The Office of the National Coordinator for Health Information Technology

21ST CENTURY CURES ACT:
INTEROPERABILITY, INFORMATION BLOCKING, AND
THE ONC HEALTH IT CERTIFICATION PROGRAM PROPOSED RULE

Application Programming Interfaces (APIs)
Certification Criterion and Associated Conditions

WHY IS IT IMPORTANT?

The 21st Century Cures Act calls on health IT developers to: Publish APIs and 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.

In order to implement the Cures Act, ONC has proposed a set of certification requirements. These proposed requirements would improve interoperability by focusing on standardized, transparent, and pro-competitive API practices. This would further support the access, exchange, and use of electronic health information (EHI) by patients and providers.

These proposals include:

- A new API certification criterion
- New standards and implementation specifications
- Detailed Conditions and Maintenance of Certification requirements

WHAT ARE THE SPECIFIC PROPOSALS?

NEW API CERTIFICATION CRITERION

ONC has proposed a new certification criterion that would require health IT developers to support API-enabled services for data on a single patient and multiple patients. Prior certification requirements did not include standard API requirements.

What kind of technical requirements would need to be met?

- The use of the Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standard along with a set of Implementation specifications that would provide known technical requirements against which app developers and other innovative services can be built.
- API access to and search capabilities for all data proposed as part of the United States Core Data for Interoperability (USCDI) for a single patient and multiple patients.
- Secure connections that include authentication and authorization capabilities in ways that enable, for example, patients to use an app to access their EHI without needing to log-in each time they use the app.

What kind of security requirements would need to be met?

While the technical documentation and standards necessary for software developers to design apps that interact with a certified API must be made openly available, that does not mean a certified API will be deployed and used without any security. Certified APIs would need to implement the SMART Application Launch Framework Implementation Guide, which is based on the OAuth 2.0 security standard that is widely used in industry. This will enable health care providers to securely deploy and manage APIs consistent with their organizational practices.

- The API technology would need to be able to establish a secure and trusted connection with apps that request data. Additionally, these apps will need to be registered prior to connecting, which means apps would not be able to connect anonymously. App registration provides API technology with the ability to safeguard against malicious apps attempting to gain unauthorized access to patient information through the API. API Technology Suppliers would not be allowed to use app registration as a reason to review specific apps. However, they would be permitted to run a process (no longer than five business days) to first verify the authenticity of an app developer associated with an app seeking to be registered.
- Health care providers retain control over how their workforce and patients authenticate when interacting with the API. For example, a patient would need to use the same credentials (e.g., username and password) they created to access their EHI through other means from their provider (e.g., patient portal) when authorizing an app to similarly access their data.
- Since patients complete the authentication process directly with their health care provider, no app will have access to their specific credentials.
- Patients will be able to limit the data they authorize their apps to access.

API CONDITIONS OF CERTIFICATION

API TECHNOLOGY ROLES

API Technology Supplier Health IT developer that creates API technology presented for certification in the ONC Health IT Certification Program

API Data Provider Health care organization that deploys the API technology

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

ONC has designed API Conditions of Certification that will complement the technical capabilities described in our other proposals, while addressing the broader technology and business landscape in which these API capabilities will be deployed and used.

Note: The API Conditions of Certification only apply to API Technology Suppliers with health IT certified to any API-focused certification criteria.

TRANSPARENCY CONDITIONS

ONC has proposed that API Technology Suppliers make business and technical documentation necessary to interact with their APIs in production freely and publicly accessible.

Note: API Technology Suppliers with API technology already certified would have six months from the final rule's effective date to revise their existing API documentation to come into compliance with the final rule.

What specific documentation is covered under this requirement?

An API Technology Supplier must publish the terms and conditions applicable to its API technology, including those relating to:

- Fees
- Restrictions
- Limitations
- Obligations
- Software application registration process requirements
- Any other material needed to develop, distribute, deploy, and use software applications that interact with the API technology

PERMITTED FEES CONDITIONS

ONC has proposed to adopt specific conditions that would set boundaries for the fees API Technology Suppliers would be permitted to charge and to whom those permitted fees could be charged.

What fees are API Technology Suppliers allowed to charge?

✔ **API Technology Suppliers are permitted to charge API Data Providers:**

- Fees to recover costs reasonably incurred to develop, deploy, and upgrade API technology.
- Fees to recover the incremental costs reasonably incurred to support the use of API technology (excluding the support of a patient's ability to access, exchange, or use their EHI).

✔ **API Technology Suppliers are permitted to charge API Users:**

- Fees for "value-added services" supplied in connection with software that can interact with API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

All other fees not addressed within the "permitted fees" would be prohibited.

OPENNESS AND PRO-COMPETITIVENESS CONDITIONS

ONC has proposed that API Technology Suppliers would have to comply with certain requirements to promote an open and competitive marketplace.

How can an API Technology Supplier meet these pro-competitive conditions?

- Grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.
- Upon request, grant API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment.
- Make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.
- Provide API technology on terms:
  - Based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.
  - That are not based in any part on whether the API User is a competitor, potential competitor, or will be using the data in a way that facilitates competition with the API Technology Supplier.
  - That are not based on the revenue or other value the API User may derive from the access, exchange, or use of the EHI obtained by means of the API technology.

MAINTENANCE OF CERTIFICATION

ONC has proposed specific requirements for API Technology Suppliers to maintain their Health IT Module certification.

What does an API Technology Supplier need to do to maintain its certification?

- Register and enable all applications for production use within one business day of completing its verification of an application developer's authenticity.
- Support the publication of "Service Base URLs" (i.e., FHIR® server endpoints) for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider, and make such information publicly available at no charge.
- An API Technology Supplier with API technology certified to § 170.315(g)(8) must provide all API Data Providers with a (g)(10)-certified API within 24 months of this final rule's effective date.