

Health Center Guidelines for Implementing FHIR and the Information Blocking Rule

Molly Rafferty post on Wednesday, September 6, 2023 | Categories: [EHR Selection and Implementation](#), [EHR Implementation](#), [Health Information Exchange](#), [Relevance of HIE](#), [Description of HIE](#), [Implementation of HIE](#), [Information Blocking](#), [Promoting Interoperability](#), [Privacy and Security](#), [Privacy & Security Best Practices](#), [HIPAA](#)



HITEQ Center, September 2023

The [21st Century Cures Act](#) and the [ONC Health IT Certification Program](#) include rules for technical configuration and use of [Health Level 7® \(HL7\) Fast Healthcare Interoperability Resources® \(FHIR\)](#) for health data exchange and accessibility. Health centers are directed to enable and publish their healthcare data locations, known as FHIR endpoints,* to and from their electronic health record (EHR). Part of the Cures Act, known as the Information Blocking Rule, mandates that patients have “easy” access to their digital medical information, costs and claims associated with their health record, and whom the data can be shared with. FHIR is a standard information protocol that is widely used in the health IT community to meet Cures Act compliance.

*An endpoint describes the technical details of a location that can be connected to for the delivery/retrieval of information. For a list of resources that are typically used to identify where to locate endpoint details, visit <https://build.fhir.org/endpoint.html>.

FHIR interface specifications define how health data is exchanged for interoperability, retrieval, use, and transmission. [Getting Started with FHIR](#) outlines these specifications and contains information on the following:

How will information be exchanged? (see Foundation Module)
How will the data be secured? (see Security and Privacy Module)
When and what data is exchanged? (see Workflow Module)
How does the data conform to the FHIR specification and Implementation Guides? (see Conformance Module)

The following sections provide guidance to health centers for implementing FHIR in compliance with the Information Blocking Rule.

Administrative Practices

- Review the Cures Act rule: [API Conditions and Maintenance of Certification requirements](#) to ensure that FHIR endpoints and Application Programming Interfaces (API) are properly registered and accessible for use. These requirements provide details for FHIR endpoints, or “service base URLs” to be published.
- Establish appropriate data exchange and network transmission agreements, such as business associate agreements and Data Use Agreements (DUA), and incorporate them into local health center HIPAA policy and procedures. Health centers should document and inventory “actors” such as systems, users, software, and data requests to align appropriate security configurations on networks. For further guidance on implementing agreements, see [NIST 800-66](#) special publication and [CMS HIPAA and Administrative Simplification](#).

FHIR API Practices

- Test, review, analyze, and continually monitor third-party FHIR Apps and APIs through integrated information security controls.
- Review the CMS article: [Best Practices for Payers and App Developers](#) to learn about resources and how to establish and maintain a secure, FHIR-based healthcare API.

Cybersecurity Management

- Implement information security best practices, user access agreements, regular monitoring of systems' software, and apply recommended configurations and patches.
- Engage the use of subject matter experts and cybersecurity resources available through the [HITEQ center](#).

Practices for Securing FHIR endpoints

- Utilize a threat management system for mobile apps and FHIR API endpoints.
- Ensure API authentication keys are secured using valid certificate key exchange, Transport Layer Security (TLS), and [certificate pinning](#).
- Use standard authentication and access controls to ensure users and systems are authorized.
- Review the API security checklists that are available via the Open Web Application Security Project (OWASP) [GraphQL - OWASP Cheat Sheet Series](#).
- Validate hosts, ensure proper web and software security configurations within the platform or FHIR “framework,” implement web application firewalls (WAFs), and access audit logs and monitoring.

Resources

1. [Cures Act Final Rule: Information Blocking Exceptions \(healthit.gov\)](#)
2. [Policies and Regulations | CMS](#)
3. [CMS Interoperability and Patient Access Final Rule \(CMS-9115-F\) | CMS](#)
4. [The Cures Act](#)
5. [Best Practices for Payers and App Developers \(cms.gov\)](#)

 Tags: HIPAA data exchange Compliance security implementation security measures
information blocking information exchange FHIR Implementation FHIR
information blocking rule information blocking badge