The Office of the National Coordinator for Health Information Technology

CERTIFICATION

CURES ACT FINAL RULE

Standards-based Application Programming Interface (API) Certification Criterion

ONC has adopted a new secure, standards-based API certification criterion in § 170.315(g)(10) to implement the 21st Century Cures Act's requirement that developers of certified health IT publish APIs that can be used "without special effort." This new certification criterion requires standardized API access for single patient and population services and is limited to API-enabled "read" services using the HL7® Fast Healthcare Interoperability Resources (FHIR®) standard. The FHIR standard, in addition to a set of adopted implementation specifications, provides known and consistent technical requirements for software developers.

What technical requirements does the new certification criterion include?

Base Standard

API technology will be required to support the FHIR Release 4 standard, namely FHIR Release 4.0.1.

App Registration

API technology will need to be able to register software applications ("apps") with the API technology's "authorization server" prior to enabling such apps to interact with the API technology.

Technical Documentation

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

Security

In general, 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, 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.

Authentication and Authorization

When a patient or provider has initiated a request for an app to receive data, the API technology must demonstrate that it supports authentication and authorization according to SMART App Launch Implementation Guide (including "patient" and "user" scopes) and the OpenID Connect standard. Additionally, for any application that is capable of maintaining a "client secret," the API technology must be able to issue a refresh token for a period of no less than three months.

When requesting access to patients' data using "system scopes," 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 Bulk Data Access Implementation Guide.

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.

Data Access and Search

For both single and population services, the API technology will be required to respond to requests for data specified in the USCDI v1 according to the US FHIR Core implementation Guide (US FHIR Core IG) for FHIR Release 4. Additionally, for multiple patients' data, the API technology will need to support "group-level export" according to the Bulk Data Access Implementation Guide. Also, the API technology will need to support all required search criteria specified in US FHIR Core IG for access requests with patient and user scope.

Token Introspection

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