Maverick Health Policy

HTI-2 Proposed Rule:
FAQs
August 5, 2024

On July 10, 2024 (officially published in the Federal Register on August 5, 2024), the Office of the National Coordinator for Health IT (ONC) proposed a new rule designed to support CMS' Advancing Interoperability and Improving Prior Authorization Processes final rule.

The new proposed rule is titled "Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability (HTI-2)" (Maverick Minute here). It is a significant body of work at 1,067 pages in its pre-published form. While it builds on ONC's prior regulatory scheme, it also introduces significant updates to the ONC Health IT Certification Program.

The HTI-2 rule proposes expanded criteria for certified application programming interfaces (APIs) that support patient access, care management, and electronic prior authorization – notably, including functionalities of payer and public health software for the first time. The proposed rule also introduces updates to the U.S. Core Data for Interoperability (USCDI) standard, advancing the baseline data elements required for health information exchange. Further, the rule introduces new requirements for the Trusted Exchange Framework and Common Agreement (TEFCA) with the goal of strengthening the privacy, security, and reliability of qualified health information networks (QHINs).

In the following overview, we will focus on the key provisions of the HTI-2 proposed rule, including the proposed certification criteria for APIs (i.e., Patient Access API, Payer-to-Payer API, Provider Access API, and Prior Authorization API), Health IT Modules that support public health data exchange, modified information blocking requirements, and more specific qualifications to become a TEFCA QHIN.

General ONC Certification FAQs

What is ONC's Health IT Certification Program?

ONC's Certification Program is a voluntary program established to ensure certified health IT adheres to the security, functionality, and technology requirements adopted by HHS. It is composed of functional requirements, known as "certification criteria," that enable health IT developers to understand the required capabilities, standards, and implementation specifications that health IT needs to meet to become certified under the Program.

If the Program is voluntary, why would health IT developers need to certify their products?

While participation in the ONC Health IT Certification Program is voluntary, the majority of large electronic health record (EHR) systems used by U.S. hospitals and office-based providers are ONC certified. The Program supports CMS' Promoting Interoperability Programs (formerly known as "meaningful use"). Beginning in 2015, eligible providers who do not use certified EHR technology (CEHRT) are penalized – receiving less than 100% of their Medicare fee schedule for professional services. As such, health IT developers – primarily EHR vendors – certify their products so providers will use them.

Since the publication of the HTI-2, HHS released another proposed rule titled "Acquisition Regulation: Information Technology; Standards for Health IT," which would require all healthcare providers and health plans that receive HHS funding to use certified health IT or, at a minimum, adhere to ONC standards. The proposed rule would apply to all solicitations and contracts, issued by or on behalf of HHS entities, that involve implementing, acquiring, or upgrading health IT used (1) for the direct exchange of individually identifiable health information between agencies and non-Federal entities, or (2) by healthcare providers, health plans, or health insurance issuers.

Effectively, this rule, if finalized, would create a regulatory reason for payer and public health IT vendors to certify under ONC's Certification Program if they want to be selected as a vendor for health plans that receive funding from HHS (e.g., Medicare Advantage plans).

Certification Criteria – APIs

Why are these updated certification criteria different than usual?

For the first time, ASTP/ONC proposed certification criteria for payer and public health software functionalities. The certification criteria are designed to align with CMS-establish API requirements, including:

- Patient Access API
- Provider Access API
- Payer-to-Payer API
- Prior Authorization API
- Provider Directory API

Notably, CMS' Advancing Interoperability and Improving Prior Authorization Processes Final Rule did not require plans to follow any specific implementation guides (IGs), instead recommending their use – for example, the Prior Authorization API (i.e., CRD IG STU 2.0.1, HL7 FHIR Da Vinci DTR IG STU 2.0.0, and PAS IG STU 2.0.1). This new proposed rule, HTI-2, creates certification criteria in ONC's Program that would require the use of such IGs to become certified.

What is the primary goal of the HTI-2 proposed rule concerning APIs?

To support data exchange between patients, providers, and payers as required by CMS regulations.

Why didn't CMS require these IGs rather than have ASTP/ONC do it under a different regulation?

CMS recommended IGs rather than requiring them to avoid locking payers into a particular version of the standards. Through ASTP/ONC's Standards Version Advancement Process (SVAP), ASTP/ONC is better suited to update required versions as necessary than CMS.

What are the specific IGs required for the Patient Access API?

ASTP/ONC proposed to adopt a "Patient Access API" certification criterion that can enable patients to access their health and administrative information by using a health application of their choice. The certification criterion provides that health IT modules supporting this API must conform to the following IGs:

Registration Requirements

- Health IT modules are required to enable a dynamic registration pathway that can support automated, scalable registration – allowing for more seamless integration.
- A functional registration pathway must be available for applications that cannot support dynamic registration – allowing apps to register using a non-standardized method.

Authentication and Authorization

- Health IT modules must support the SMART App Launch IG to grant access to patient data.
- For dynamically registered apps, health IT modules must support asymmetric certificate-based authentication – providing a higher level of security for patient-facing applications.

Security Measures

- Beginning January 1, 2028, health IT modules must support multi-factor authentication for patient-facing apps.

Data Access

- Health IT modules must allow patients to access and share their clinical and coverage information using the HL7 FHIR Da Vinci Payer Data Exchange (PDex) IG v2.0.0 STU2.
- Health IT modules must use the OAuth2.0 or SMART-on-FHIR Member-Authorized Exchange IG to authenticate and share information between patients, apps, and health plans.
- Health IT modules must support HL7 FHIR U.S. Core IG, ensuring data shared through the API adheres to standard formats and structures for U.S. healthcare data.
- Health IT modules must enable patients to access their claims data through a standardized API, following the HL7 FHIR Consumer Directed Payer Data Exchange (CARIN IG for Blue Button) IG, v2.0.0 STU 2. This guide supports the exchange of financial data such as adjudicated claims, cost-sharing details, and encounter information.
- The rule distinguishes between authenticated and unauthenticated APIs for accessing formulary data. Authenticated APIs can integrate formulary data with personally identifiable information (PII) and protected health information (PHI), while unauthenticated APIs provide access to public formulary data.
  - Health IT modules must publish information regarding a payer's drug formulary according to at least one version of the HL7 FHIR Da Vinci Payer Data Exchange (PDex) US Drug Formulary IG, v2.0.1 STU2. This helps patients understand drug costs, compare alternatives, and make informed decisions about their prescriptions.

What are the specific IGs required for the Provider Access API?

ASTP/ONC proposed adopting a "Provider Access API—Client" criterion and a "Provider Access API—Server" criterion to help providers retrieve patient data. The "Client" criterion enables providers to request and receive patient data from payers. The “Server” criterion ensures that payers can respond to data requests from providers and supply the necessary patient information.

Provider Access API – Client

- Health IT modules must support the ability to request patient history according to the HL7 FHIR Da Vinci Payer Data Exchange (PDex) IG v2.0.0 STU2.
- Health IT modules must support interaction with a "PDEX Server" and adhere to the corresponding client capabilities outlined in the PDex Server Capability Statement and related HL7 FHIR Profiles and Resources.
- Health IT modules must support requesting and receiving information on groups of patients, following the FHIR R4 standard and the Bulk Data Access IG.
- The health IT module must be capable of receiving, parsing, and writing patient health history and coverage information, following the PDex IG, CARIN IG for Blue Button, and US Core IG standards.

Provider Access API – Server: Registration

- Like the Patient Access API criterion, the server must support functional and dynamic registration.

Provider Access API – Server: Authentication and Authorization

- Health IT modules must support the SMART App Launch IG to grant access to patient data.
- For dynamically registered apps, health IT modules must support asymmetric certificate-based authentication – providing a higher level of security for patient-facing applications.

Provider Access API – Server: Data Access

- Health IT modules must allow providers to access and share clinical and coverage information using the HL7 FHIR Da Vinci Payer Data Exchange (PDex) IG v2.0.0 STU2.
- The module must support bulk data requests according to the FHIR R4 standard.
- The module must also conform to the Bulk Data Access IG (v1.0.0—STU 1 or v2.0.0—STU 2).
  - The module must support the ability to export data on groups of patients using the "GroupLevelExport" operation.
  - The module must also support the "_type" query parameter, which allows providers to specify the types of data they need within the bulk export. This can include specific data classes such as lab results, encounter details, or medication history, enabling more targeted and relevant data exports.
    - Up until December 31, 2027, the Health IT Module can comply with either the GroupLevelExport operation or both the GroupLevelExport operation and the _type query parameter. Starting January 1, 2028, compliance with both requirements becomes mandatory.

What are the specific IGs required for the Payer-to-Payer API?

ASTP/ONC proposed to adopt a “Payer-to-Payer API” certification criterion that support the exchange of health data between payer systems when a patient transitions from one payer to another. The certification criterion provides that health IT modules supporting this API must conform to the following IGs:

Registration Requirements

- Like the Patient Access API criterion, the server must support functional and dynamic registration.

Authentication and Authorization Requirements

- For dynamically registered apps, health IT modules must support asymmetric certificate-based authentication – providing a higher level of security for patient-facing applications.

Data Access Requirements

- Health IT modules must allow patients to access and share their clinical and coverage information using the HL7 FHIR Da Vinci Payer Data Exchange (PDex) IG v2.0.0 STU2.
- Health IT modules must support HL7 FHIR U.S. Core IG, ensuring data shared through the API adheres to standard formats and structures for U.S. healthcare data.
- Health IT modules must enable patients to access their claims data through a standardized API, following the HL7 FHIR Consumer Directed Payer Data Exchange (CARIN IG for Blue Button) IG, v2.0.0 STU 2. This guide supports the exchange of financial data such as adjudicated claims, cost-sharing details, and encounter information.
- The module must also conform to the Bulk Data Access IG (v1.0.0—STU 1 or v2.0.0—STU 2).
    - The module must support the ability to export data on groups of patients using the "GroupLevelExport" operation.
    - The module must also support the "_type" query parameter, which allows providers to specify the types of data they need within the bulk export. This can include specific data classes such as lab results, encounter details, or medication history, enabling more targeted and relevant data exports.
        - Up until December 31, 2027, the Health IT Module can comply with either the GroupLevelExport operation or both the GroupLevelExport operation and the _type query parameter. Starting January 1, 2028, compliance with both requirements becomes mandatory.
- Support the following Data Retrieval Methods:
    - “Query all clinical resource individually”
    - “$patient-everything operation”
    - “Bulk FHIR Asynchronous protocols”

What are the specific IGs required for the Prior Authorization API?

ASTP/ONC proposed adopting a “Prior Authorization API—Provider” criterion and a “Prior Authorization API—Payer” criterion to help facilitate the prior authorization process. The “Provider” criterion facilitates providers' ability to request coverage information and prior authorization from payers. The “Payer” criterion enables payers to process and respond to prior authorization requests, send necessary documentation, and communicate decisions.

In general, these APIs should be built on the HL7 FHIR Da Vinci Burden Reduction IGs – which provide a standardized framework for conducting electronic prior authorization transactions.

Those IGs are Coverage Requirements Discovery (CRD), Documentation, Templates and Rules (DTR), and Prior Authorization Support (PAS).

Prior Authorization API – Provider

- CRD
    - Health IT modules must support the ability to initiate coverage discovery, allowing providers to identify coverage requirements when scheduling future encounters or making treatment decisions.
    - The module must support workflow triggers (e.g., appointment-book, encounter-start, and order-select) to automate the initiation of coverage discovery based on specific events in the care process.
        - These triggers are facilitated through CDS Hooks, ensuring that the process is embedded within the provider's clinical workflow.
- DTR
    - The health IT module must support the ability to request and populate prior authorization documentation templates from payer systems, streamlining the process of gathering the necessary information for submission.
    - Light vs. Full DTR Capabilities
        - For EHRs that rely on SMART on FHIR apps to manage form filling, the module must support the ability to launch these apps and handle the necessary authentication and authorization.
        - For EHRs that manage form filling internally, the module must support the internal management of documentation. It must handle the creation and management of documentation based on payer rules and templates within the EHR itself, reducing dependency on external applications.
- PAS
    - Health IT module must support the ability to submit prior authorization requests to payer systems, including all necessary documentation generated through the DTR process.
    - The module must be able to process responses from payers, including approvals, denials, and requests for additional information, ensuring that providers have real-time updates on the status of their requests.
    - The module must support subscriptions to receive notifications about pending authorization responses, keeping providers informed of any delays or additional requirements.

Prior Authorization API – Payer

- CRD
    - Health IT module must support the ability to receive and respond to coverage discovery requests, providing necessary information to the provider's system in real-time.
- DTR
    - Module must support the ability to provide documentation templates and rules to providers, ensuring that the documentation process is consistent and comprehensive.
- PAS

- Module must support the ability to receive, process, and respond to prior authorization requests. This includes providing detailed responses such as approvals, denials, or requests for additional information.
- The module must support the ability to manage subscriptions, ensuring that providers receive timely updates on the status of their prior authorization requests.

Does this include prescription drug prior authorization?

Yes. Certification criterion for e-prescribing as recommended by ONC's federal advisory committee would be mandatory, to better support electronic prior authorization processes for drugs covered under a prescription benefit.

Why did ONC create these criteria for prior authorization?

It is well-settled that prior authorization processes have caused delays in patient care as clinicians must contend with the myriad and non-uniform requirements set by health plans who determine whether services are covered. ONC created the prior authorization criteria to help reduce the burden and complexity associated with prior authorization processes and make sure that patients receive care in a timely manner at the lowest possible administrative cost.

Are payer health IT vendors incentivized to certify to these criteria?

As it stands, there is no regulatory reason or incentive for payer health IT vendors to certify under ONC's program. Most payer health IT vendors avoid the certification process because doing so would subject them to information blocking rules, which could mean $1 million penalties for unreasonably limiting the exchange, access, or use of electronic health information (EHI). One way to "unreasonably limit" the exchange, access, and use of EHI is over-charging for the right to access, use, or exchange health data – potentially threatening a source of revenue for payer health IT vendors.

In the current environment, where there is a proposed rule that would require payers that receive funding from HHS to use certified health IT, payers may have the regulatory support to require their vendors to be certified (if this proposed rule is finalized as currently written). This means that payer health IT vendors will have little choice but to certify if they want to continue to serve members of federal health programs.

Certification Criteria – Public Health

What did ONC propose for health IT for public health?

ONC proposed three primary things to help improve public health data exchange:

1. An update to existing criteria for reporting public health data. Many of these criteria were updated for the first time since 2015, and using the most recent standards will help ensure the transmission or bi-directional exchange of public health data.

   a. The revised standards include: Immunizations, Syndromic surveillance, Electronic Lab Reporting, Computerized provider order entry – laboratory, Cancer Registry Reporting, Antimicrobial Use and Resistance Reporting, and Health Care Surveys.
   b. ONC proposed to add Birth Rates and Prescription Drug Monitoring as new criteria for transmission and bi-directional exchange, respectively.

2. ONC proposed new certification criteria for health IT for public health that supports the ability to receive, validate, parse, and filter data. ONC hopes that this will set minimum system capabilities and close gaps between certified health IT vendors and health IT for public health. The certification criteria include: Immunizations, Syndromic surveillance, Electronic Lab Reporting, Cancer Pathology Reporting, Birth Reporting, Prescription Drug Monitoring Reporting.

3. ONC proposed a new, FHIR-based API for public health reporting. This would establish requirements for public health data exchange for data senders. ONC hopes this will streamline and reduce reporting burden for healthcare organizations, as well as increase public health authorities' access to data.

Are they voluntary?

Yes, the new certification criteria for health IT for public health are voluntary.

Why did ONC propose these new criteria and API for public health?

Despite efforts in recent years to improve public health data sharing, there are still significant struggles in sharing public health data. Data is often siloed, and public health authorities struggle to access the data or communicate with one another. These updated and new certification criteria and proposed API are designed to address these issues and improve public health data exchange between providers, public health authorities, and payers.

How does this align with other federal efforts to improve public health data?

ONC's proposals are designed to support and align with the CDC's Public Health Data Strategy.

Information Blocking Updates

What is "information blocking" and why is ASTP/ONC proposing updates?

Information blocking refers to practices that unreasonably interfere with the access, exchange, or use of electronic health information (EHI). The 21st Century Cures Act initially defined and prohibited information blocking, and the ASTP/ONC established regulations to enforce these prohibitions.

The updates proposed under HTI-2 are designed to address specific scenarios where providers might not intentionally be engaging in information blocking but could still be perceived as doing so under the current regulations. This includes scenarios involving sensitive areas like reproductive health services, where sharing information might expose patients or providers to legal risks.

What specific changes are proposed to definitions used in information blocking regulations?

The term “health care provider” was updated to make it explicitly clear what labs and pharmacists are included in the definition, without changing who meets the requirements.

The terms “interfere with” and “interference” were updated to add a section to codify the acts and omissions that constitute interference; however, the rule noted that the proposed section would not be an exhaustive catalog. The following practices are explicitly described in the rule:

- Actions to impose delays on EHI use
- Non-standard implementation to limit interoperability
- Improper inducements or discriminatory contract provisions
- Omissions when action is necessary to facilitate information sharing

Are there any updates to information blocking exceptions?

Infeasibility Exception

- HTI-2 would revise the applicability exclusion of the *third-party seeking modification use* condition, changing “health care provider” to “covered entity.”
- ONC is also proposing to extend the exclusion so that it wouldn’t apply when a non-HIPAA-covered healthcare provider requests modification use from an actor who would be the provider’s business associate if the provider were a HIPAA-covered entity.
- The proposed rule also revises the *responding to requests* condition to offer a more flexible response timeframe. Under HTI-2, an actor could satisfy the condition in several ways:
    - First, by initiating discussions of alternative ways for information sharing between the actor and requestor within 10 days of the request.
    - Second, if the discussion does not reach successful EHI fulfillment, the actor must provide the requestor with a written response indicating the reason for infeasibility for discontinuation of discussions.
    - It would also establish a maximum timeframe in which discussions must reach a plan to proceed or determine that the request is not feasible.
- For infeasibility consistent with *uncontrollable events, segmentation, and third-party seeking modification use* conditions, HTI-2 would retain the *responding to requests* conditions existing requirement to respond within 10 business days of the actor receiving the request but edit the wording to make it clear when the 10-day timeframe begins.

Protecting Care Access Exception

- This exception would protect patients, providers, or other caregivers from legal action if they sought, obtained, or facilitated lawful reproductive health care. This would apply where an actor limits the sharing of EHI related to reproductive healthcare to protect the patient from potential legal action.

Requestor Preferences Exception

- This exception would give actors certainty that by honoring certain requestor preferences, they would not be engaging in information blocking.

- When requestor preferences are expressed or confirmed in writing for the following, it would not be considered information blocking:
  - Limitations on the amount of EHI made available to the requestor.
  - The conditions under which EHI is made available to the requestor.
  - When EHI is made available to the requestor for access, exchange, or use.

TEFCA

- HTI-2 would give actors assurance that complying with TEFCA requirements as a QHIN, Participant, or Subparticipant would not be considered an interference.

TEFCA Provisions

What did HTI-2 propose regarding TEFCA?

TEFCA is a policy initiative designed to make it easier to exchange electronic health information even though the parties have different computer systems that do not "talk" to each other. TEFCA was created to establish a unified framework for nationwide health information exchange through Qualified Health Information Networks (QHINs) – entities that go through a rigorous process and sign agreements that will ensure the secure and appropriate transfer of health data.

The HTI-2 rule proposes specific qualifications and requirements for entities designated as QHINs under TEFCA.

What are the proposed requirements for an entity to be designated as a QHIN under TEFCA?

The proposal outlines three key requirements for an entity to be designated as a QHIN:

Ownership Requirements

- The entity must be a U.S. entity, meaning it is organized in a U.S. state, commonwealth, or under U.S. federal law, and has its principal place of business in the United States.
- None of the entity's specified leadership or owners with a 5% or greater interest may appear on the Department of Treasury's Specially Designated Nationals and Blocked Persons List.

Exchange Requirements

- The entity must demonstrate the capability to exchange information among more than two unaffiliated organizations.
- It must be able to exchange all required health information.
- The entity must exchange information for at least one of the stated Exchange Purposes (e.g., treatment, payment, healthcare operations).
- It must also have the ability to receive, respond to, and initiate transactions for Exchange Purposes.

Designated Network Service

- The entity must meet specific network performance standards.

What are the ongoing requirements for a QHIN to maintain its designation?

To maintain its initial designation, a QHIN must continue to meet the ownership, exchange, and network service requirements necessary for initial designation. In addition, the QHIN must maintain an enforceable dispute resolution policy to address conflicts that arise during exchange.

Further, the QHIN must implement privacy and security policies, including:

- Adhering to a nationally recognized security framework.
- Employing a chief information security officer.
- Disclosing breaches involving PHI.
- Completing annual security assessments by a qualified independent third party.
- All individually identifiable health information exchanged by the QHIN must be encrypted.

Finally, the QHIN must maintain insurance and financial reserves to support its operations.

If a QHIN fails to meet these ongoing requirements, it may face suspension or termination; however, it has the option to appeal those decisions and rectify any deficiencies that led to that decision.

Other Provisions

How does HTI-2 impact the USCDI?

The rule proposed to set an expiration date for USCDI v3 of January 1, 2028, then requiring the adoption of USCDI v4.

What does the HTI-2 rule propose regarding the Real-Time Prescription Benefit (RTPB) criterion?

HTI-2 introduces a new certification criterion for RTPB tools, based on the NCPDP RTPB standard. These tools allow providers and patients to compare drug costs, view out-of-pocket expenses, and check if prior authorization is needed for specific medications.

Starting January 1, 2028, RTPB will be required in the definition of "Base EHR," meaning health IT modules must support RTPB transactions, enable users to request and receive prescription benefit details and notify them of any transaction errors.

The proposal also includes expanding certification to cover vaccines, while excluding devices and supplies for now.

What are the proposed changes to the Electronic Prescribing Certification Criterion under the HTI-2 rule?

HTI-2 proposes incorporating the NCPDP SCRIPT standard version 2023011 into the Electronic Prescribing Certification Criterion, effective January 1, 2028.

Key changes include renaming and revising certain prescription transactions, removing the requirement for medication history transactions due to adoption challenges, and making prior authorization transactions mandatory.

Additionally, the rule proposes updating RxNorm for medication coding, requiring the exchange of race and ethnicity information in prescription transactions, and including the electronic prescribing certification criterion in the definition of "Base EHR."

Where can I find more information on this rule?

ONC published 10 fact sheets about the proposed rule:

1. An Overview
2. Key Dates
3. E-Prescribing
4. Information Blocking Definitions
5. Information Blocking Exceptions
6. Public Health
7. TEFCA
8. USCDI Version 4
9. Modular API Capabilities
10. Patient, Provider Payer API

If you require any further analysis of this rule, or how it intersects with HHS' proposed rule on requiring payers who receive HHS funding to use certified health IT, please contact eric.schiavone@maverickhealthpolicy.com.