Promoting an Open and Transparent API Ecosystem: API Conditions and Maintenance of Certification Requirements for Certified API Developers in the ONC Health IT Certification Program

November 2024

This fact sheet describes the application programming interfaces (APIs) requirements and expectations for Certified API developers participating in the ONC Health IT Certification Program (Certification Program). It serves as a resource to help patients, clinicians, researchers, and other interested parties understand the requirements that apply to developers of certified health IT with products certified to any of the API certification criteria (45 CFR 170.315(g)(7) through (10)).

Key Terms	Definition	Example
Certified API Developer	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)	EHR developer
Certified API technology	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)	EHR
API Information Source	An organization that deploys certified API technology created by a Certified API Developer	Hospital, clinical setting
API User	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	Developers and end-users of a health monitoring app

API Conditions of Certification

The 21st Century Cures Act of 2016 (Public Law 114-225), referred to herein as the Cures Act, requires Certified Health IT developers to publish 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 also states that a Certified Health IT 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."

Several aspects of these statutory requirements for health IT developers go beyond just the technical functionality of the products they present for certification. This fact sheet describes these requirements and provides examples of how Certified Health IT developers can meet them. We strongly encourage Certified Health IT developers and Certified API developers to review the Certification Companion Guides and API Resource Guide.

API Transparency Conditions at § 170.404(a)(2)

What developers must do…

→ Publish and maintain complete business and technical documentation, including terms and conditions for use of their certified API technology, via a publicly accessible link.

How to achieve this…

- → Include the following information in published terms and conditions so apps can use the certified API technology:
  - Fees described in detailed, plain language including to whom they apply, circumstances in which they apply, and amount;
  - Restrictions, limitations, and obligations associated with the use of a Certified API Developer's certified API technology;
  - Requirements for the process of registering an app; and
  - Other similar requirements needed to interact with and use the certified API technology for both API Information Sources and API Users.
- → Provide a publicly accessible link to this information to their ONC-Authorized Certification Body (ACB) to be published on the Certified Health IT Product List (CHPL). Ensure this link continues to be accessible and up to date for the duration of the product's certification to any of the § 170.315(g)(7) through (10) criteria.

API Fees Conditions at § 170.404(a)(3)

What developers must do…

- → Charge fees related to certified API technology in ways that are fair and reasonable and only for activities and services expressly permitted, such as recovering API use costs and value-added services.
- → Clearly and transparently disclose all fees associated with use of their certified API technology, including information on whom the fees apply and, the circumstances under which these fees apply.
- → Maintain detailed records of any fees charged for use of the certified API technology, including the methodology(ies) used to calculate such fees, particularly for variable fees, and the specific costs to which such fees are attributed.

How to achieve this…

- → Include fee information as part of the publicly accessible business documentation. Ensure the potential charges related to the certified API technology are clearly expressed.
- → Ensure fees are objective and can be uniformly applied across all similar API Information Sources and Users. This means that if a fee is charged for one API User, the same fee should be applied to all other API Users in similar circumstances regardless of the API User's size, revenue, or relationship with the Certified API developer.
- → Review the list of prohibited fees outlined at § 170.404(a)(3)(i)(C) to determine whether any fees charged may be interpreted as prohibited. For examples of these prohibited fees, refer to the Cures Act Final Rule preamble at 85 FR 25754.
- → If an API User or API Information Source files a complaint related to potentially prohibited fees to the Certified API developer, ASTP/ONC, or their ONC-Authorized Certification Body (ONC-ACB), collaborate with the reporting individual or entity, and if necessary, with the ONC-ACB, and ASTP/ONC, to evaluate the appropriateness of the fee.

API Openness and Pro-Competitive Conditions at § 170.404(a)(4)

What developers must do…

- → Grant API Information Sources and API Users the necessary rights to access, use, develop, and market applications utilizing the certified API technology without imposing discriminatory or anti-competitive conditions and provide the necessary support for effective ongoing use.

How to achieve this…

- → Allow API Information Sources to independently permit API Users to interact with the certified API technology.
- → Promote competition and access to the certified API technology by providing equal access and services to all users, including third party API developers, under clearly documented, fair, and non-discriminatory terms, regardless of the users' size or location.
- → Provide effective support and services necessary to enable development, deployment, and use of certified API technology by API Information Sources and API Users.
- → Strive to maintain compatibility of API technology as it is changed and updated, by providing advance notice to API Information Sources and API Users of planned changes to certified API technology or the terms and conditions, giving reasonable opportunity for their application to be updated.

API Maintenance of Certification Requirements

Authenticity verification and registration for production use requirements § 170.404(b)(1)

What developers must do…

- → Verify API User authenticity and enable their applications for production use within specified timeframes.

How to achieve this…

- → The API developer must ensure that the application authenticity verification process is objective, uniform for all API Users, and completed within ten business days of receiving an API User's request. The process should be automated where possible to ensure compliance. Once verified, the application must be registered for production use within five business days.
- → Publish and maintain up to date the terms and conditions used to verify the authenticity of API Users.
- → Clearly indicate the process by which an API User can register with certified API technology, document all terms and conditions related to this registration process.
- → Provide and maintain current the contact information on the website and CHPL listing and ensure timely and adequate response to any incoming requests, questions, or complaints.

Service base URL publication requirements at § 170.404(b)(2)

What developers must do…

- → Publish and maintain a publicly accessible FHIR endpoint directory of all customers using the certified API technology.

How to achieve this…

- → Make public, through CHPL, and maintain the endpoints and related organization details in a directory, including organization names, locations, and facility identifiers, in FHIR Endpoint and Organization resource format. These Organization and Endpoint FHIR resources must be collected into a FHIR Bundle.
- → Use the Inferno Service Base URL Test Kit, and SMART App Launch Test Kit (via the user-access brands and endpoints test suite) to help self-assess the conformance of the FHIR Endpoint and Organization resource Bundle.
- → Monitor the uptime of the link to the endpoint lists by downloading the API Service Base URL Availability Report.