ONC Health IT Developer Roundtable

ASTP/ONC Certification and Testing Division

Agenda

→ **Certification Deadlines**

- Decision Support Interventions
- Standards-based Service Base URLs

→ **API Conformance**

- Standardized API for Patient and Population Services at 45 CFR 170.315(g)(10)
- Conditions and Maintenance of Certification requirements at 45 CFR 170.404

Disclaimers and Public Comment Guidance

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.

By December 31, 2024

- Developers with health IT certified to the clinical decision support certification criterion adopted at § 170.315(a)(9) must:

  - Update their certificate(s) for the decision support interventions certification criterion at § 170.315(b)(11)

  - Provide such certified health IT to customers

- In addition, developers with health IT certified to § 170.315(g)(10) must publish their customers' service base URL information (FHIR Endpoints) according to specific adopted standards referenced in § 170.404(b)(2)

  - NOTE: Certified API Developers have the flexibility to consider using "Organization" and "Endpoint" FHIR® resources profiles, such as the profiles in the User-access Brands and Endpoints specification or Validated Healthcare Directory IG.

ASTP

Considerations for developers certifying to § 170.315(b)(11)

- Definition for Predictive DSI includes three parts, all of which must be true:

  1. Technology that supports decision-making based on algorithms or models that

  2. derive relationships from training data and then

  3. produces an output that results in prediction, classification, recommendation, evaluation, or analysis

- This definition includes both generative and predictive AI that supports decision-making

- Only "supplied" DSIs are subject to ONC requirements (e.g., source attributes and risk management practices)

  - ONC interprets "supplied by" to include interventions authored or developed by the health IT developer as well as interventions authored or developed by other parties that the health IT developer includes as part of its Health IT Module, such as "when entities have contracts specifically covering the enablement and use of such technologies."

  - The concept of "supplied by" means that the Certified Health IT developer has taken on stewardship and accountability for that Predictive DSI for the purposes of the Health IT Module.

  - ONC interprets "as part of its Health IT Module" to mean that the Certified Health IT developer has explicitly offered or provided its customers the technical capability to use or support a Predictive DSI

  - "As part of its Health IT Module" includes any supplied DSIs that are a part of a (b)(11)-certified, CHPL-listed product. This means that if a developer supplies a Predictive DSI as part of a product that is (b)(11)-certified, the developer must include source attributes and other requirements for that Predictive DSI.

ASTP

Clarification regarding DSI source attributes

ONC understands that health IT developers may not have access to complete source attribute information for all decision support interventions (DSIs) they supply, especially for DSIs developed and deployed many years prior. In cases like this and others where source attribute information is not available, a Health IT Module certified to § 170.315(b)(11) should clearly indicate "Unknown" when a source attribute listed is not available for the user to review. While we understand that in some cases the source attributes may not be available, we note that we expect health IT developers to exercise due diligence before making a determination that a source attribute's information is "Unknown." We also note that developers certified to § 170.315(b)(11) are required under § 170.402(b)(4) Assurances Maintenance of Certification, starting January 1, 2025, and on an ongoing basis thereafter, to review and update as necessary source attribute information. Where source attribute information later becomes known, developers would be expected to make such information available to their end users. (9/16/24 clarification, See also 89 FR 1245 for Assurance Condition requirements)

See https://www.healthit.gov/test-method/decision-support-interventions for all DSI clarifications

ASTP

Getting Real About Information Blocking and APIs

ASTP / ONC Blog about Info Blocking and APIs

- Assistant Secretary and National Coordinator Micky Tripathi recently published a blog on info blocking and conformance to API requirements in the ONC Certification Program

- ASTP / ONC priority to ensure that Certified API Developers conform to Program requirements for certified API technology

- Upcoming resources, communications, webinars, and more to clarify and provide additional guidance regarding compliance with Program API requirements

Summary of API Feedback: Part 1

API Documentation and App Developer Feedback

- CHPL information and API documentation out of date
- Service base URLs and organization details not being published or out of date
- No channel for feedback on API documentation and registration

App Registration and App Developer Lockout

- Not enough documentation for app developers to register apps and no support point of contact
- App registration not supported in timely manner
- Delay and unequal treatment of registration requests
- Not allowing app registration without patient request
- API User authenticity verification process may require sharing unnecessary information
- Potentially having to manually register with each provider API
- "Value added services" being used to gatekeep API access, including registration
- Onerous fees, pricing practices, contractual terms, and intellectual property requirements

ASTP

Summary of API Feedback: Part 2

Failure to respond to API access requests

- Not providing written and timely responses to denials for access to EHI
- Requiring extraneous HIPAA Business Associate Agreements as a pre-requisite for patients to have electronic access to their information

App Developer and Patient Experience

- Limited access to sandboxes and synthetic data
- API bandwidth limitations make it challenging for apps to function
- Patient education during app authorization may involve info blocking practices
- Some app authorization menus are difficult to use, lacking features such as "select all" or "de-select all" options

ASTP

Accessing API Documentation and URL Issues

Issues:

- Unresolvable hyperlinks in CHPL
- Service Base URL list does not directly link to a list of customer service base URLs
- API Documentation hyperlink does not directly link to API Documentation
- Links may direct to developer homepage, which requires the user to navigate a website and hinders automation
- Not publishing patient access API service base URLs
- Service base URLs often do not contain healthcare organization details

According to Program requirements, Certified API Developers must:

- Keep their API documentation links up-to-date
- Publish and keep up-to-date service base URL for all customers
- Publish service base URLs and organization details in FHIR bundle format as specified at 45 CFR 170.404(b)(2) by December 31, 2024

The Office of the National Coordinator for
Health Information Technology

API Technical Documentation Issues

Contact Name:	
Contact Email:	
Organization Name:	
Client Name:	
Redirect URL:	
Launch URL:	

Scope(s):
- [ ] launch
- [ ] launch/patient
- [ ] openid
- [ ] fhirUser
- [ ] offline_access

- [ ] patient/Patient.read
- [ ] patient/AllergyIntolerance.read
- [ ] patient/CarePlan.read
- [ ] patient/CareTeam.read
- [ ] patient/Condition.read
- [ ] patient/Device.read
- [ ] patient/DiagnosticReport.read
- [ ] patient/DocumentReference.read
- [ ] patient/Encounter.read
- [ ] patient/Goal.read
- [ ] patient/Immunization.read
- [ ] patient/Location.read
- [ ] patient/Medication.read
- [ ] patient/MedicationRequest.read
- [ ] patient/Observation.read
- [ ] patient/Organization.read
- [ ] patient/Practitioner.read
- [ ] patient/PractitionerRole.read
- [ ] patient/Procedure.read
- [ ] patient/Provenance.read
- [ ] patient/RelatedPerson.read

- [ ] user/Patient.read
- [ ] user/AllergyIntolerance.read
- [ ] user/CarePlan.read
- [ ] user/CareTeam.read
- [ ] user/Condition.read
- [ ] user/Device.read
- [ ] user/DiagnosticReport.read
- [ ] user/DocumentReference.read
- [ ] user/Encounter.read
- [ ] user/Goal.read
- [ ] user/Immunization.read
- [ ] user/Location.read
- [ ] user/Medication.read
- [ ] user/MedicationRequest.read
- [ ] user/Observation.read
- [ ] user/Organization.read
- [ ] user/Practitioner.read
- [ ] user/PractitionerRole.read
- [ ] user/Procedure.read
- [ ] user/Provenance.read
- [ ] user/RelatedPerson.read

Register

Example obtained from ONC SITE page
Refer to Code of Federal Register for complete requirements

Issues:

- Not enough public information to support registration process

- No support contact information

- No ability to provide feedback to developer on registration process

- No ability to provide feedback on developer technical documentation

- API documentation not up-to-date

According to Program requirements, Certified API Developers must:

- Publish and keep up-to-date complete business and technical documentation

- Include in their API technical documentation all information needed to register an app in a production environment, including terms of use and registration process requirements

API Registration Challenges

Issues:

- Third-party app developers required to obtain individual registration and approval for each health system or provider organization.

- Third-party app developers required to complete separate manual questionnaires for each service base URL (i.e., FHIR endpoint).

- Registration is not completed in a timely manner.

Program Requirements:

- API maintenance of certification requirements require Certified API Developers to register apps for production use with their § 170.315(g)(10)-certified Health IT Module. Additionally, it sets a specific timeline for Certified API Developers to process these registration requests.

- Authenticity verification of API Users (optional): Objective process that should be the same for all API Users, completed **within ten business days** of receiving an API User's registration request.

- Registration for production use: Must be done **within five business days** of completing authenticity verification.

ASTP

Non-Standard and Extra Registration Burdens

Issues:

- Implementers are requiring patients to authorize apps through non-standard processes, including out-of-band methods, and requiring patient requests through their healthcare providers for app connections.

- Patients are being forced to create separate logins with data holders, instead of being able to use the same login they have for their patient portal, to connect third-party apps.

Program Requirements:

- The API Condition of certification requirements require Certified API Developers to publish APIs and allow electronic health information from such technology to be accessed, exchanged, and used without special effort.

- A § 170.315(g)(10)-certified Health IT Module must support:

  - Application registration with the Health IT Module's "authorization server."

  - Standardized (according to the SMART App Launch Framework) authentication and authorization during the process of granting access to patient data.

ASTP

Extraneous Pre-requisites before App Registration for Patient Access

Issue: Requiring extraneous HIPAA Business Associate Agreements or business partnerships or agreements as a pre-requisite for registration of apps for patient access to EHI

Example situation: A Certified API Developer requires app developers to sign a HIPAA Business Associate Agreement before registering their apps for patient access for production use.

Program Guidance and Requirements:

Certified API Developers shall not require HIPAA Business Associate Agreements nor business partnerships nor agreements as a pre-requisite for app registration for patient access to their EHI via certified API technology.

ASTP

Misuse of Value-Added Services

Issues:

- "Consumer education" appears as intimidating warning messages that discourage patients from connecting their third-party app.

- In some instances, third-party app developers have the option to pay a fee to become a "known" app and have the warning messages removed for their users.

Program Requirements:

- Certified API Developers are allowed to charge fees for value-added services related to certified API technology, including a reasonable profit margin. However, such services can not be required for the **efficient and effective** development and deployment of production-ready software that interacts with certified API technology.

- The value-added services must be supplemental to the **efficient and effective** development, testing, and deployment of production-ready software applications interacting with certified API technology.

- All fees related to certified API technology not otherwise permitted according to 45 CFR 170.404(a)(3) are prohibited from being imposed by a Certified API Developer.

ASTP

App authorization – interference vs education

Example authorization screen of FHIR Server

Issue: Certified API Developers must avoid information blocking when educating patients about the privacy and security practices of applications.

Example situation: Certified health IT displays a notification to the patient as part of app authorization about whether the app developer's privacy policy and practices meet "best practices" set by the market.

Avoiding Info Blocking by ensuring provided information:

- Focuses on any current privacy and/or security risks posed by the app

- Is factually accurate, unbiased, objective, and not unfair or deceptive.

- Is communicated in a non-discriminatory manner.

App authorization – ease of use features

Inferno ONC Standardized API Demo Server

Please select which scopes you would like to authorize. To select a granular resource scope, first de-select the full resource scope. SMART V1 scopes will automatically be converted to V2 if any granular scopes are selected.

☑ launch/patient
☑ openid
☑ fhirUser
☑ offline_access
☑ patient/Medication.read
☑ patient/AllergyIntolerance.read
☑ patient/CarePlan.read
☑ patient/CareTeam.read
☑ patient/Condition.read
☐ patient/Condition.rs?category=http://hl7.org/fhir/us/core/CodeSystem/condition-category|health-concern
☐ patient/Condition.rs?category=http://terminology.hl7.org/CodeSystem/condition-category|encounter-diagnosis
☐ patient/Condition.rs?category=http://terminology.hl7.org/CodeSystem/condition-category|problem-list-item
☑ patient/Device.read
☑ patient/DiagnosticReport.read
☑ patient/DocumentReference.read
☐ patient/DocumentReference.rs?category=http://hl7.org/fhir/us/core/CodeSystem/us-core-documentreference-category|clinical-note
☑ patient/Encounter.read
☑ patient/Goal.read
☑ patient/Immunization.read
☑ patient/Location.read
☑ patient/MedicationRequest.read
☑ patient/Observation.read
☐ patient/Observation.rs?category=http://hl7.org/fhir/us/core/CodeSystem/us-core-category|sdoh
☐ patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|social-history
☐ patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|laboratory
☐ patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|survey
☐ patient/Observation.rs?category=http://terminology.hl7.org/CodeSystem/observation-category|vital-signs
☑ patient/Organization.read
☑ patient/Patient.read
☑ patient/Practitioner.read
☑ patient/Procedure.read
☑ patient/Provenance.read
☑ patient/PractitionerRole.read

[Authorize]

Issue: FHIR scope authorization interface may be difficult for some patients to use due to lack of certain features (e.g., "select all", "de-select all").

Example situation: Patient wants to authorize all scopes requested by an app. However, the certified API technology by default has no scopes selected. This makes it cumbersome for the patient to authorize all scopes, since each scope must be individually and manually selected.

Consider including in certified API technology: User interface options such as "select all" and "de-select all" for the scope authorization interface.

Example authorization screen from Inferno Reference Server

ASTP

Developer Testing Environment ("Sandboxes")

Issue:
Developers offer limited access to development sandboxes and synthetic information.

Example Situation:
An app developer may want to test their app works correctly with certified API technology before interacting with a production deployment.

Consider including in certified API technology:
Test environment ("developer sandbox") and synthetic information that app developers can use to test their app before interacting with production environment.

ASTP

Program Requirements Refresher

API Technical Requirements

Compliance with Program requirements: API technical requirements – Summary

Application Registration
- Functional requirement for apps to register with authorization server

Secure Connection
- Follow security requirements for US Core IG and SMART App Launch IG

Authentication and Authorization for Patient and User Scopes
- Conform with SMART App Launch IG for standalone and EHR launch
- Enable persistent access via issuance of refresh tokens

Patient Authorization Revocation
- Functional requirement to enable patients to revoke authorization within 1 hour of the request

Authentication and Authorization for System Scopes
- Conform with SMART Backend Services specification

Token Introspection
- authorization server to validate issued tokens in accordance with SMART App Launch IG

Supported Search Operations
- Conform with US Core IG for single patients; Bulk Data Access IG for multiple patients

Data Response
- Respond to requests for a single patient's data and multiple patients' data
- Conform with US Core IG and Bulk Data Access IG, including group export, for data in USCDI

Documentation
- Publish publicly available API documentation

ASTP

Compliance with Program requirements: API technical requirements – Summary

Application Registration

- Functional requirement for apps to register with authorization server

Secure Connection

- Follow security requirements for US Core IG and SMART App Launch IG

Authentication and Authorization for Patient and User Scopes

- Conform with SMART App Launch IG for standalone and EHR launch
- Enable persistent access via issuance of refresh tokens

Patient Authorization Revocation

- Functional requirement to enable patients to revoke authorization within 1 hour of the request

Authentication and Authorization for System Scopes

- Conform with SMART Backend Services specification

Token Introspection

- authorization server to validate issued tokens in accordance with SMART App Launch IG

Supported Search Operations

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

Data Response

- Respond to requests for a single patient's data and multiple patients' data
- Conform with US Core IG and Bulk Data Access IG, including group export, for data in USCDI

Documentation

- Publish publicly available API documentation

ASTP

Compliance with Program requirements:
API technical requirements – App Registration

Application registration - Enable an application to register with the Health IT Module's "authorization server."

- Must demonstrate app registration capability for certification testing

- Must also document app registration process in publicly published API documentation

- App developer affirmations used for registration must be treated in a good faith manner

- (Optional) May have API User authenticity verification process; details at 45 CFR 170.404(b)(1)(i)

- Must register API Users within five business days of completing the optional API User authenticity verification process

ASTP

Compliance with Program requirements:
API technical requirements – Documentation

Both APIs (Single and Multiple Patients)

- **Documentation** – must include complete accompanying documentation that contains details of supported APIs including:
  - *specific technical details* such as API syntax, function names, return variables, and exceptions and exception handling methods
  - *software components and configurations* necessary for an app to successfully interact with the API
  - *registration requirements and attributes* necessary for an app to be registered with a Health IT Module's authorization server

This API documentation must be kept up-to-date at a publicly accessible hyperlink in CHPL!

ASTP

Program Requirements Refresher

API Conditions and Maintenance of Certification

Application Programming Interfaces (APIs) - § 170.404

- API Condition and Maintenance of Certification requirements address Certified API Developers' technical and business practices for Health IT Modules certified to § 170.315(g)(7) through (g)(10)

- Condition of Certification requirements: § 170.404(a)

- Maintenance of Certification requirements: § 170.404(b)

Definitions for terms used in § 170.404

Terms for the actors and systems addressed by the API Conditions and Maintenance of Certification requirements are defined in 45 CFR 170.404(c)

Definitions in § 170.404(c)

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 Condition of Certification: Overview

General

This section establishes that 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, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws

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
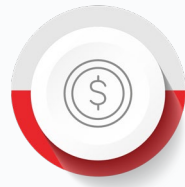
Fees

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 can be charged
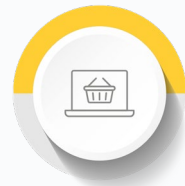
Openness and Pro-Competitive

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

ASTP

API Condition 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

ASTP

API Condition 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

All fees not explicitly permitted are prohibited

ASTP

API Condition of Certification: Openness and Pro-Competitive Condition

What are the requirements of certified API developers to promote an 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

ASTP

API Maintenance of Certification

The API maintenance of certification requirements address additional ongoing requirements that must be met by Certified API Developers

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

ASTP

Current Service Base URL Publication Requirements

Background: Maintenance of certification requirement at § 170.404(b)(2) requiring Certified API Developers to publish, at no charge, the service base URLs (i.e., FHIR endpoints) for all their Health IT Modules certified to § 170.315(g)(10) that can be used by patients to access their electronic health information

Before HTI-1: Publication format was "a machine-readable format"

HTI-1 Update: Standardized publication format and requirement for organization details

- Each Service base URL must be published in FHIR Endpoint resource format
- Organization details (including name, location, and facility identifier) for each service base URL must be published in FHIR Organization resource format
- Endpoint and Organization resources must be collected in FHIR Bundle resource format for publication
- Compliance date of December 31, 2024

Benefit: Having all healthcare organizations serviced by the service base URL accessible and in a standardized format would help app developers easily fetch information to enable patients and other users to access, exchange, and use information (89 FR 1285)

ASTP

Compliance with Program requirements: Conditions and Maintenance of Certification

- Among the many concerns raised is the possibility of **Certified API developers potentially being out of compliance with Conditions and Maintenance of Certification requirements** specific to APIs (45 CFR 170.404) and information blocking (45 CFR 170.401)

- Failure to meet requirements impacts participation in the Certification Program and broader health IT ecosystem. It affects:

  - Trust in Health IT: Reduces confidence in your technology.

  - Technology adoption: When API performance or availability is inconsistent, users become less likely to adopt new technologies. That slows innovation and impacts your product's success.

  - Increased Costs & Inefficiency: nonconformities with the Certification Program will lead to inefficiencies, driving up costs as developers and users spend more time addressing compliance gaps.

  - Patient Outcomes: Ultimately, unreliable APIs and health IT systems create delays in data access, directly affecting patient care. Poor API performance can have real-world consequences for those relying on timely, accurate data.

- Compliance is not just a box to check at the beginning of your journey with the Certification Program, it's foundational to the success of your products, the efficiency of the healthcare system, and the care patients receive

ASTP

Compliance with Program requirements: Information Blocking

- Failure to meet API Conditions and Maintenance of Certification requirements under 45 CFR 170.404, may also indicate information blocking violations under 45 CFR 170.401

- Certified API Developers, as actors subject to information blocking regulations (45 CFR part 171), are engaging in information blocking if they knowingly, or should reasonably know, that their actions (or inactions) are likely to interfere with the access, exchange, or use of EHI, unless the practice is required by law or falls under an established exception

- Our collaboration with the HHS Office of Inspector General (OIG) and the Centers for Medicare & Medicaid Services (CMS) is essential to preventing and addressing information blocking
  - The OIG is ready to investigate potential cases of information blocking. If a health IT developer, health information network, or health information exchange is found guilty, they can face fines of up to $1 million per violation.
  - For healthcare providers, the OIG refers cases to CMS, which applies the appropriate penalties based on the provider's actions.

ASTP

Compliance with Program requirements:
Surveillance and Enforcement

- ASTP remains committed to maintaining the integrity and effectiveness of the Certification Program

- Through ongoing oversight, the Certification Program ensures compliance with its requirements, including the API and Information Blocking Conditions and Maintenance of Certification requirements

- When necessary, enforcement through <u>direct review</u> of certified health IT and their developers, may lead to <u>suspension</u> or <u>termination</u> of certifications

- Particularly serious non-conformities may could also result in the developer being <u>banned</u> from the Certification Program

ASTP

Next Steps and Upcoming Educational Resources

Next Steps and Upcoming Educational Resources

Improved feedback channels

New dedicated section for API-related complaints and inquiries in Health IT Feedback and Inquiry Portal

"Do's and Don'ts" of Certified API Technology and Developers

Resource for Certified API Developers containing guidance about good and bad practices to maintain compliance with Program requirements

API Conditions and Maintenance of Certification Fact Sheet

Resource summarizing Certified API Developer obligations for condition and maintenance of Certification

API Documentation Resource / Checklist

Resource containing guidance and expectations for the contents of Certified API Developer API documentation

ASTP

HHS | ASTP

Reach out via phone or web

📱 202-690-7151

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

Stay connected, follow us on social media channels

𝕏 @onc_healthIT

in Office of the National Coordinator for Health Information Technology

▶ https://www.youtube.com/user/HHSONC

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