7 (HL7®) Version 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, October 30, 2019

- § 170.215(a)(2): FHIR® US Core Implementation Guide STU V3.1.1
- § 170.215(a)(3): HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0
- § 170.215(a)(4): HL7® FHIR Bulk Data Access (Flat FHIR) (V1.0.0:STU 1)
- § 170.215(b): OpenID Connect Core 1.0 incorporating errata set 1

III. Standardized API Certification Criterion - § 170.315(g)(10)

This section considers the standardized API for patient and population services certification criterion, including all of the content contained in the ONC Cures Act Final Rule API preamble, the IFC API preamble, and the regulation paragraphs in § 170.315(g)(10).

A. TOOLS FOR API TESTING AND CERTIFICATION

1. Inferno Program Edition

The Inferno Program Edition is used for (g)(10) API testing for the ONC Health IT Certification Program.

The Inferno Program Edition is a streamlined testing tool for services seeking to meet the requirements of the Standardized API for Patient and Population Services criterion finalized at § 170.315(g)(10). It is based on the requirements in the ONC Cures Act Final Rule and associated test procedure for § 170.315(g)(10). This tool is used for testing and certification to the § 170.315(g)(10) certification criterion for the ONC Health IT Certification Program.

B. INFORMATION AND CLARIFICATIONS FOR ENTIRE CRITERION

1. Standardized API for Single Patient Services

170.315(g)(10) requires certified Health IT Modules to support API for single patient services.

The § 170.315(g)(10) certification criterion includes requirements for Health IT Modules to support an API for single patient services in § 170.315(g)(10)(i)(A), § 170.315(g)(10)(ii)(A), § 170.315(g)(10)(iii), § 170.315(g)(10)(iv)(A), § 170.315(g)(10)(v)(A), § 170.315(g)(10)(vii), and § 170.315(g)(10)(viii).

2. Standardized API for Multiple Patient Services

170.315(g)(10) requires certified Health IT Modules to support API for multiple patient services.

The § 170.315(g)(10) certification criterion includes requirements for Health IT Modules to support an API for multiple patient services in § 170.315(g)(10)(i)(B), § 170.315(g)(10)(ii)(B), § 170.315(g)(10)(iii), § 170.315(g)(10)(iv)(B), § 170.315(g)(10)(v)(B), § 170.315(g)(10)(vii), and § 170.315(g)(10)(viii).

We have not included a requirement for Bulk FHIR import because the standards for these features are still being developed by industry. Applications or systems seeking to import information formatting according to the HL7® FHIR Bulk Data Access (Flat FHIR) (V1.0.0:STU 1) can use several methods developed by industry, or can refer to Bulk FHIR import methods being defined by HL7 at the HL7 FHIR Bulk Data GitHub page.

3. Applicability

170.315(g)(10) is for all health IT developers who are certifying to the EHR base definition. The API certification criterion finalized in § 170.315(g)(10) was included as part of the EHR Base Definition at § 170.102. While developers of health information technology are not required by the ONC to meet certification requirements, including certification requirements that are included as part of the EHR Base Definition, several federal, state and tribal entities, including Centers for Medicare & Medicaid Services, Centers for Disease Control and Prevention, and other programs reference the ONC Health IT Certification Program and require the use of certified health IT for program participation.

4. Clarifications

Clarifications Included in (g)(10) Certification Companion Guide (CCG):

- On December 31, 2022, the API certification criterion in § 170.315(g)(10) replaces the "application access—data category request" certification criterion (§ 170.315(g)(8)).
- Health IT Modules are not required to support patient-facing API-enabled "read" services for multiple patients for the purposes of this certification criterion.
- The clinical note text included in any of the notes described in the "Clinical Notes Guidance" section of the US Core IG adopted in § 170.215(a)(2) must be represented in a "plain text" form, and it would be unacceptable for the note text to be converted to another file or format (e.g., .docx, PDF) when it is provided as part of an API response. The intent of this policy is to prohibit Health IT Modules from converting clinical notes from a "machine readable" format to a non-"machine readable" format (e.g., PDF). Clinical note text that originates from outside Health IT Modules should be exchanged using its original format. Additionally, "plain text" does not necessarily mean the FHIR "contentType" "text/plain."
- The US Core IG (3.1.1) Profile "StructureDefinition-us-core-patient" element "name.suffix" is required for testing and certification in the ONC Health IT Certification Program to meet the USCDI requirement to support the "Patient Demographics" Data Class: "Suffix" Data Element.
- Either the US Core IG (3.1.1) Profile "StructureDefinition-us-core-patient" element "name.period" or "name.use" is required for testing and certification in the ONC Health IT Certification Program to meet the USCDI requirement to support the "Patient Demographics" Data Class: "Previous Name" Data Element.
- A Health IT Module must support at least one Choice or Reference for US Core IG "must support" elements with multiple Choices or References, respectively.
- A Health IT Module must be conformant to the US Core IG for all Choices and References included in its standardized API, and cannot misrepresent Choices via the standardized API (e.g. a Health IT Module cannot transform "integer" values to "string" values).
- A health IT developer must document which US Core IG Choices and References are supported by their Health IT Module via public technical documentation to meet the requirements in § 170.315(g)(10)(viii) and the transparency conditions in § 170.404(a)(2).

Examples of "must support" in the US Core IG 3.1.1:

In US Core 3.1.1, the profile element Observation.value[x] contains the following Choices: "Quantity, CodeableConcept, string, boolean, integer, Range, Ratio, SampledData, time, dateTime, Period." A Health IT Module must support at least one of these Choices via the (g)(10) standardized API.

In US Core 3.1.1, the profile element Provenance.agent.who contains the following References: "US Core Practitioner Profile | US Core Patient Profile | US Core Organization Profile." A Health IT Module must support at least one of these References via the (g)(10) standardized API.

Additional Clarifications to the (g)(10) CCG:

- The API certification criterion in § 170.315(g)(10) replaces the "application access—data category request" certification criterion (§ 170.315(g)(8)) and supports API-enabled "read" services for single and multiple patients.
- The term "services" includes all § 170.315(g)(10)-related technical capabilities included in a Health IT Module presented for testing and certification. The API-enabled "read" services for single patients is intended to support EHI requests and responses for individual patient records and the API-enabled "read" services for multiple patients is intended to support EHI requests and responses for multiple patients' records.
- The scope of patient cohorts for "population services" can include various groups defined at the discretion of the user of the API-enabled "read" services for multiple patients, including, for example, a group of patients that meet certain disease criteria or fall under a certain insurance plan.
- The information blocking policies established by the ONC Cures Act Final Rule do not compel health care providers to implement Health IT Modules certified to requirements in 170.315(g)(10).
- While there may be slight variation between each instance of a Standardized API for Patient and Population Services Health IT Module implemented by API Information Sources, we believe the standards that form the basis of the § 170.315(g)(10) certification criterion will enable interoperability across implementations.

C. DATA RESPONSE (SINGLE PATIENT) - § 170.315(G)(10)(I)(A)

Regulation text: (i) *Data response.* (A) Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted in § 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.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

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

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

D. DATA RESPONSE (MULTIPLE PATIENTS) - § 170.315(G)(10)(I)(B)

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

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- Health IT Modules may support scopes using either "system/*.read" or a list of "system/[resource].read," where [resource] is the FHIR resource name, to enable the export of multiple patients' data as a group.
- During testing and certification for multiple patient services, Health IT Modules must demonstrate support for "Encounter," "Organization," and "Practitioner" US Core IG FHIR Profiles. Health IT Modules must demonstrate support for "Location" and "PractitionerRole" FHIR resources by providing these resources as part of the multiple patient services response, or by including them as contained resources as part of the multiple patient services response.
- Health IT Modules must support provenance according to the "Basic Provenance Guidance" section of the US Core IG.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

E. SUPPORTED SEARCH OPERATIONS (SINGLE PATIENT) - § 170.315(G)(10)(II)(A)

Regulation text: (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."

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported and are in scope for testing.

Additional Clarifications to the (g)(10) CCG

- The scope of data available in the data responses defined in § 170.315(g)(10)(i) must be supported for searches for multiple patients via the supported search operations finalized in § 170.315(g)(10)(ii).

F. SUPPORTED SEARCH OPERATIONS (MULTIPLE PATIENTS) - § 170.315(G)(10)(II)(B)

Regulation text: (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).

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- *No additional clarifications.*

Additional Clarifications to the (g)(10) CCG

- The scope of data available in the data responses defined in § 170.315(g)(10)(i) must be supported for searches for multiple patients via the supported search operations finalized in § 170.315(g)(10)(ii).
- The HL7 FHIR Bulk Data Access (Flat FHIR) (v1.0.0: STU 1) implementation specification adopted in § 170.215(a)(4) includes mandatory support for the "group-export" "OperationDefinition."

G. APPLICATION REGISTRATION - § 170.315(G)(10)(III)

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

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- Health IT presented for testing and certification must support application registration regardless of the scope of patient search utilized by the application (e.g. single or multiple).

- This certification criterion requires a health IT developer, as finalized in the Condition of Certification requirements, to demonstrate its registration process, but does not require conformance to a standard.
- The third-party application registration process that a health IT developer must meet under this criterion is not a form of review or "vetting" for purposes of this criterion.

Additional Clarifications to the (g)(10) CCG

- We expect that apps executed within an implementer's clinical environment will be registered with an authorization server, but we do not require a health IT developer to demonstrate its registration process for these "provider-facing" apps.
- The requirement that health IT developers must enable an application to register with the § 170.315(g)(10)-certified Health IT Module's authorization server only applies for the purposes of demonstrating technical conformance to the finalized certification criterion and API Condition and Maintenance of Certification requirements. The practices by all parties (including implementers of Health IT Modules) other than developers of certified Health IT Modules are not in scope for this certification criterion nor the associated Condition and Maintenance of Certification requirements.
- Any practices associated with third-party application review or "vetting" by implementers must not violate the information blocking provisions established in the ONC Cures Act Final Rule.

H. SECURE CONNECTION (PATIENT / USER SCOPES) - § 170.315(G)(10)(IV)(A)

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

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- Connections below TLS version 1.2 must be denied.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

I. SECURE CONNECTION (SYSTEM SCOPES) - § 170.315(G)(10)(IV)(B)

Regulation text: (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).

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- Connections below TLS version 1.2 must be denied.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

J. FIRST-TIME AUTHENTICATION / AUTHORIZATION FOR SINGLE PATIENT SERVICES - § 170.315(G)(10)(V)(A)(1)

Regulation text: *(v) Authentication and authorization—(A) Authentication and authorization for patient and user scopes—(1) First time connections—(i)* Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b). (*ii*) A Health IT Module's authorization server must issue a refresh token valid for a period of no less than three months to applications capable of storing a client secret. (*iii*) A Health IT Module's authorization server must issue a refresh token for a period of no less than three months to native applications capable of securing a refresh token.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- Health IT Modules will be explicitly tested for US Core IG operations using authentication and authorization tokens acquired via the process described in the implementation specification adopted in § 170.215(a)(3).
- Only the relevant parts of the OpenID Connect Core 1.0 including errata set 1 adopted in § 170.215(b) that are also included in the implementation specification adopted in § 170.215(a)(3) will be in-scope for testing and certification.
- The “SMART on FHIR Core Capabilities” in § 170.215(a)(3) are explicitly required for testing and certification because these capabilities are otherwise indicated as optional in the implementation specification.
- As part of the “permission-patient” “SMART on FHIR Core Capability” in § 170.215(a)(3), Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their electronic health information(EHI) based on FHIR resource-level scopes. Specifically, this means patients would need to have the ability to authorize access to their EHI at the individual FHIR resource level, from one specific FHIR resource (e.g., “Immunization”) up to all FHIR resources necessary to implement the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2).
- Although Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on FHIR resource-level scopes, Health IT Modules are not prohibited from presenting authorization scopes in a more user-friendly format (e.g. grouping resources under categories, renaming the scopes for easier comprehension by the end-user, using more granular scopes), as long as the ability for patients to authorize applications based on resource-level scopes is available, if requested by the patient.
- Health IT Modules will only be tested for the “Patient Access for Standalone Apps” and “Clinician Access for EHR Launch” scenarios described in the standard adopted at § 170.215(a)(3).
- Since “Encounter” is not currently a USCDI Data Class or Data Element, we will not test Health IT Modules for support for “context-ehr-encounter” or “context-standalone-encounter” SMART on FHIR Core Capabilities described in the standard adopted at § 170.215(a)(3).
- Implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of the information blocking provisions.

- As part of the requirements at § 170.315(g)(10)(v)(A)(1)(iii), health IT developers must publish the method(s) by which their Health IT Modules support the secure issuance of an initial refresh token to native applications according to the technical documentation requirements at § 170.315(g)(10)(viii) and transparency conditions at § 170.404(a)(2).
- Application developer affirmations to health IT developers regarding the ability of their applications to secure a refresh token, a client secret, or both, must be treated in a good faith manner consistent with the provisions established in the openness and pro-competitive conditions at § 170.404(a)(4).
- Health IT developers can determine the method(s) they use to support interactions with native applications and are not required to support all methods third-party application developers seek to use.

Additional Clarifications to the (g)(10) CCG

- We expect implementers of § 170.315(g)(10)-certified Health IT Modules to have the capability of revoking refresh tokens where appropriate.
- Neither § 170.315(g)(10) nor applicable API Condition and Maintenance of Certification requirements require restricting discretion of implementers (health care providers, clinician practices, hospitals, etc.) to set the length of refresh tokens for users of the API including patients and health care providers to align with their institutional policies.
- Implementers of § 170.315(g)(10)-certified Health IT Modules are not prohibited from implementing their § 170.315(g)(10)-certified Health IT Modules in accordance with their organizational security policies and posture, including by instituting policies for re-authentication and re-authorization (e.g., health care providers and/or patients could always be required to re-authenticate and re-authorize after a set number of refresh tokens have been issued).
- Patients are not prohibited from changing the length of refresh tokens to the degree this option is available to them.
- Implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of information blocking provisions applicable to them and that requiring patients to re-authenticate and re-authorize at a high frequency could inhibit patient access and implicate information blocking.

Refresh Tokens for Native Applications

In OAuth 2.0 and the SMART IG, some "native" applications are unable to claim they are "confidential." By definition, these non-confidential "native" applications do not have a client secret to exchange during the client authentication process. However, there are additional methods that non-confidential "native" applications can use to increase refresh token security during the first part of the OAuth 2.0 flow. Methods like Proof Key for Code Exchange (PKCE), the use of application-claimed, private-use Uniform Resource Identifier (URI) schemes as redirect URIs, and utilizing on device secure storage techniques to securely store the refresh token can increase refresh token security during the first part of the OAuth 2.0 flow. Methods like these ensure that an authorization server issues initial access and refresh tokens to the correct corresponding authorized application. The paragraph in § 170.315(g)(10)(v)(A)(1)(iii) requires that Health IT Modules provide support for the issuance of an initial refresh token to "native" applications capable of securing a refresh token. The diagram below explains provides additional explanation.

K. SUBSEQUENT AUTHENTICATION / AUTHORIZATION FOR SINGLE PATIENT SERVICES - § 170.315(G)(10)(V)(A)(2)

Regulation text: (*2*) *Subsequent connections.* (*i*) Access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application. (*ii*) A Health IT Module's authorization server must issue a refresh token valid for a new period of no less than three months to applications capable of storing a client secret.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- *No additional clarifications.*

Additional Clarifications to the (g)(10) CCG

- For subsequent connections, certified Health IT Modules are not required to issue a new refresh token, but must issue a refresh token valid for a new period of no less than three months. Whether the application receives a "new" refresh token is an implementation decision left to the health IT developer, as long as the "refreshed" refresh token is valid for a new period of no less than three months.

Refresh Tokens and Clients "Capable of Storing a Client Secret"

As specified in RFC 6749 (OAuth 2.0) and the HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0 (SMART IG), authorization servers send and receive refresh tokens from their clients in two different parts of an OAuth 2.0 flow. First, after resource owner authorization, the authorization server sends an initial refresh token to the client with the initial access token. Second, when an access token has expired and needs to be refreshed, a client exchanges a refresh token for a new access token and optionally another refresh token, which occurs without user authorization. During both of these exchanges, security is increased (i.e. protecting against leaked refresh tokens) for "confidential" clients that have a client secret used for client authentication. The (g)(10) criterion paragraphs at § 170.315(g)(10)(v)(A)(1)(ii) and § 170.315(g)(10)(v)(A)(2)(ii) require that clients "capable of storing a client secret" must be given refresh tokens during both these parts of the OAuth 2.0 flow. Requiring that such clients be given a refresh token valid for a new period of three months during this second part of the OAuth 2.0 flow enables indefinite persistent access without the need for user re-authorization. The diagram below provides additional explanation.

L. AUTHENTICATION / AUTHORIZATION FOR MULTIPLE PATIENT SERVICES - § 170.315(G)(10)(V)(B)

Regulation text: (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.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- *No additional clarifications.*

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

M. PATIENT AUTHORIZATION REVOCATION - § 170.315(G)(10)(VI)

Regulation text: (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.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- This is a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop.

- Patients are expected to have the ability to revoke an authorized application's access to their EHI at any time.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

N. TOKEN INTROSPECTION - § 170.315(G)(10)(VII)

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

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- Although ONC does not specify a standard for token introspection, ONC encourages industry to coalesce around using a common standard, like OAuth 2.0 Token Introspection (RFC 7662).

Additional Clarifications to the (g)(10) CCG

- No additional clarifications.

O. TECHNICAL API DOCUMENTATION CONTENT - § 170.315(G)(10)(VIII)(A)

Regulation text: (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.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

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

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

P. TECHNICAL API DOCUMENTATION AVAILABILITY - § 170.315(G)(10)(VIII)(B)

Regulation text: (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.

Clarifications Included in (g)(10) Certification Companion Guide (CCG)

- *No additional clarifications.*

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

IV. API Condition and Maintenance of Certification - § 170.404

This section considers the API Condition and Maintenance of Certification requirements, including all the content contained in the ONC Cures Act Final Rule Conditions of Certification API preamble, the ONC Interim Final Rule API preamble, and the regulation paragraphs in § 170.315(g)(10).

A. INFORMATION AND CLARIFICATIONS FOR ENTIRE 170.404 CONDITION AND MAINTENANCE OF CERTIFICATION

1. Applicability

170.404 applies to all health IT developers with health IT certified to 170.315(g)(7) – 170.315(g)(10).

We described several actors in the preamble and regulation text for § 170.404. These actors are defined at § 170.404(c), and include "API Information Source", "API User", and "Certified API Developer". We clarified in preamble and have included in the CCG for § 170.404 that "A person or entity is permitted to serve more than one role for the terms defined in § 170.404(c)" and "Stakeholders meet the definition of a term defined in § 170.404(c) based on the context in which they are acting." Generally, the API Conditions and Maintenance of Certification requirements finalized in § 170.404 apply to Certified API Developers only, which are health IT developers with Health IT Modules certified to § 170.315(g)(7), § 170.315(g)(8), § 170.315(g)(9) and/or § 170.315(g)(10). API Users and API Information Sources, unless they are also acting as a Certified API Developer, are not required to conform to § 170.315(g)(10) or abide by the requirements in § 170.404. The ONC Health IT Certification Program does not have certification criteria for patient-facing applications developed by API Users.

2. Certified APIs and HIPAA Privacy Rule

Certified API Developers must publish Service Base URLs for patient access.

Certified API Developers are required to publish Service Base URLs (§ 170.404(b)) that can be used by patients to exercise their HIPAA Privacy Rule right of access. Additionally, the Standardized API for Patient and Population Services can be used by entities to share treatment, payment, and health care operations information with other authorized parties. The Office of Civil Rights created a page titled "The access right, health apps, & APIs" which explains some of these clarifications in context of APIs.

3. Clarifications

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- The Conditions and Maintenance of Certification requirements only apply to practices of Certified API Developers with respect to the capabilities included in § 170.315(g)(7) through (10).

Additional Clarifications to the (g)(10) CCG

- Regarding the recommendation by commenters that the scope of "all data elements" include the Data Elements of the standard adopted in § 170.213 and FHIR resources referenced by the implementation specification adopted in § 170.215(a)(2), we note that both the standard and implementation specification are included in the interpretation of "all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws" above. We note that this specific interpretation does not extend beyond the API Condition and Maintenance of Certification requirements finalized in § 170.404 and cannot be inferred to reduce the scope or applicability of other Cures Act Conditions of Certification or the information blocking provisions of the ONC Cures Act Final Rule, which include a larger scope of data.

B. API CONDITION OF CERTIFICATION GENERAL REQUIREMENTS - § 170.404(A)(1)

Regulation text: (a) *Condition of certification requirements*—(1) *General.* A Certified API Developer must publish APIs and allow electronic health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- The data required and that must be supported to demonstrate conformance to the final § 170.315(g)(10) certification criterion (including all of its associated standards and implementation specifications) constitutes "all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws."

Additional Clarifications to the (g)(10) CCG

- No additional clarifications.

C. API TRANSPARENCY CONDITIONS - § 170.404(A)(2)

Regulation text: (2) *Transparency conditions*—(i) *Complete business and technical documentation.* A Certified API Developer must publish complete business and technical documentation, including the documentation described in paragraph (a)(2)(ii) of this section, via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. (ii) *Terms and conditions*—(A) *Material information.* A Certified API Developer must publish all terms and conditions for its certified API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be: (*1*) Needed to develop software applications to interact with the certified API technology; (*2*) Needed to distribute, deploy, and enable the use of software applications in production environments that use the certified API technology; (*3*) Needed to use software applications, including to access, exchange, and use electronic health information by means of the certified API technology; (*4*) Needed to use any electronic health information obtained by means of the certified API technology; (*5*) Used to verify the authenticity of API Users; and (*6*) Used to register software applications. (B) *API fees.* Any and all fees charged by a

Certified API Developer for the use of its certified API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to: (*1*) The persons or classes of persons to whom the fee applies; (*2*) The circumstances in which the fee applies; and (*3*) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- This provision of the Condition of Certification requirements does not prohibit additional content or limit the type of content a Certified API Developer may include in its terms and conditions. A Certified API Developer would be permitted to include consumer protections in its terms and conditions documentation.
- As part of the requirements at § 170.315(g)(10)(v)(A)(1)(iii), health IT developers must publish the method(s) by which their Health IT Modules support the secure issuance of an initial refresh token to native applications according to the technical documentation requirements at § 170.315(g)(10)(viii) and transparency conditions at § 170.404(a)(2).

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

D. API FEES CONDITIONS - GENERAL CONDITIONS - § 170.404(A)(3)(I)

Regulation text: (3) *Fees conditions*—(i) *General conditions*—(A) *All fees.* All fees related to certified API technology not otherwise permitted by this section are prohibited from being imposed by a Certified API Developer. The permitted fees in paragraphs (a)(3)(ii) and (iv) of this section may include fees that result in a reasonable profit margin in accordance with § 171.302. (B) *Permitted fees requirements.* For all permitted fees, a Certified API Developer must: (*1*) Ensure that such fees are based on objective and verifiable criteria that are uniformly applied to all similarly situated API Information Sources and API Users; (*2*) Ensure that such fees imposed on API Information Sources are reasonably related to the Certified API Developer's costs to supply certified API technology to, and if applicable, support certified API technology for, API Information Sources; (*3*) Ensure that such fees to supply and, if applicable, support certified API technology are reasonably allocated among all similarly situated API Information Sources; and (*4*) Ensure that such fees are not based on whether API Information Sources or API Users are competitors, potential competitors, or will be using the certified API technology in a way that facilitates competition with the Certified API Developer. (C) *Prohibited fees.* A Certified API Developer is prohibited from charging fees for the following: (*1*) Costs associated with intangible assets other than actual development or acquisition costs of such assets; (*2*) Opportunity costs unrelated to the access, exchange, or use of electronic health information; and (*3*) The permitted fees in this section cannot include any costs that led to the creation of intellectual property if the actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property. (D) *Record-keeping requirements.* A Certified API Developer must keep for inspection detailed records of any fees charged with respect to the certified API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- Certified API Developers and API Users have the ability to collaborate and form relationships, so long as these relationships do not conflict with any of the provisions of the ONC Cures Act Final Rule or other applicable federal and state laws and regulations.
- While the permitted fees set the boundaries for the fees Certified API Developers are permitted to charge and to whom those permitted fees can be charged, they do not prohibit who may pay the Certified API Developer's permitted fee. In other words, these conditions limit the party from which a Certified API Developer may require payment, but they do not speak to who may pay the fee.
- Fees charged for "value-added services" can arise between an API Information Source and Certified API Developer or API User.
- Our goal with the requirement that fees be "objective and verifiable" is to require Certified API Developers to apply fee criteria that, among other things, will lead the Certified API Developer to come to the same conclusion with respect to the permitted fee's amount each time it administers a fee to an API Information Source or API User. Accordingly, the fee cannot be based on the Certified API Developer's subjective judgment or discretion.
- Non-exhaustive examples of fees for services that Certified API Developers would be prohibited from charging:
  - Any fee for access to the documentation that a Certified API Developer is required to publish or make available under this Condition of Certification requirement.
  - Any fee for access to other types of documentation or information that a software developer may reasonably require to make effective use of certified API technology for any legally permissible purpose.
  - Any fee in connection with any services that would be essential to a developer or other person's ability to develop and commercially distribute production-ready applications that use certified API technology. These services could include, for example, access to "test environments" and other resources that an application developer would need to efficiently design and develop apps. The services could also include access to distribution channels if they are necessary to deploy production-ready software and to production resources, such as the information needed to connect to certified API technology (e.g., service base URLs) or the ability to dynamically register with an authorization server.
- Fees for requirements beyond what a Certified API Developer considers necessary to successfully deploy applications in production are considered supplemental to the development, testing, and deployment of software applications that interact with certified API technology, and can be classified as permitted fees for value-added services as finalized in § 170.404(a)(3)(iv).
- The API Condition and Maintenance of Certification covers a narrower scope of potential fees than the information blocking section. The fees in this Condition and Maintenance of Certification are specific to certified API technology while the fees discussed in the information blocking section of the ONC Cures Act Final Rule relate to the access, exchange, or use of EHI regardless of the particular technology used.

Additional Clarifications to the (g)(10) CCG

- A requirement in § 170.404(a)(3)(i)(A) states that permitted fees in paragraphs § 170.404(a)(3)(ii) and § 170.404(a)(3)(iv) may include fees that result in a reasonable profit margin in accordance with the information blocking Fees Exception finalized in § 171.302.
- Any fee that is not covered by an exception would be suspect under the information blocking provisions established in the ONC Cures Act Final Rule, and would equally not be permitted by this API Condition of Certification requirement.
- Health IT developers are permitted to offer discounts to customers, as long as the discounted fees do not constitute information blocking and otherwise conform to ONC Cures Act Final Rule requirements as well as all other applicable laws.

E. API FEES – PERMITTED FEE (DEVELOPMENT, DEPLOYMENT, UPGRADES) - § 170.404(A)(3)(II)

Regulation text: (ii) *Permitted fee—development, deployment, and upgrades.* A Certified API Developer is permitted to charge fees to an API Information Source to recover the costs reasonably incurred by the Certified API Developer to develop, deploy, and upgrade certified API technology.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- The nature of the costs charged under § 170.404(a)(3)(ii) depends on the scope of the work to be undertaken by a Certified API Developer (i.e., how much or how little labor an API Information Source requires of the Certified API Developer to deploy and upgrade the certified API technology).
- Regarding the "development, deployment, and upgrades" described in § 170.404(a)(3)(ii), while we understand that there is overlap between features of the certified API technology and the "broader EHR product," we refer specifically to development, deployment, and upgrades made to "certified API technology" as defined in § 170.404(c). Namely, development, deployment, and upgrades made to the capabilities of certified Health IT Modules that fulfill the API-focused certification criteria adopted at § 170.315(g)(7) through (10).
- Regarding the use of the term "developing" in § 170.404(a)(3)(ii), fees for "developing" certified API technology comprise the Certified API Developer's costs of designing, developing, and testing certified API technology. Fees for developing certified API technology must not include the Certified API Developer's costs of updating the non-API related capabilities of the Certified API Developer's existing Health IT Modules, including its databases, as part of its development of the certified API technology. These costs are typically connected to past business decisions made by the Certified API Developer and typically arise due to Health IT Modules being designed or implemented in nonstandard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI.

- Regarding the use of the term "deploying" in § 170.404(a)(3)(ii), a Certified API Developer's fees for "deploying" certified API technology comprise the Certified API Developer's costs of operationalizing certified API technology in a production environment. Such fees include, but are not limited to, standing up hosting infrastructure, software installation and configuration, and the creation and maintenance of API Information Source administrative functions. Fees for "deploying" certified API technology do not include the costs associated with managing the traffic of API calls that are used to access the certified API technology, which a Certified API Developer can only recover under the permitted fee for usage support costs (§ 170.404(a)(3)(iii)). We emphasize that for the purpose of this Condition of Certification, we consider that certified API technology is "deployed" by the customer—the API Information Source—that purchased or licensed it.
- Regarding the use of the term "upgrading" in § 170.404(a)(3)(ii), a Certified API Developer's fees for "upgrading" certified API technology comprise the Certified API Developer's costs of supplying an API Information Source with an updated version of certified API technology. Such costs would include the costs required to bring certified API technology into conformity with new requirements of the Program, upgrades to implement general software updates (not otherwise covered by development fees or under warranty), or developing and releasing newer versions of the certified API technology at the request of an API Information Source. The nature of the costs that can be charged under this category of permitted fees depends on the scope of the work undertaken by a Certified API Developer (i.e., how much or how little labor an API Information Source requires of the Certified API Developer to upgrade the certified API technology being supplied from one version or set of functions to the next).
- Should API Users generate revenue from the use of their apps, any fee an API Information Source may impose would not be in scope for this Condition and Maintenance of Certification, but could be subject to the information blocking provisions of the ONC Cures Act Final Rule. Accordingly, we emphasize that such stakeholders should take care to ensure they are compliant with the information blocking provisions in the ONC Cures Act Final Rule and other Federal and State laws and regulations that may prohibit or limit certain types of relationships or remuneration.

Additional Clarifications to the (g)(10) CCG

- Should API Users stand to generate revenue from the use of their apps, any fee an API Information Source may impose would not be in scope for this Condition of Certification but would be subject to information blocking provisions established by the ONC Cures Act Final Rule if the API Information Source is a "covered actor" for purposes of information blocking. Accordingly, we emphasize that such stakeholders should take care to ensure they do not engage in information blocking and are compliant with other Federal and State laws and regulations that may prohibit or limit certain types of relationships involving remuneration.

F. API FEES – PERMITTED FEE (RECOVERING API USAGE COSTS) - § 170.404(A)(3)(III)

Regulation text: (iii) *Permitted fee—recovering API usage costs.* A Certified API Developer is permitted to charge fees to an API Information Source related to the use of certified API technology.

The fees must be limited to the recovery of incremental costs reasonably incurred by the Certified API Developer when it hosts certified API technology on behalf of the API Information Source.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- "Usage-based" fees are fees imposed by a Certified API Developer to recover costs typically incurred for supporting API interactions at increasing volumes and scale within established service levels. That is, "usage-based" fees recover costs incurred by a Certified API Developer due to the actual use of the certified API technology once it has been deployed (e.g., costs to support a higher volume of traffic, data, or number of apps via the certified API technology).
- A Certified API Developer's "incremental costs" comprise the Certified API Developer's costs that are directly attributable to supporting API interactions at increasing volumes and scale within established service levels.
- A Certified API Developer should "price" its costs of supporting access to the certified API technology by reference to the additional costs that the Certified API Developer would incur in supporting certain volumes of API use.
- Usage fees for certified API technology will only apply when the Certified API Developer acts on behalf of the API Information Source to deploy its certified API technology. In scenarios where the API Information Source, such as a large hospital system, assumes full responsibility for the technical infrastructure necessary to deploy and host the certified API technology it has acquired, the volume and scale of its usage would be the API Information Source's sole responsibility, and a Certified API Developer would not be permitted to charge usage-based fees.
- The costs recovered under "usage-based" fees can only reflect "post-deployment" costs. As such, "usage-based" fees cannot include any costs necessary to prepare and "get the certified API technology up, running, and ready for use," which are costs that must be recovered as part of the deployment services delivered by the Certified API Developer if permitted under § 170.404(a)(3)(ii).
- We clarify that API usage fees related to API "read" services for multiple patients would be calculated using a similar methodology to calculate API usage fees related to API "read" services for single patients. These "usage-based" fees are fees imposed by a Certified API Developer to recover the costs typically incurred to support API interactions for API "read" services for multiple patients once these services have been deployed. This could include, but not be limited to, costs to support a higher volume of traffic, data, or number of apps via the certified API technology (which could include higher costs for hardware, including server space).

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

G. API FEES – PERMITTED FEE (VALUE-ADDED SERVICES) - § 170.404(A)(3)(IV)

Regulation text: (iv) *Permitted fee—value-added services.* A Certified API Developer is permitted to charge fees to an API User for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- We clarify that the value-added services need to be provided in connection with and supplemental to the development, testing, and deployment of production-ready software applications that interact with certified API technology. A fee is permitted if it relates to a service that a software developer can elect to purchase from a Certified API Developer, but is not required to purchase in order to develop and deploy production-ready apps for certified API technology.
- We note that examples used to illustrate when a fee would or would not qualify as a "value-added service," such as app store listing, are demonstrative, but not required unless otherwise noted in the regulation text.
- We permit fees for services associated with the listing and promotion of apps beyond basic application placement so long as the Certified API Developer ensures that basic access and listing in the app store is provided free of charge (if an application developer depended on such listing to efficiently and effectively develop and deploy production-ready apps for use with certified API technology).
- To the degree that a health IT developer offers value-added services associated with certified API technology, the Condition of Certification covers its practices related to certified API technology only. Conversely, this Condition of Certification would not apply to any practices that do not involve certified API technology.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

H. API OPENNESS AND PRO-COMPETITIVE CONDITIONS - § 170.404(A)(4)

Regulation text: (4) *Openness and pro-competitive conditions; general condition.* A Certified API Developer must grant an API Information Source the independent ability to permit an API User to interact with the certified API technology deployed by the API Information Source. (*i*) *Non-discrimination.* (A) A Certified API Developer must provide certified API technology to an API Information Source on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship. (B) The terms on which a Certified API Developer provides certified API technology must be based on objective and verifiable criteria that are uniformly applied to all substantially similar or similarly situated classes of persons and requests. (C) A Certified API Developer must not offer different terms or services based on: (*1*) Whether a competitive relationship exists or would be created; (*2*) The revenue or other value that another party may receive from using the API technology. (ii) *Rights to access and use certified API technology—*

(A) *Rights that must be granted.* A Certified API Developer must have and, upon request, must grant to API Information Sources and API Users all rights that may be reasonably necessary to: (*1*) Access and use the Certified API Developer's certified API technology in a production environment; (*2*) Develop products and services that are designed to interact with the Certified API Developer's certified API technology; and (*3*) Market, offer, and distribute products and services associated with the Certified API Developer's certified API technology. (B) *Prohibited conduct.* A Certified API Developer is prohibited from conditioning the receipt of the rights described in paragraph (a)(4)(ii)(A) of this section on: (*1*) Receiving a fee, including but not limited to a license fee, royalty, or revenue-sharing arrangement; (*2*) Agreeing to not compete with the Certified API Developer in any product, service, or market; (*3*) Agreeing to deal exclusively with the Certified API Developer in any product, service, or market; (*4*) Obtaining additional licenses, products, or services that are not related to or can be unbundled from the certified API technology; (*5*) Licensing, granting, assigning, or transferring any intellectual property to the Certified API Developer; (*6*) Meeting any Certified API Developer-specific testing or certification requirements; and (*7*) Providing the Certified API Developer or its technology with reciprocal access to application data. (iii) *Service and support obligations.* A Certified API Developer must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of certified API technology by API Information Sources and API Users in production environments. (A) *Changes and updates to* certified *API technology.* A Certified API Developer must make reasonable efforts to maintain the compatibility of its certified API technology and to otherwise avoid disrupting the use of certified API technology in production environments. (B) *Changes to terms and conditions.* Except as exigent circumstances require, prior to making changes to its certified API technology or to the terms and conditions thereof, a Certified API Developer must provide notice and a reasonable opportunity for API Information Sources and API Users to update their applications to preserve compatibility with certified API technology and to comply with applicable terms and conditions.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- For the requirement that a Certified API Developer must provide notice and a reasonable opportunity for API Information Sources and API Users to update their applications to preserve compatibility with certified API technology and to comply with applicable terms and conditions, we note that the notice could include a public notice made available on a website, but also encourage Certified API Developers to contact API Information Source customers and registered API Users (application developers) directly prior to updating business and technical documentation.
- For third-party applications chosen by individuals to facilitate their access to their electronic health information (EHI) held by actors, there would not be a need for a business associate agreement as discussed in the ONC Cures Act Final Rule . There would also generally not be a need for “vetting” on security grounds and such vetting actions otherwise would be an interference.
- We clarify that this rule does not prohibit Certified API Developers from forming business relationships with API Users.
- Application developer affirmations to health IT developers regarding the ability of their applications to secure a refresh token, a client secret, or both, must be treated in a good faith manner consistent with the provisions established in the openness and pro-competitive conditions at § 170.404(a)(4).

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

I. API MAINTENANCE OF CERTIFICATION REQUIREMENTS - § 170.404(B)(1)

Regulation text: (b) *Maintenance of certification requirements*—(1) *Authenticity verification and registration for production use.* The following apply to a Certified API Developer with a Health IT Module certified to the certification criterion adopted in § 170.315(g)(10): (i) *Authenticity verification.* A Certified API Developer is permitted to institute a process to verify the authenticity of API Users so long as such process is objective and the same for all API Users and completed within ten business days of receipt of an API User's request to register their software application for use with the Certified API Developer's Health IT Module certified to § 170.315(g)(10). (ii) *Registration for production use.* A Certified API Developer must register and enable all applications for production use within five business days of completing its verification of an API User's authenticity, pursuant to paragraph (b)(1)(i) of this section.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- This requirement applies to a Certified API Developer with a Health IT Module certified to the certification criterion adopted in § 170.315(g)(10).
- The authenticity verification process finalized in § 170.404(b)(1)(i) is optional, but if instituted, the authenticity verification process must be completed within 10 business days.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

J. API SERVICE BASE URL PUBLICATION - § 170.404(B)(2)

Regulation text: (2) *Service base URL publication.* A Certified API Developer must publish the service base URLs for all Health IT Modules certified to § 170.315(g)(10) that can be used by patients to access their electronic health information. The Certified API Developer must publicly publish the service base URLs: (i) For all of its customers regardless of whether the Health IT Modules certified to § 170.315(g)(10) are centrally managed by the Certified API Developer or locally deployed by an API Information Source; and (ii) In a machine-readable format at no charge.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- Certified API Developers must make available appropriately scoped service base URLs that can be used by patients to access their EHI for Health IT Modules certified to § 170.315(g)(10).
- As discussed in section VIII.C.6.c of the ONC Cures Act Final Rule, API Information Sources who locally manage their FHIR servers without Certified API Developer assistance cannot refuse to provide to Certified API Developers the FHIR service base URL(s) that is/are necessary for patients to use to access their EHI. Equally, pursuant to this Maintenance of Certification requirement, Certified API Developers would be required to publish the FHIR service base URLs they centrally manage on behalf of API Information Sources.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

K. ROLLOUT OF (G)(10)-CERTIFIED APIS - § 170.404(B)(3)

Regulation text: (3) *Rollout of (g)(10)-certified APIs.* A Certified API Developer with certified API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Information Sources with such certified API technology deployed with certified API technology certified to the certification criterion in § 170.315(g)(10) by no later than December 31, 2022.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- A Certified API Developer with certified API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Information Sources with such certified API technology with certified API technology certified to the criterion in § 170.315(g)(10) by no later than December 31, 2022.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

L. COMPLIANCE FOR EXISTING CERTIFIED API TECHNOLOGY - § 170.404(B)(4)

Regulation text: (4) *Compliance for existing certified API technology.* By no later than April 5, 2021, a Certified API Developer with Health IT Module(s) certified to the certification criteria in § 170.315(g)(7), (8), or (9) must comply with paragraph (a) of this section, including revisions to their existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- By no later than April 5, 2021, a Certified API Developer with Health IT Module(s) certified to the certification criteria in § 170.315(g)(7), (8), or (9) must comply with § 170.404(a), including revisions to its existing business and technical API documentation and make such documentation available via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

M. DEFINITIONS - § 170.404(C)

Regulation text: (c) *Definitions.* The following definitions apply to this section: *API Information Source* means an organization that deploys certified API technology created by a "Certified API Developer;" *API User* means a person or entity that creates or uses software applications that interact with the "certified API technology" developed by a "Certified API Developer" and deployed by an "API

Information Source;" *Certified API Developer* means a health IT developer that creates the "certified API technology" that is certified to any of the certification criteria adopted in § 170.315(g)(7) through (10); and *Certified API technology* means the capabilities of Health IT Modules that are certified to any of the API-focused certification criteria adopted in § 170.315(g)(7) through (10).

Clarifications Included in 170.404 Certification Companion Guide (CCG)

- API Users can include, but are not limited to, software developers, patients, health care providers, and payers.
- A person or entity is permitted to serve more than one role for the terms defined in § 170.404(c).
- Stakeholders meet the definition of a term defined in § 170.404(c) based on the context in which they are acting.

Additional Clarifications to the (g)(10) CCG

- *No additional clarifications.*

V. Real World Testing Condition and Maintenance of Certification

Health IT developers are required to test the real-world use of APIs.
The API criteria (§ 170.315(g)(7) through § 170.315(g)(10)) are included under the Real World Testing Condition and Maintenance of Certification requirements of the ONC Cures Act Final Rule in §170.405, which states "A health IT developer with Health IT Module(s) certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (10), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed." More information can be found on the Real World Testing Fact Sheet.

VI. Standards Version Advancement Process (SVAP)

Health IT developers are permitted to test and certify using newer versions of implementation guides that have been approved by the ONC National Coordinator.
ONC has established the voluntary Standards Version Advancement Process (SVAP) to enable health IT developers to incorporate newer versions of approved standards and implementation specifications, as part of the Real World Testing Condition and Maintenance of Certification requirements (§ 170.405) of the 21st Century Cures Act.

Using SVAP, certified health IT developers are permitted to voluntarily use a more advanced version of the standard(s) and implementation specification(s) approved by the National Coordinator, than is adopted in the ONC 2015 Edition Certification Criteria. Currently, this flexibility is limited to standards and implementation specifications that are adopted in the certification criteria required to meet the Real World Testing Condition of Certification, which include § 170.315(b), (c)(1) through (c)(3), (e)(1), (f), (g)(7) through (g)(10), and (h). Health IT developers must ensure that they address standards adopted under SVAP in their Real World Testing plans and results submitted to Authorized Certification Bodies. More information can be found on the SVAP landing page and the SVAP Fact Sheet.