ONC Cures Rule: 2015 Edition API Certification Criteria and API Conditions & Maintenance of Certification

Office of the National Coordinator for Health IT

May 6, 2020

The Office of the National Coordinator for Health Information Technology

Please Note:

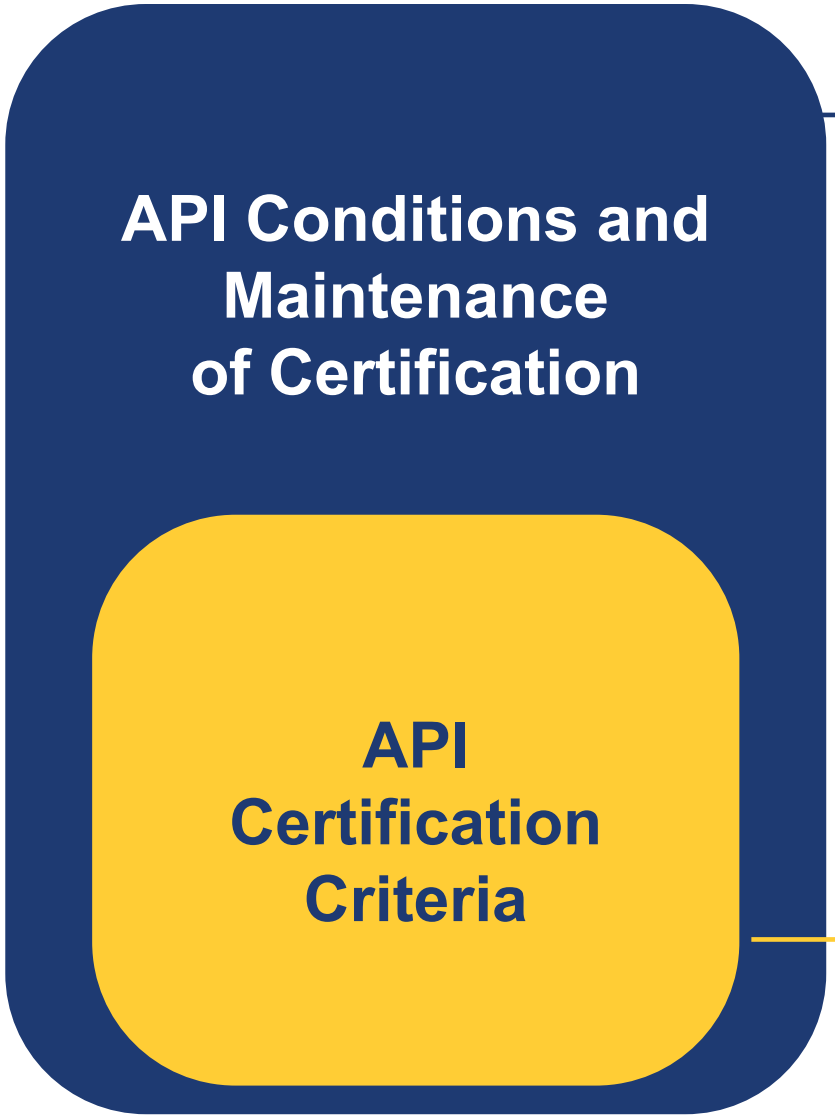
- The materials contained in this presentation are based on the provisions contained in 45 C.F.R. Parts 170 and 171. While every effort has been made to ensure the accuracy of this restatement of those provisions, this presentation is not a legal document. The official program requirements are contained in the relevant laws and regulations. Please note that other Federal, state and local laws may also apply.

- This communication is produced and disseminated at U.S. taxpayer expense.

Purpose of the Final Rule

- ✓ **Patients**: Right of Access to their Chart, Supporting Patient Privacy and Security, the Ability to Shop for Care and Avoid Bankruptcy
- ✓ **Doctors and Hospitals**: Making Patient's Chart Data Requests Easy and Inexpensive, Allowing Choice of Software, Implementation
- ✓ **Patients, Doctors, and Hospitals**: Improving Patient Safety
- ✓ **Health IT Developers**: Minimizing API Development and Maintenance Costs, Protecting Intellectual Property
- ✓ **American Public**: Maximizing Innovation, Transparency in Health Care

Application Programming Interfaces - § 170.404



API Conditions and Maintenance of Certification

Applies to actions and behaviors of certified health IT developers related to the use of their Certified API Technology

API Certification Criteria

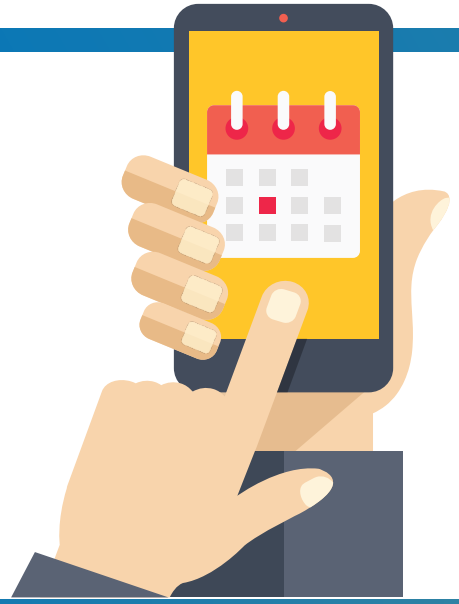
- Certified API criteria (§ 170.315(g)(7) through (10))
- Scope of EHI limited to United States Core Data for Interoperability (USCDI)
- Includes new 2015 Edition Secure, Standards Based API criteria (§ 170.315(g)(10))
  - “read-only” focus
  - HL7® FHIR® Release 4.0.1 as base standard
  - Support for single patient and population services

United States Core Data for Interoperability Standard

The United States Core Data for Interoperability (USCDI) standard will replace the Common Clinical Data Set (CCDS) definition 24 months after publication of this final rule.

USCDI includes the following new required data classes and data elements:

- Provenance
- Clinical Notes
- Pediatric Vital Signs
- Address, Email & Phone Number



Health IT developers need to update their certified health IT to support the USCDI for all certification criteria affected by this change within 24 months after the publication of the final rule.

USCDI - Standards Version Advancement Process

ONC will establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion.

United States Core Data for Interoperability Standard

"Data Element" is the most granular level at which a piece of data is exchanged.

"Data Class" is an aggregation of various Data Elements by a common theme or use case.

DATA CLASS

Allergies and Intolerance

Represents harmful or undesirable physiological response associated with exposure to a substance.

DATA ELEMENT	APPLICABLE STANDARD(S)
Substance (Medication)	• RxNorm, January 6, 2020 Full Release Update • The Unified Code of Units for Measure, Revision 2.1
Substance (Drug Class)	• SNOMED International, Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) U.S. Edition, September 2019 Release
Reaction	• SNOMED International, Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) U.S. Edition, September 2019 Release

https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

2015 Edition API Certification Criteria - § 170.315(g)(10)

Standardized Application Programming Interface (API) for Patient and Population Services

- Established a new application programming interface (API) certification criterion that requires health IT developers to support standardized APIs for single patient and population services.
- Replaces § 170.315(g)(8) in 2015 Edition
- Certification criterion is limited to API-enabled "read" services using the HL7® Fast Healthcare Interoperability Resources (FHIR) Release 4 standard**, namely FHIR Release 4.0.1**
- The use of the FHIR standard and a set of implementation specifications provides known technical requirements against which third-party apps can be developed.

Supports two types of API-enabled services:

» Services for which a **single patient's data** is the focus

» Services for which **multiple patients' data** are the focus

API Criterion – App Registration

Certified API Technology will need to be able to register an application with the certified API technology's authorization server.

Applicable Standard(s): None

API Criterion - Security

Certified API technology will need to establish a secure and trusted connection with apps using Transport Layer Security (TLS) version of 1.2 or higher for all transmissions.

Additionally, certified API technology will be required to perform additional authentication and authorization using specified implementation specifications before an app can be used by a provider for clinical purposes or authorized by a patient to receive their data.

Applicable Standard(s):

- HL7 FHIR US Core Implementation Guide STU 3.1.0
- HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0

API Criterion – Data Response

Single Patient

Certified API technology will need to respond to API requests for data specified in USCDI v1.

Applicable Standard(s):

- FHIR Release 4.0.1
- HL7 FHIR US Core Implementation Guide STU 3.1.0

Additional Context(s):

- Require support for mandatory capabilities in US Core Server Capability Statement for each FHIR profile mapped to USCDI data element.
- Require support for all “mandatory” and “must support” data elements for each FHIR profile mapped to USCDI data element in the standards and implementation specification.

API Criterion – Data Response

Multiple Patient

API technology will need to respond to API requests for multiple patients' data as a group for each data specified in USCDI v1

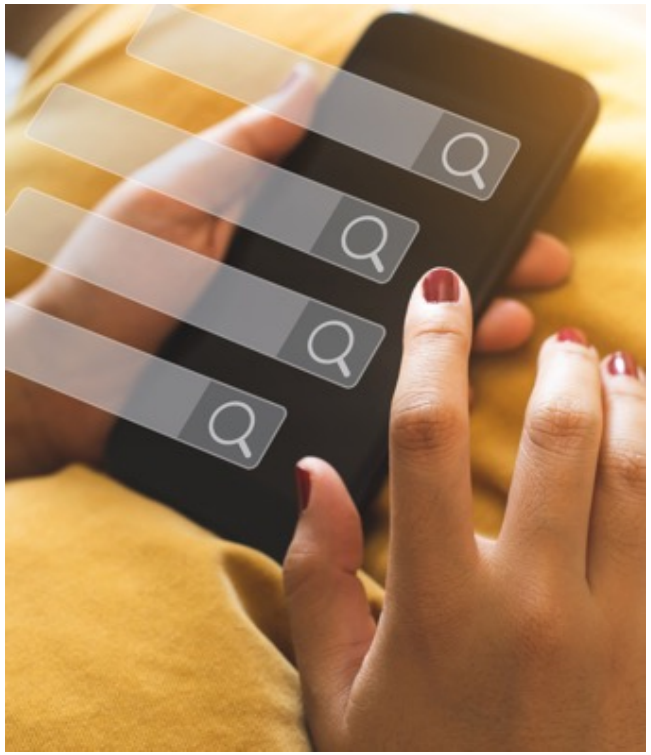
Applicable Standard(s):

- FHIR Release 4.0.1
- HL7 FHIR US Core Implementation Guide STU 3.1.0
- FHIR Bulk Data Access (Flat FHIR) Implementation Guide (v1.0.0: STU 1)

Additional Context(s):

- Require support for group level export operation ("group-export")
- Require support for all "mandatory" and "must support" data elements for each FHIR profile mapped to USCDI data element in the standards and implementation specification.

API Criterion – Search



Single Patient

Certified API technology will need to respond to search requests for single patient data consistent with search criteria included in the US FHIR Core Implementation Guide

Applicable Standard(s):

- HL7 FHIR US Core Implementation Guide STU 3.1.0

Additional Context(s):

- Require support for mandatory capabilities in US Core Server Capability Statement for each FHIR profile mapped to USCDI data elements

API Criterion – Search

Multiple Patient

Certified API technology will need to respond to search requests for multiple patient data consistent with search criteria included in the FHIR Bulk Data Access (Flat FHIR) Implementation Guide

Applicable Standard(s):

- FHIR Bulk Data Access (Flat FHIR) Implementation Guide (v1.0.0: STU 1)

API Criterion - Authentication and Authorization for Patient and User Scopes

When a patient or provider has initiated a request for an app to receive data, the certified API technology must demonstrate that it supports authentication and authorization according to SMART App Launch Implementation Guide and the OpenID Connect standard.

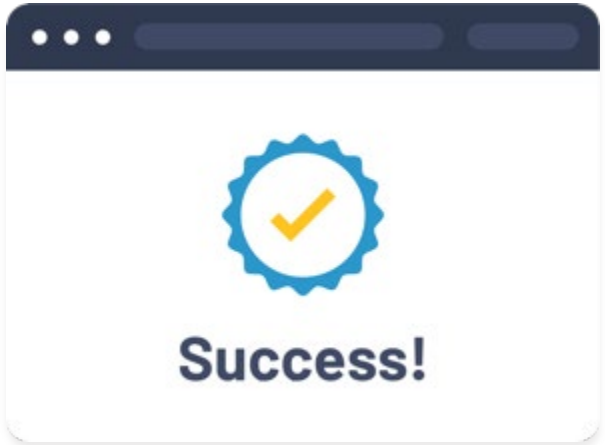
Applicable Standard(s):

- HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0
- OpenID Connect Core 1.0, incorporating errata set 1

Additional Context(s):

- Require mandatory support for “SMART Core Capabilities”
- For any application that is capable of storing a “client secret,” the API technology must be able to issue a refresh token for a period of no less than three months.

API Criterion - Authentication and Authorization for System Scopes



Certified API technology must perform authentication and authorization during the process of granting an app access to patient data in accordance with the “SMART Backend Services Authorization Guide” section of the FHIR Bulk Data Access Implementation Guide.

Applicable Standard(s):

- FHIR Bulk Data Access (Flat FHIR) Implementation Guide (v1.0.0: STU 1)

API Criterion – Additional Required Capabilities

Patient Authorization Revocation

When directed by a patient, API technology's authorization server must be able to revoke an authorized app's access to patient data.

Applicable Standard(s): None

Token Introspection

API technology's authorization server must provide capability to receive and validate tokens it has issued.

Applicable Standard(s): None

Technical Documentation

All technical documentation necessary for developers to design and register software application that interact with certified API technology must be made available via publicly accessible hyperlink.

§170.315(g)(10)Test Procedure and Inferno Program Edition Testing Tool

Test Procedure and Testing Tool for (g)(10)

Test Procedure

- Outlines steps for testing and certification
- https://www.healthit.gov/topic/certification-ehrs/onc-health-it-certification-program-test-method-2020-preview

Paragraph (b)(10)(i) Single patient electronic health information export

System Under Test	Test Lab Verification
Provision Users 1. The health IT developer provides documentation attesting that the Health IT Module can limit users who can perform an electronic health information export for a single patient using one of the following methods: • Grant a set of users the ability to perform the export • Grant system administrator(s) the ability to perform the export **Electronic Health Information Export** 2. The health IT developer provides documentation attesting that a user of the Health IT Module can perform an electronic health information export for a single patient at any time the user chooses without developer assistance, and that the export: • Is created in a timely fashion; and • Includes all the electronic health information for a single patient as described in § 170.315(b)(10)(i)(A); • Creates export files that are electronic and are in a computable format; and • Includes a publicly accessible hyperlink of the export's format.	**Provision Users** 1. The tester verifies via documentation that the Health IT Module can limit users who can perform an electronic health information export for a single patient using one of the following methods: • Grant a set of users the ability to perform the export • Grant system administrator(s) the ability to perform the export **Electronic Health Information Export** 2. The tester verifies via documentation that a user of the Health IT Module can perform an electronic health information export for a single patient at any time the user chooses without developer assistance, and that the export: • Is created in a timely fashion; and • Includes all the electronic health information for a single patient as described in (b)(10)(i)(A); • Creates export files that are electronic and are in a computable format; and • Includes a publicly accessible hyperlink of the export's format.

Testing Tool

- Inferno Program Edition

Summary of (g)(10) Test Procedure: Sections

Application Registration

- Functional requirement for apps to register with authorization server

Secure Connection

- Follow security requirements for US Core IG and SMART IG

Authentication and Authorization for Patient and User Scopes

- Conform with SMART IG

Patient Authorization Revocation

- Functional requirement to enable patients to revoke authorization at any time

Authentication and Authorization for System Scopes

- Conform with Backend Services Authorization section of Bulk IG

Token Introspection

- Functional requirement for authorization server to validate issued tokens

Supported Search Operations

- Conform with US Core IG for single patients; Bulk IG for multiple patients

Data Response

- Conform with US Core IG and USCDI for single patients; Bulk IG, US Core IG, and USCDI for multiple patients

Documentation

- Publish publicly available API documentation

API Conditions of Certification – § 170.404

Application Programming Interfaces (APIs) - § 170.404

ONC has established API Conditions of Certification to address the use of certified API technology and the healthcare ecosystem in which certified API technology will be deployed, including health IT developers' business practice.

SCOPE OF ELECTRONIC HEALTH INFORMATION

The scope of patients' electronic health information that must be accessible via certified API technology is limited to the data specified in the United States Core Data for Interoperability standard (USCDI).

CERTIFICATION

Key Definitions

Certified API technology

Capabilities of health IT that fulfill any of the API-focused certification criteria adopted in the rule

Certified API Developer

Health IT developer that creates the "certified API technology"

API Information Source

Organization that deploys certified API technology

API User

Persons and entities that create or use software applications that interact with "certified API technology"

API Conditions of Certification – High Level Overview

Transparency

This condition clarifies the publication requirements on certified API developers for their business and technical documentation necessary to interact with their certified API technology.

Fees

This condition sets criteria for allowable fees, and boundaries for the fees certified API developers would be permitted to charge for the use of the certified API technology, and to whom those fees could be charged.

Openness and Pro-Competitive

These conditions set business requirements that certified API developers will have to comply with for their certified API technology to promote an open and competitive marketplace.

API Conditions of Certification – Transparency Condition

What documentation is required for certified API developers?

This condition requires certified API developers to publish complete business and technical documentation necessary to interact with the certified API technology.

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.

All the documentation must be accessible via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

API Conditions of Certification – Fees Condition

What fees related to certified API technology are allowed?

Certified API developers are permitted to charge fees to API Information Sources for the development, deployment and upgrade of their API technology.

Certified API developers are permitted to charge API Information Sources towards recovering API usage costs (if applicable).

Certified API developers are permitted to charge API Users for value-added services related to API technology so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software.

API Conditions of Certification – Openness and Pro-Competitive Condition

What are the requirements of certified API developers to promote Open and Competitive Marketplace?

Certified API developers must grant API Information Sources the independent ability to permit API Users to interact with the certified API technology deployed by the API Information Source.

Ensure that the terms associated with certified API technology are non-discriminatory, that the API Information Source and API Users are provided with the necessary rights to access and use the certified API technology, and certain prohibited conduct is expressed to ensure open and competitive environment.

Adhere to specific service and support obligations in order to enable the effective use of certified API technology by API Information Sources and API Users.

API Maintenance of Certification

The API maintenance of certification requirements address ongoing requirements that must be met by certified API developers and their certified API technology

Requirements for Certified API developer related to use of certified API technology adopted in **§ 170.315(g)(10)**

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.

Application Registration

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.

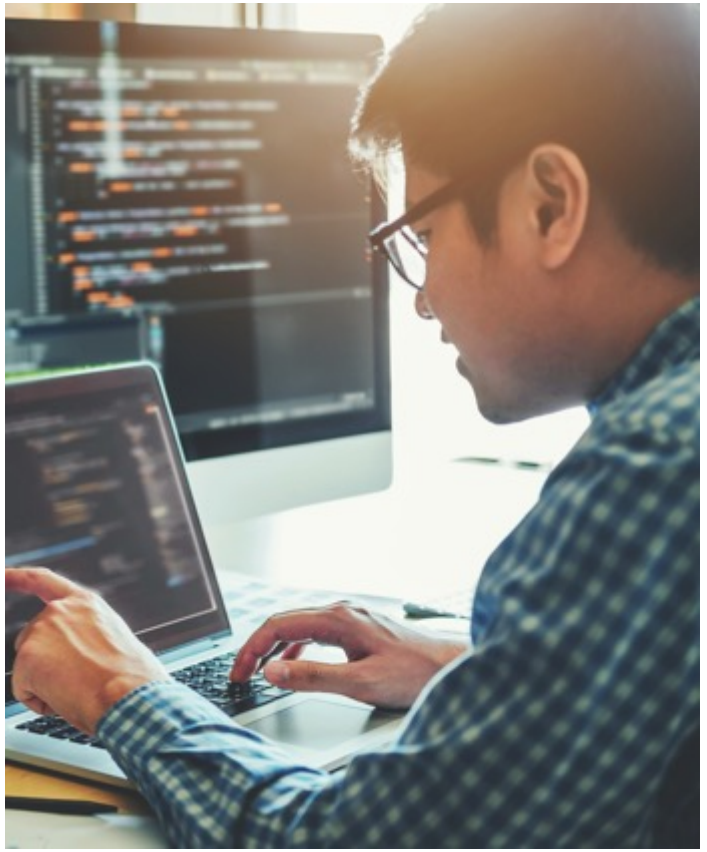
Service Base URL Publication

Certified API developers are required to publish service base URLs for all its customers of certified API technology that can be used by patients to access their electronic health information.

API Maintenance of Certification – Compliance Responsibilities

- Certified API developer with API technology certified to the certification criteria in § 170.315(g)(7), (8), or (9) must comply with the API Conditions of Certification within 6 months of the Cures Act Final Rule's publication date.

- Certified API Developer with certified API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Information Sources API technology certified to the certification criterion in § 170.315(g)(10) by no later than 24 months from the Cures Act Final Rule's publication date.



Please visit www.healthit.gov/curesrule

- View the Final Rule
- Fact Sheets
- Upcoming Webinar Schedule
- Previously recorded webinars
- Additional resources

The Office of the National Coordinator for Health Information Technology

Contact ONC

Add additional call to action or relevant speaker information and contact details.

Phone: 202-690-7151

Health IT Feedback Form: https://www.healthit.gov/form/healthit-feedback-form

Twitter: @onc_healthIT

LinkedIn: Search “Office of the National Coordinator for Health Information Technology”

HealthIT.gov

Subscribe to our weekly eblast at healthit.gov for the latest updates!