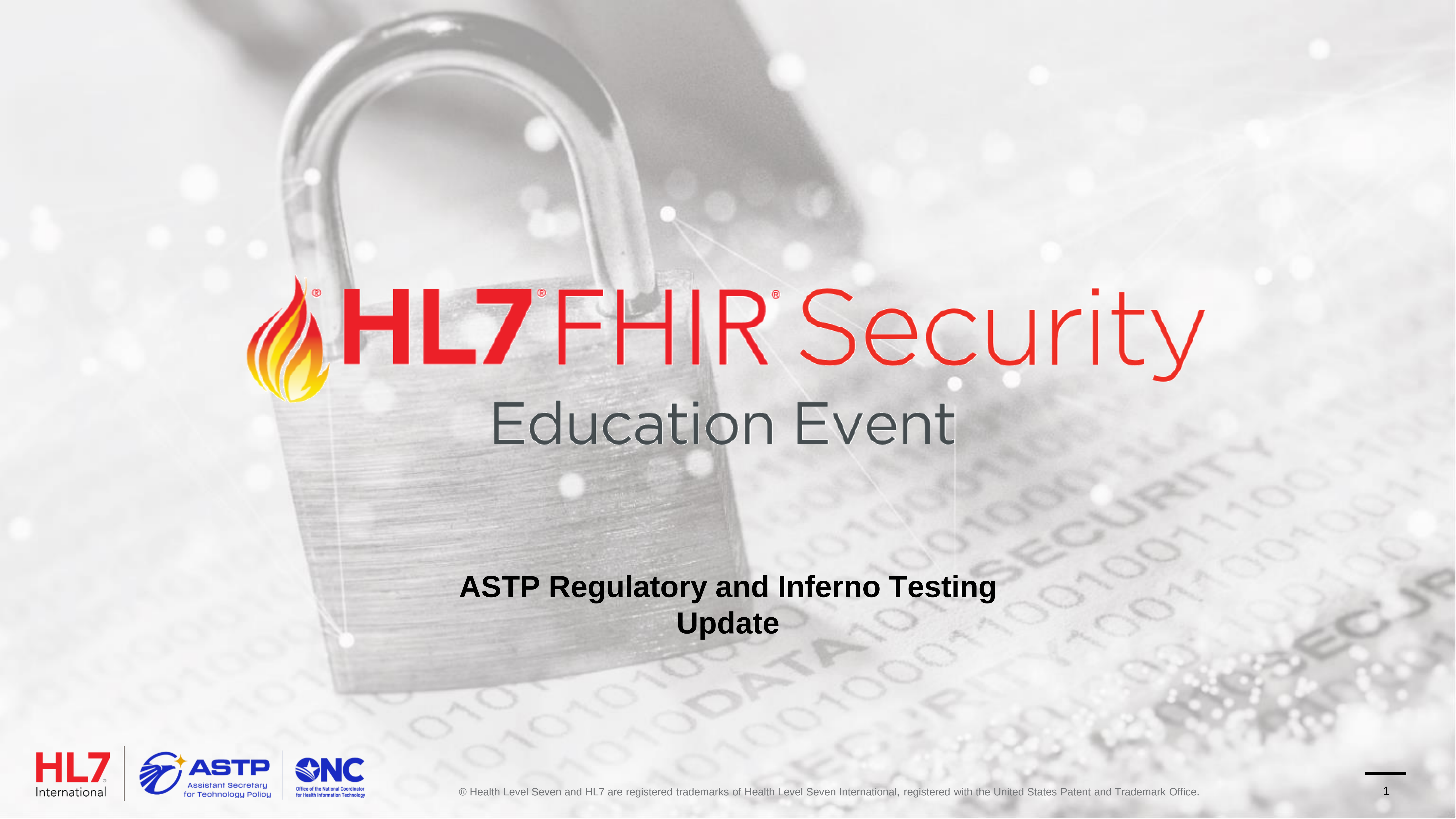


HL7® FHIR® Security

Education Event

ASTP Regulatory and Inferno Testing Update

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

® Health Level Seven and HL7 are registered trademarks of Health Level Seven International, registered with the United States Patent and Trademark Office.

Introductions

- Scott Bohon
  - Information Technology Specialist, ASTP Tools & Testing Branch
- John Bender
  - Public health analyst, ASTP Tools & Testing Branch
- Keith Carlson
  - IT Cybersecurity Specialist, ASTP Tools & Testing Branch
  - FHIR R4 Certified
  - Subject Matter Expert for Privacy and Security criteria and API criteria in the ONC Certification Program

NOTE: Assistant Secretary for Technology Policy/Office of the National Coordinator for Health IT (hereafter ASTP)

Disclaimers and Public Comment Guidance

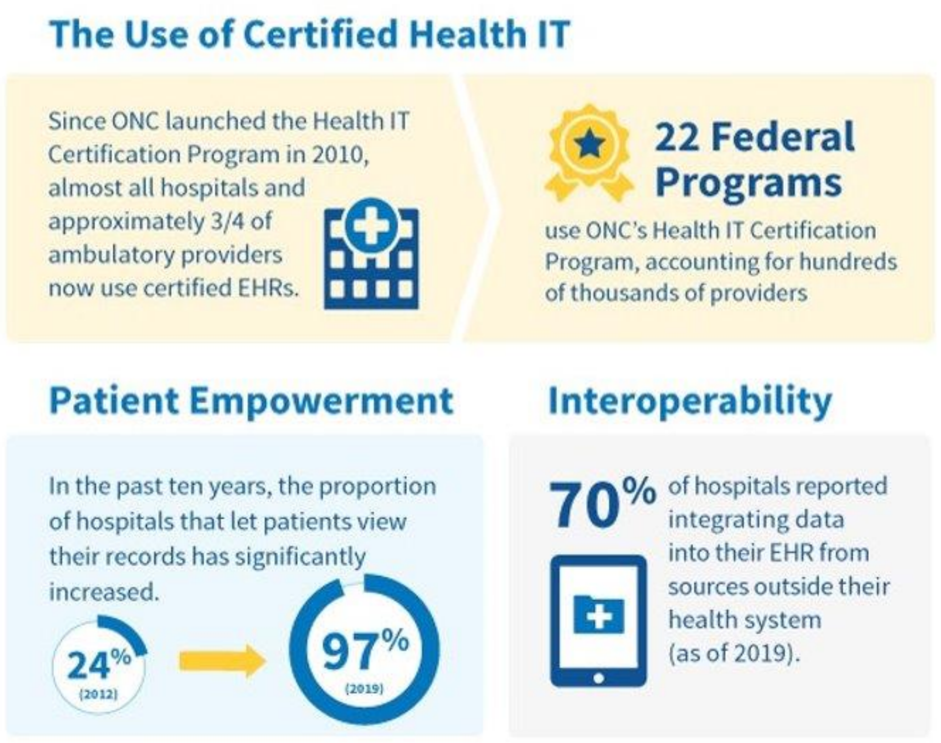
- The materials contained in this presentation are based on the provisions contained in 45 C.F.R. Parts 170 and 171. While every effort has been made to ensure the accuracy of this restatement of those provisions, this presentation is not a legal document. The official program requirements are contained in the relevant laws and regulations. Please note that other Federal, state and local laws may also apply.
- The materials contained in this presentation are based on the proposals in the “Health Data, Technology, and Interoperability (HTI-2): Patient Engagement, Information Sharing, and Public Health Interoperability” proposed rule. While every effort has been made to ensure the accuracy of this restatement of those proposals, this presentation is not a legal document. The official proposals are contained in the proposed rule.
- ONC must protect the rulemaking process and comply with the Administrative Procedure Act. During the rulemaking process, ONC can only present the information that is in the proposed rule as it is contained in the proposed rule. ONC cannot interpret that information, nor clarify or provide any further guidance.
- ONC cannot address any comments made by anyone attending the presentation or consider any such comments in the rulemaking process, unless submitted through the formal comment submission process as specified in the Federal Register.
- This communication is produced and disseminated at U.S. taxpayer expense.

Agenda

- Quick Intro: FHIR API Requirements in the ONC Certification Program
- HTI-1 Updates
- HTI-2 Updates
- Inferno Testing Updates and Demo

ONC Health IT Certification Program

- Through the combination of CMS payment incentives and ONC’s Health IT certification program, hospitals and providers rapidly adopted certified EHRs and ushered the modernization of the U.S. health care system.
- This has promoted:
  - a more effective marketplace, greater competition, increased consumer choice, and improved health outcomes
  - the seamless exchange of electronic health information across a variety of methods and platforms
  - a safe and secure health IT infrastructure for patients and healthcare providers
  - increased ease-of-use of health IT



The Use of Certified Health IT

Since ONC launched the Health IT Certification Program in 2010, almost all hospitals and approximately 3/4 of ambulatory providers now use certified EHRs.

22 Federal Programs use ONC’s Health IT Certification Program, accounting for hundreds of thousands of providers

Patient Empowerment

In the past ten years, the proportion of hospitals that let patients view their records has significantly increased.

24% (2012) → 97% (2019)

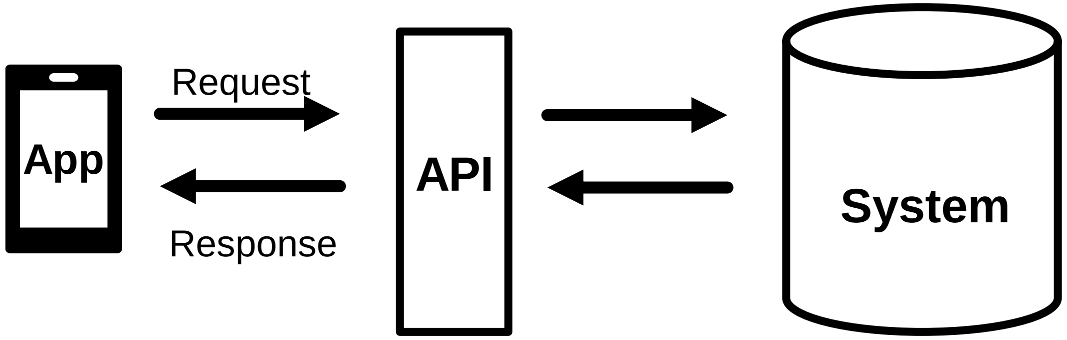
Interoperability

70% of hospitals reported integrating data into their EHR from sources outside their health system (as of 2019).

API Access “Without Special Effort”

Requirement from Congress

APIs that allow health information from certified technology to be accessed, exchanged, and used without special effort. (21st Century Cures Act)



ASTP Implementation

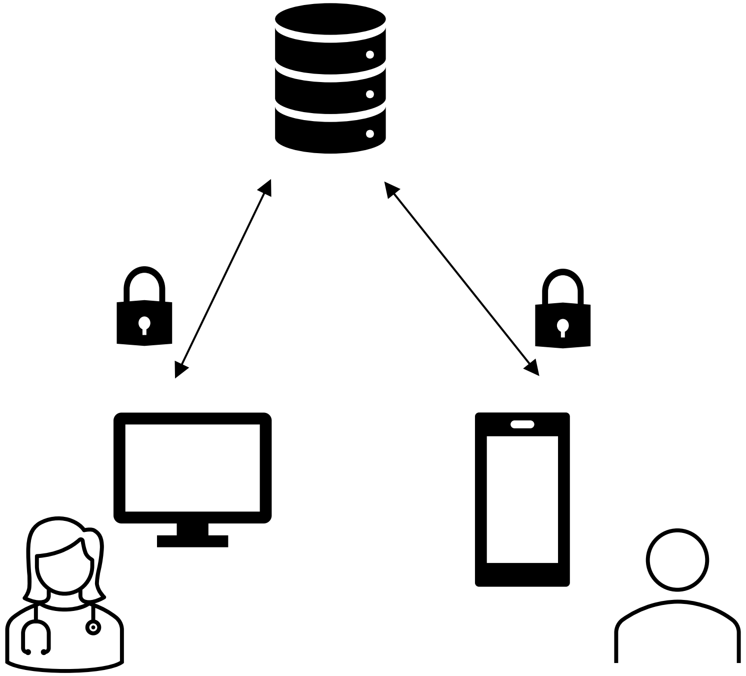
- Certification requirements at 45 CFR 170.315(g)(10) and 170.404
- Standards based API
  - FHIR, USCDI, US Core, SMART App Launch, and Bulk Data
- Use cases
  - Data for third party patient and provider facing apps
  - Efficient access to large volumes of information on groups of patients

HTI-1 Update: SMART App Launch v2.0

Transition to SMART App Launch v2: The HTI-1 Final Rule adopts the SMART App Launch v2 guide for use in the ONC Certification Program. This implementation guide is referenced in authentication and authorization requirements for the § 170.315(g)(10) criterion. ONC Certification Program adoption of the SMART App Launch v1 guide expires January 1, 2026.

Security Enhancements compared to SMART v1:

- *Proof Key for Code Exchange (PKCE)* - mitigates authorization code interception attacks.
- *CRUDS Scope Syntax* - refined syntax for more granular permissions.
- *Finer-grained resource constraints using search parameters* - more detailed scope constraints based on FHIR REST API search parameter syntax
- *Asymmetric Client Authentication* - authentication of "confidential" OAuth clients using secure key pairs (public and private).



HTI-1 Update: Token Revocation

Background: In the HTI-1 Final Rule, ASTP finalized a requirement for the § 170.315(g)(10) criterion that a Health IT Module's authorization server must be able to revoke and must revoke an authorized application's access at a patient's direction within 1 hour of the request.

This security enhancement supports:

- timely responses to privacy concerns
- mitigation of unauthorized data access
- alignment with industry best-practices for short-lived access tokens

HTI-2 Proposals: Security across APIs, part 1

- **Consistency across proposed API criteria**
- **SMART App Launch Framework**
  - Certain parts of SMART App Launch IG proposed depending on the criterion (e.g., standalone, EHR launch, backend services)
  - *(g)(10) Standardized API for patient and population services*
  - *(g)(20) Standardized API for public health*
  - Most of the patient, provider and payer proposed criteria:
    - *(g)(30) Patient access API*
    - *(g)(32) Provider access API – server*
    - *(g)(33) Payer to payer API*
    - *(g)(34) Prior authorization API – provider*
    - *(g)(35) Prior authorization API – payer*

HTI-2 Proposals: Security across APIs, part 2

- **UDAP: Security for Scalable Registration, Authentication, and Authorization**
  - Certain parts of HL7 UDAP Security IG proposed in criteria listed above, depending on the criterion (e.g., consumer-facing, business-to-business)
  - Requires trust framework and verifiable signed certificates to enable dynamic registration and authentication of clients
- **CDS Hooks**
  - Security model described in the CDS Hooks implementation guide including mutual authentication, trust, authorization, etc.
  - *(g)(10) Standardized API for patient and population services*
  - *(g)(34) Prior authorization API – provider*
  - *(g)(35) Prior authorization API – payer*

HTI-2 Proposals: SMART App Launch 2.2

- **Proposal Overview**: In the HTI-2 Proposed Rule, ASTP proposes to adopt the SMART App Launch v2.2 guide as the authentication and authorization standard required for FHIR API Certification, with a proposed effective date of January 1, 2028.
- **Security Enhancements compared to SMART v2.0 (if finalized):**
  - Cross-Origin Resource Sharing (CORS) - servers supporting browser-based apps must enable CORS to allow public discovery endpoints for any origin and token/FHIR API endpoints for registered origins.
  - Absolute URLs for /metadata - requirement for metadata URLs to be absolute (not relative) to remove ambiguity.
  - Token expiration handling - clarification regarding the “exp” field in the token introspection response, ensuring consistency between the “exp” field in the token introspection response and the “expires_in” interval in the original access token response.
- **User-access Brands and Endpoints (Brands)**: In the HTI-2 Proposed Rule, ASTP also proposes to adopt the Brands specification as the standard format for publication of API Discovery Details (i.e., FHIR endpoints and organization details).
  - Helps support clear identification of legitimate healthcare provider endpoints.

HTI-2 Proposals: Privacy and Security Certification Framework

- **Background**: Health IT Modules must meet specific privacy and security criteria to receive certification from an ONC-Authorized Certification Body (ONC-ACB) (see 45 CFR 170.550(h)(1)).
- **HTI-2 proposed rule**: ASTP proposes that to get certified to certain proposed and existing FHIR API criteria, Health IT Modules must also meet the following criteria (see proposed 170.550(h)(3)(viii)):
  - (d)(1): Attest to health IT module’s ability to authenticate a user and provision their authorized access
  - (d)(2): Attest to health IT module’s ability to record actions related to EHI (i.e., audit logs) in accordance with ASTM E2147-18
  - (d)(9): Attest to use of a FIPS 140-2 complaint trusted connection
  - (d)(12) [**HTI-2 proposed updated criterion]**: Protect stored authentication credentials using NIST approved encryption or hashing functions
  - (d)(13): For the time period up to and including December 31, 2027, attest yes or no to health IT module support for multi-factor authentication

HTI-2 Proposals: Multi-factor Authentication

- **§ 170.315(d)(13) (MFA) Updates in HTI-2 Proposed rule**:
  - Replace current “yes” or “no” attestation with new requirements.
  - Health IT certified to (d)(13) must support multi-factor authentication (MFA) and allow users to configure, enable, and disable MFA settings.
- **Integration with Other Criteria**:
  - Reference updated MFA requirements in various criteria with authentication use cases.
- **Applicability to FHIR API Criteria:**
  - Include MFA support in FHIR APIs for patient-facing authentication.
  - **Proposed Criteria:**
    - § 170.315(g)(10): Standardized API for patient and population services.
    - § 170.315(g)(30): Patient access API (for health and administrative information).

HTI-2 Proposals: Dynamic Client Registration

The HTI-2 Proposed Rule includes proposals to require components of the HL7 UDAP Security IG:

- Propose to require for the § 170.315(g)(10) “Standardized API for patient and population services” criterion support for dynamic client registration and subsequent authentication and authorization for dynamically registered patient-facing, user-facing, and system confidential applications.

- Propose to require support for dynamic client registration capabilities for other proposed certification criteria as well.

- Propose to adopt the HL7® Unified Data Access Profiles (UDAP™) Security for Scalable Registration, Authentication, and Authorization Implementation Guide Release 1.0.0 implementation guide (UDAP Security IG v1).

- Propose to add new requirements related to dynamic client registration in the API Conditions and Maintenance of Certification in § 170.404.

- Propose to require support for these proposed dynamic registration capabilities by December 31, 2027.

Inferno Framework

https://inferno.healthit.gov/

Certification Testing

Is an official testing tool for the ONC Certification Program

FHIR Profile Testing

Designed to test FHIR, including US Core, Bulk Data, SMART, and more

Interactive and Automated

Tests support both user guided and automated interfaces

Open Source & Transparent

Freely available code and documentation for open and accessible testing

Recent Inferno Updates

- **ONC Certification (g)(10) Standardized API Test Kit**, the official testing tool for the § 170.315(g)(10) “Standardized API for patient and population services” certification criterion, has been updated to align with the requirements specified in the HTI-1 Final Rule.

- **US Core Test Kit** has been updated to include tests for US Core 7.0.0. US Core 7.0.0 supports implementation of USCDI v4 in FHIR. Developers can use this Test Kit to self-assess if their servers conform to requirements in the US Core 7.0.0 implementation guide.

- **UDAP Security Test Kit**: A new Inferno Test Kit has been released to support developer self-assessment testing of the HL7 UDAP Security implementation guide. This Test Kit provides tests for parts of the HL7 UDAP Security IG v1, including metadata discovery, dynamic client registration, and authentication and authorization for consumer-facing and business-to-business apps.

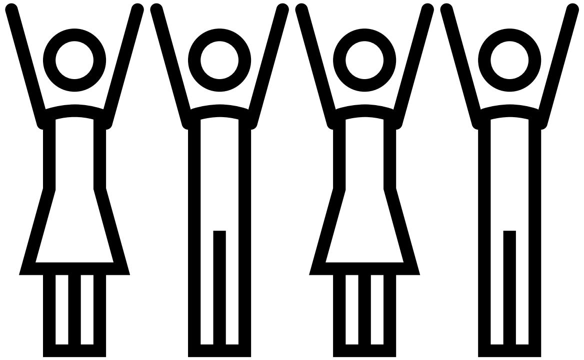
- These Inferno Test Kits are available on Inferno.HealthIT.gov

Inferno Demo

https://inferno.healthit.gov/

Get Involved

- ASTP Website
  - https://www.healthit.gov/
- Health IT Feedback and Inquiry Portal
  - https://inquiry.healthit.gov/
- Comment on regulations
  - HTI-2 comment period ends on October 4, 2024
- Inferno Tech Talks – Second Wednesday of every month
  - https://inferno.healthit.gov/events/
- Health IT Developer Roundtables
  - https://www.healthit.gov/newsroom/events



Thank you! Questions?

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

- @onc_healthIT
- 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!