INDUSTRY STANDARDS FOR COMPLIANCE WITH HEALTH IT POLICY AND INTEROPERABILITY

HEALTHCARE INTEROPERABILITY WITH AWS

CONTENTS

Background and Context

In 2016, the US Federal Government passed new legislation intended, among other things, to foster greater interoperability of health data between organizations for the benefit of patients. In order to substantiate the new legislation, the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC)

published final rules for organizations handling health data with very specific compliance requirements to be enacted over multiple phases. Many such organizations have found the complexity, ambiguity, and changing deadlines of the regulations to be confusing. This whitepaper seeks to offer clarity to AWS customers and partners implementing solutions compliant with these final rules.

Current Interoperability Policy Overview

In this section, we will dive into the next level of detail regarding policy, legislation, and regulation.

Open discussions between regulatory bodies like the ONC (Office of the National Coordinator) and CMS (Centers for Medicare and Medicaid Services) with industry providers, payors, developers, and consultants have given rise to new standards and guidelines that have shaped digital transformation in healthcare.

New policy legislation in the form of the 21st Century Cures Act **(link)** has the goal of making healthcare data more interoperable and accessible to patients. More specifically, CMS, ONC, the Trusted Exchange Framework and Common Agreement (TEFCA), and the ever-evolving US Core Data Interoperability (USCDI) data element standards aim to implement this legislation through compliance requirements and prescriptive criteria for meeting them.

While these policy mandates have been pushed out through separate regulatory bodies and frameworks, they do have several common points of intersection as well as distinction. Unfortunately, this has led to confusion on the part of stakeholders rushing to meet compliance deadlines.

Understanding what the goals of the different regulatory bodies and frameworks are as well as what they do, how they function in the overall pursuit of interoperability, and what rules they have already effected may be helpful in guiding organizations as they look to meet the different compliance criteria and deadlines:

USCDI

The United States Core Data for Interoperability plays a major role in the 21st Century Cures Act across both the ONC, CMS and, as we will see later, TEFCA. While the USCDI is included in standards and criteria from all three regulatory bodies, there are a few core distinctions in how the datasets operate within each as well as how they function for the different industry actors.

The USCDI establishes a minimum set of data classes that are required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time.

Data classes listed in the USCDI are represented in a technically agnostic manner.

1. USCDI v1— Required—CCDS (Common Clinical Data Set) plus Clinical Notes and Provenance
2. Candidate Data Classes—Under consideration for USCDI v2
3. Emerging Data Classes– Begin evaluating for candidate status[1]

USCDI is derived from the US Core Implementation Guide (IG)-see below for an explanation of what IGs are. Learn more about the FHIR US Core Implementation guide here.

CMS

The core driver of CMS within the shift towards interoperability is to encourage payers and providers to implement APIs on EHR (Electronic Health Record) systems in order to to improve the electronic exchange of healthcare data and improve care coordination. This is intended to reduce workflow burden as processes like prior authorization become automated and streamlined between payer to payer or payer to provider functions.

The Centers for For Medicare and Medicaid Services has two policies from the May 2020 Interoperability and Patient Access Final Rule that are now in effect:

1. ADT CoP (Condition of Participation) Requirement: states that hospitals with certain EHR capabilities must send admission, transfer, and discharge (ADT) messages.
   Deadline: April 30, 2021
   Purpose: Notification for patients and care providers via application. This is a stipulation of the patient access requirement of the 21st Century Cures Act.
2. Patient Access and Provider Directory API:
   a. CMS requires payers taking part in Medicaid Advantage (MA), Children's Health Insurance Fee-For-Service programs (CHIPS FFS), Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally Facilitated Exchanges (FFEs) to convert unstructured PDF documents into FHIR data elements to support data exchange requirements of the Patient Access API.

   b. MA organizations, Medicaid state agencies, Medicaid managed care plans, CHIP state agencies and CHIP managed care entities are required to offer a

[1] The Draft Trusted Exchange Framework and U.S. Core Data for Interoperability Overview (USCDI) 2018. More information can be found at https://www.healthit.gov/TEFCA.

public facing Provider Directory API which must include data on a payer's network of contracted providers.
Deadline: July 1st, 2021
Purpose: Patient access and the movement towards FHIR standardization are major goals of this rule enactment.

While the above noted policies have gone into effect, there are more that are scheduled to begin in the upcoming 2022 and 2023 performance years.

API Name	Supporting IGs	Who is impacted?	Deadline
Patient Access API	• The CARIN Consumer Directed Payer Data Exchange IG (also referred to as the CARIN IG for Blue Button®) • HL7 FHIR Da Vinci PDex IG • HL7 US Core IG • HL7 FHIR Da Vinci - PDex US Drug Formulary IG	Payers Providers ISVs	July 1st, 2021
Provider Access API	• See Above IGs for Patient Access API	Payers Providers ISVs	July 1st, 2021

Payer-to-Payer API	• See Above IGs for Patient Access API	Payers	N/A ("CMS will not take enforcement action against certain payers for the payer-to-payer data exchange provision of the May 2020 Interoperability and Patient Access final rule until future rulemaking is finalized.")
Provider Directory API	• HL7 FHIR Da Vinci PDex Plan Net IG	Payers Providers	July 1st, 2021
EHI Scope Expansion to include full electronic Designated Record Set (DRS)		Payers Providers ISVs	October 6th, 2022

USCDI: CMS Perspective

USCDI defines data elements for patient access, provider access, payer access, provider directory, or prior authorization APIs. Ready-made implementation guides using the HL7 Da Vinci FHIR standard across the different data elements are a resource that payers can use to meet CMS criteria of the 21st Century Cures Act.

HL7 FHIR US Core IG 4.0.1 should cover:

- Allergies and intolerances
- Assessment and plan of treatment
- Care team members
- Clinical notes
- Clinical tests
- Diagnostic imaging
- Encounter information
- Goals
- Health concerns
- Immunizations
- Laboratory
- Medications
- Patient demographics
- Problems
- Procedures
- Provenance
- Smoking status
- Unified device identifier for patient's implantable devices
- Vital signs

Organizations can find more details in version 2 of the USCDI here.

ONC

The Office of the National Coordinator for Health IT (ONC) developed a Final Rule to the 21st Century Cures Act that specifies technical standards and definitions for key actors and stakeholders to remain compliant to the new rule and furthers the possibilities for a more portable national healthcare system.

In regards to interoperability and information blocking, the Final Rule sets specific technical implementations in the following areas:

- The Electronic Health Information (EHI) Export Certification Criterion
- FHIR API Certification Criterion
- Compliance Timeline
- Patient EHI Access and Authorization

ISVs and SIs should pay close attention to upcoming compliance dates for payer and provider organizations in order to develop competitive products for a marketplace that is demanding tools for interoperability as a result of this policy momentum. Below, you will find a table that lists and describes criteria as prescribed by CMS and ONC rules as well as compliance dates. Of note is that many of these dates will be happening within the next year or two. That means

organizations are in a crunch to discover and implement solutions that will allow them to meet policy criteria.

Certification Criterion	Regulation Text Citation*	Description	Deadline
EHI Export	§170.315(b)(10)	*Export files with all of a single patient's electronic health information the health IT produces and electronically manages on that patient.*	***December 31, 2023***
End-User Device Encryption	§170.315(d)(7)	***EHI must be encrypted when stored on technology designed to store it after the technology on the device stops.***	December 31, 2022
View, download, and transmit to 3rd Party	§170.315(e)(1)	*Patients must be able to use internet-based technology to view, download, and transmit their health information to a 3rd party*	
Patient Health Information (PHI) Capture	§170.315(e)(3)	*A user can identify, record, and access information directly and electronically shared by a patient*	
Consolidated CDA Creation	§170.315(g)(6)	*Health IT can create a C-CDA file in accordance with the HL7 C-CDA Release 2.1 IG that includes at a minimum all of the data classes in the USCDI.*	***December 31, 2023.***
Application Access-All Data Request	§170.315(g)(9)	*The API must include accompanying documentation which contains API syntax, function names, required and optional parameters and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.*	
Standardized API for Patient and Population Services	§170.315(g)(10)	*mplements HL7 FHIR as the standard framework for third-party API integration for patient and population ervices.*	***No later than 24 months after publication date (December 31, 2022).***
Authentication, Access Control, Authorization	§170.315 (d)(1)	*§Following the user's authentication, the technology establishes permissions associated with the user's ability to access electronic health information and the actions the user is permitted to perform with the technology.*	
Encrypt authentication credentials	§170.315(d)(12)	*§Health IT developers must attest "yes" or "no" to whether the Health IT Module encrypts authentication credentials. The criterion places no requirements on health IT customers, such as health care providers, to implement these capabilities*	

		(if present in their products) in their health care settings.	
Multi-factor authentication	***§170.315(d)(13)***	***Health IT developers must attest "yes" or "no" to whether the Health IT Module supports multi-factor authentication. The criterion places no requirements on health IT customers, such as health care providers, to implement these capabilities (if present in their products) in their health care settings.***	

USCDI: ONC Perspective

The USCDI is made up of a standard set of health data elements for interoperable health exchanges across the United States. The ONC specifically governs what the USCDI is and supports a forum for individual health IT stakeholders to submit new data elements and classes for future versions of the USCDI. The current USCDI V2 **(link)** supports data classes for:

- Allergies and Intolerances
- Encounter information
- Clinical Notes and Tests
- Medications
- Patient Demographics
- Laboratory Tests
- Immunizations
- Provenance
- Procedures
- Assessments and Treatment Plans
- Diagnostic Imaging
- Care Team Members
- Vital Signs

ISVs and SIs can check updates on the USCDI through the ONC portal as well as submit new data class elements through the ONDEC (ONC New Data Element and Class) Submission System. By developing products and applications accordingly, these health IT stakeholders will be one step closer to passing the information blocking criteria present in the final rule.

TEFCA

While the USCDI does provide some level of interoperability standardization across multiple regulatory frameworks, TEFCA will expand on some of the current limitations by providing an infrastructure for oversight on the major principles defined by the framework for interoperability.

The Trusted Exchange Framework and Common Agreement is ONC's method of providing a national interoperability standard through the secure exchange of structured and unstructured electronic health information amongst health information networks. The plan is to implement the Common Agreement across state and regional Health Information Networks (HINs) that share basic clinical information with one another. The overarching goal is to reduce administrative burden across the nation while creating a base foundation for universal interoperability across state-level and regional networks.

TEFCA Principles

The following consist of a bird's eye view of how stakeholders should practice under TEFCA policies:

- Standardization: Federally recognized standards for interoperability
- Transparency: All exchanges are conducted openly
- Cooperation and Non-Discrimination: Collaboration across stakeholders and business competitors
- Security: EHI is exchanged in a manner that promotes patient safety and data integrity
- Access: Patients have easy access to care information
- Accountability: Lower the cost of care and improve the health of the population via bulk data exchange

While TEFCA is still in its nascent stages of development, steps have been taken to solidify its place in the interoperability policy landscape through the appointment of a Recognized Coordinating Entity (RCE). Qualifying HINs will apply to become Qualified Health Information Networks (QHINs) by signing the Common Agreement in 2022.

By applying specific policy rules across payer, provider, and vendor stakeholders, TEFCA will be one of the most instrumental regulatory bodies in health IT. Understanding what the general direction of the framework is prior to the Common Agreement going into effect will be advantageous to stakeholders.

Draft TEFCA Requirements

Current TEFCA standards are relatively ambiguous, in order to provide the private sector with the freedom to create innovative products that work within the framework's key principles for nationwide, interoperable exchange.

The latest draft in 2019 outlines a common set of principles, terms, and conditions that will support the 2022 release of the Common Agreement for nationwide interoperable data exchange. Some major points of interest for stakeholders include:

- Initial QHIN application and onboarding: Opportunities for payers, providers, and developers to take a more active role in the network and provides the ability to locate and transmit EHI between multiple persons and entities
- Data Quality and Minimum Necessary Requirements
    - Patient Demographic Data for Matching
    - Patient matching evaluation conducted 18 months after Common Agreement execution by QHIN
    - Minimum Necessary Requirements: Use of and disclosure of EHI in accordance with HIPAA Rules
- Transparency:
    - Fee schedule: Disclosure of Fees to RCE for use of service within 30 days of Common Agreement going live.
- Cooperation and Non-Discrimination:
    - Prohibition of EHI exclusivity
    - No anti-competitive effects that could be deemed discriminatory towards competitors
- Privacy and Security:
    - Minimum security EHI requirements defined by HIPAA
    - NIST cybersecurity framework
- Participant Minimums: minimum obligations across all framework standards

Major changes between Draft 1 and Draft 2 include:

1. QHINs now have 18 months instead of 12 to update agreements and technical requirements
2. Exchange purposes now include Quality Assessment and Improvement as well as Business Planning and Development
3. QHIN prerequisites have been updated to require that the HIN show reasonable evidence of exchanging EHI as well as provide a reasonable plan for how it will achieve Common Agreement requirements

At the moment, a draft of the framework for network to network health information exchange (QHIN technical framework) has been released and is available for comment. This is the latest update from ONC and the Seqoia Project and applies to stakeholders that have applied to become participating QHINs.

Some areas of interest include:

- “QHIN Query” information exchange modality for patient query, document query, and document retrieval
- QHIN Message delivery between provider organizations, public health reporting, information submission, care plan updates, and clinical alerts
- Participating QHIN Requirements:
    - C-CDA 2.1
    - USCDI V1 data elements
    - All known demographics supported by the IHE Cross Community Patient Discovery (XCPD) profile in Query Solicitations
    - Audit logging
    - Patient lookup via Record Locator Service (RLS), QHIN-level electronic Master Person Index (eMPI), and federated patient lookup
    - Connectivity between QHIN and downstream QHIN subparticipant
- FHIR roadmap support for QHIN to QHIN exchange models
    - OAuth not designed for multi-hop security model
- Major opportunities for stakeholders via QTF (Qualified Health Information Network Technical Framework) feedback

There are many aspects to TEFCA and the road towards nationalized interoperability is a long one. The opportunities, however, are many and organizations across the care continuum should pay close attention to dates as well as participate in feedback to help drive the best way forward.

It’s clear to see that while there are several distinctions amongst the various frameworks and regulatory bodies, there are also several areas of overlap. The aim for this section is to highlight those specific areas for further exploration by stakeholder type in the sections ahead. As standardization becomes established in the industry, the criteria for fulfilling these standards will likely evolve. Therefore, keeping a constant eye on regulation changes and updates to technology and how they fill the gaps in care will be important for industry stakeholders.

This compliance guide has been developed to offer a general roadmap that payers, providers, ISVs, and SIs can use as a tool to judge what the specific criteria are and when compliance must be met. With some of the compliance deadlines having already passed, some of the criteria should have already been instituted. Regardless, they are included here to provide context to the general pattern of how policy makers are implementing compliance across the entire industry.

In the next sections, we will go over specific policy points while pointing out which actors will be affected as well as how they can enact practices that allow them to remain compliant after the deadlines have arrived. This document provides AWS customers with clear guidance on implementing technical measures in support of compliance with Conditions and Maintenance of Certification across the multiple regulatory frameworks and guidelines.

Disclaimer: As with most new policies being rolled out, many of the technical implementations we prescribe in this guide are subject to change in line with policy criteria detail changes. We recommend organizations periodically review regulatory requirements for interoperability and information blocking or institute a compliance coordinating team that can keep up to date with policy changes.

Official Data Consolidation - Payers and Providers

One of the major issues that have come up for Payers and Providers when it comes to implementing the 21st Century Cures Act is the issue of data consolidation.

Organizations have pockets of data in many different places. Because business practices evolved without an emphasis on data, the issue of data inventory has been a major roadblock to seamless data transfer and interoperability. Additionally, different business units keep data in different places.

However, there is no authoritative place in the organization for all the clinical information for a patient. When business units like the Care Coordination Group get data from one location and the Quality Measurement team gets it from elsewhere, it is not so much the underlying API technology that is the burden as the specific business practice of data consolidation amongst healthcare actors.

In order to properly solve this problem, organizations must consolidate data in one authoritative place in order to integrate and normalize it so that it provides value to the patient.

"The API Condition of Certification requirement in Section 4002 of the Cures Act requires health IT developers to publish APIs that allow "health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law." The requirement also states that a developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws."[2]

[2] 85 FR 25739

The healthcare organization can achieve this by:

- Defining how data is consolidated within the organization
- Identifying what the official data sources are for any one particular data element
- Determining the formats those systems and sources generate when exporting data in order to best apply a transformation layer

We have adopted the HL7 FHIR US Core Implementation Guide STU 3.1.0 (US Core IG)[3] implementation specification in § 170.215(a)(2). We note that we adopted the latest version of the US Core IG at the time of the final rule publication. The US Core IG defines the minimum conformance requirements for accessing patient data using FHIR Release 4 (adopted in § 170.215(a)(1)), including profiled resources, operations, and search parameters for the Data Elements required in the USCDI implementation specification (adopted in § 170.213).[4]

Providers can implement the above compliance measure by partnering with developers that have tested their tools against this implementation criterion.

More specifically, those developers that have successfully tested with the Inferno tool have developed FHIR implementations consistent with ONC specifications.

As the push towards FHIR readiness will drive data standardization between organizations, one QHIN is specifically looking to build FHIR data repositories in payer platforms that can interact with the APIs within their own FHIR-enabled platform that facilitates broad healthcare data interoperability.

The process includes:

1. Data Assessment to develop a compliance strategy based on the source system and data readiness of the payer organization. If organizations have their data in a FHIR repository already, they can use their own API to call the HIE API.

2. Data sources are pulled into a centralized repository where a transformation layer is applied.

3. Additional feeds and custom specifications are applied to accommodate gaps in the HL7 US Core IG as well as unique customer needs.

After the payer, provider, or hospital obtains data from the patient, they can send it into the HIE where the HIE can integrate it so that it is available via an API.

[3] US Core Implementation Guide standards are in constant flux. This whitepaper is going by the most recent implementation guide at the time of publication. See publication history here.
[4] 85 FR 25740

As the practice becomes more common, getting the data back out to patients for review in a short period of time will become increasingly important. As a result, there will be a need for a daily refresh update with formats that can go through an ETL (Extract, Transform, Load) and can be served up as an API in the backend.

At the moment, QHINs are looking to implement FHIR-ready standard IGs to data elements on a regular basis and then serve them back to the partner organization. Additionally, brokering user management and user identity functions will make the data readily available to the patient.

We recognize that our formal adoption of the HL7 FHIR standard and the associated implementation specifications referenced in § 170.315(g)(10) would be consistent across all Health IT Modules presented for certification.[5]

The above policy excerpt notes an important rule that providers should keep in mind when looking to partner with ISVs.

TEFCA and USCDI Data Class Evolution

Organizations, however, should not be completely satisfied with "rule compliance" because, as we noted before, rules are subject to change rapidly. Use cases with TEFCA at the center in the next few years may result in USCDI data expansion that will become API and interface requirements for Health IT developers and vendors[6]. These organizations should be ready for this in the future as data standardization processes become normalized and TEFCA takes on a greater influence in future ONC requirements.

The USCDI establishes a minimum set of data classes that are required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time.

Data classes listed in the USCDI are represented in a technically agnostic manner.

1. USCDI v1— Required—CCDS (Common Clinical Data Set) plus Clinical Notes and Provenance
2. Candidate Data Classes—Under consideration for USCDI v2
3. Emerging Data Classes– Begin evaluating for candidate status[7]

Application and Service Validation - ISVs

[5] 85 FR 25748
[6] Q&A: SHIEC's Lisa Bari on 'Critical Time for HIE's in this Country'
[7] The Draft Trusted Exchange Framework and U.S. Core Data for Interoperability Overview (USCDI) 2018. More information can be found at https://www.healthit.gov/TEFCA.

As it stands now, the Final Rule to the 21st Century Cures Act has no process for vetting applications and services that make use of SMART on FHIR authorization in order to process data through an app that is connected to the API. Essentially, an "authorized" web service can collect everything on a patient's device - all an organization needs to do is obtain consent from the patient to pull their data. Instead, providers should partner with organizations like state HIEs that have come up with their own processes for application validation.

For some HIEs, the app can register with a source organization like a payer via the HIE's developer portal.

During registration, the application will need to:

1. Attest to organization-specific privacy and security policies.

2. Request tokens to facilitate the authorization and authentication process in alignment with SMART on FHIR, OAuth2.0, and OpenID Connect standards.

Token introspection will allow implementers of § 170.315(g)(10)-certified Health IT Modules to use API authorization servers and authorization tokens with various resource servers. This functionality has the potential to reduce complexity for implementers of § 170.315(g)(10)-certified Health IT Modules authorizing access to several resource servers and reduces the overall effort and subsequent use of § 170.315(g)(10)-certified Health IT Modules consistent with the goals of section 4002 of the Cures Act to enable the use of APIs without "special effort." Although we do not specify a standard for token introspection, we encourage industry to coalesce around using a common standard, like OAuth 2.0 Token Introspection (RFC 7662).[8]

Some HIEs specifically work with organizations to provide a solution by using the organization's current member ID structure to provide an authentication layer that matches consumers to the source system.

This works by using a patient attribution service that stores the member-specific location of its data to make future API calls. When a member queries for their data, the application has already confirmed that it can access the data from the Payer within the developer portal.

Authentication and Authorization processes occur in alignment with SMART on FHIR via OAuth2.0 and OpenID Connect standards.

Health IT Modules presented for testing and certification must demonstrate the ability to perform user authentication, user authorization, and issue a refresh token valid for a period of at least 3 months during its initial connection with an application to access data for a single patient.[9]

[8] 85 FR 25748
[9] 84 FR 7483

While developing a process unique for the organization will likely be required in most instances, the ideal scenario is that the HIE can integrate with the organization's already existing identity management solution in order to facilitate API calls.

While these processes have facilitated the validation process for applications to "pipeline" large amounts of quality healthcare data, the issue of privacy still remains a concern with the lion's share of the responsibility resting with the patient.

While this remains a gap in current privacy regulation, the best that can be done is for organizations like payers, providers, ISVs, and SIs receiving patient information to use the same approach towards security as they would with patient data received by other means. This means making sure the organization has practices in place that follow HIPAA privacy rule standards.

However, ISVs must attest "yes" or "no" to their ability to provide multi factor authentication (170.315(d)(13)) as part of their health IT module.

The attestations will serve to identify whether or not certified health IT supports encrypting authentication credentials and/or multi-factor authentication (MFA). While these criteria provide increased transparency, they do not require new development or implementation to take place.[10]

If an application attests to the security and privacy policies of an organization within the HIE developer portal and passes FHIR standard compliance tests (via a program like Inferno), the organization holding patient data cannot stop the app from accessing data due to the information blocking stipulations present in the Final Rule.

At the end of the day, the patient makes the final decision on what applications get access to their health information. A clear communications workflow, including one that states who has permission to access which data, present in the attestation process for the patient, can help mitigate this tension as the rules continue to evolve around patient access to health information. For example, push notifications and app-based reminders for granting permissions can serve as placeholders for more permanent solutions in the future.

HIPAA's Privacy Rule puts the onus on the patient to provide credentials to applications and services that have access to the API via SMART on FHIR, Oauth2.0, or OpenID Connect.

Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

[10] 85 FR 25645

(i) Psychotherapy notes; and

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[11]

If the ISV application meets all of the requirements but the HIE still has concerns, this will engage the information blocking ambiguity that is currently present in the Final Rule. While the company connecting the API may have a privacy policy in place for public consumption, the HIE still does not know how the data will be used by the company. As we previously noted, subscribing to the CARIN alliance code of conduct can help clear any doubts at this time.

These gaps in security and privacy will become more clear as the compliance period in the timeline approaches. The ONC roadmap has 10 year milestones that can give companies an insight of where they see the vision unfolding for the move towards greater data flow**.**

Description	**Date**
ISVs prohibited from restricting certain communications	4/5/2021
EHI definition is limited to the EHI identified by the data elements represented in the USCDI	4/5/2021-10/5/2022
Submission of initial real world testing plans for 2022	12/15/2021
First attestation to Conditions of Certification required	4/1/2022
EHI definition is no longer limited to the EHI identified by the data elements represented in the USCDI	10/6/2022
HL7 FHIR API capability and other Cures Update Criteria must be made available	12/31/2022
Submit initial real world testing results	3/15/2023
EHI export capability must be made available	12/31/2023

There are, however, technical pieces in place within OAuth2.0 and SMART on FHIR to make sure there is a secure chain of data flow for ISVs.

The Right to Access rule implies that patients need to be educated on which platforms they are permitting access to. Since there are no current penalties for violating patient privacy after the patient has granted app authorization through SMART on FHIR, third party vendors and organizations should be prepared to join the CARIN Alliance, signing up to its informal code of conduct, to follow and to show solidarity with protecting patient information as interoperability becomes more common.

[11] 45 CFR § 164.524

A company concerned with patient trust can use the registration process as the template guide for privacy and security compliance recommendations as their application is developed. The trust framework can be downloaded here and a request for membership can be found here.

Additionally, ISVs can utilize the privacy policy best practices set by the ONC and other Health IT resources as a set of business practice guidelines and can test whether they meet FHIR standards using the Inferno tool offered by the ONC, regardless of what organizations, developers, or portals they are registered with. This will give the developer an understanding of whether or not they are capable of meeting the technical requirements for application-driven interoperability.

Data Integrity - Payers and Providers

When transferred from source to source, i.e. payer to provider, data integrity often comes into question as a result of the specific standards that have been implemented at the organization. Additionally, data transfer from organization to organization can result in the transfer of stale or inaccurate data.

These data integrity issues serve as challenges to the proper aggregation of data for accurate patient information. With the goal of patient access being the ability to review and critique results for accuracy, payers and providers can choose to partner with organizations that have rigorously tested their tools for data accuracy and integrity.

As we have mentioned earlier, the Inferno tool helps to implement a consistent FHIR standard across all data elements. This can be particularly useful when looking to transfer data between organizations utilizing different EHR systems. While no current standard exists for cleaning up the data, this tool can prevent inaccurate data from propagating within organizations that can result in lawsuits from the systematic mishandling of data streams.

From the HIE perspective, data should be presented in a consistent manner. Data should be taken from one system or multiple systems and multiple file formats and converted into one consistent FHIR format with semantic equivalence preserved. At the moment this can only be done by specialized tools or experts with the specific knowledge of how to do that.

When the source system data is converted into “Format X”, the data changes. It changes again when “Format X” data is converted into FHIR resources. An HIE can provide a transformation layer to the source data in order to maintain data integrity throughout the process towards patient access.

FHIR resources include provenance metadata that adds an additional layer of context to the original data source and can provide additional verification around data integrity. This can help teams understand and detect how data integrity may have been compromised.

Data Consistency and Raw Data - ISVs and SIs

The current SMART-authorized API allows third party applications to connect to EHRs through FHIR interfaces. The patient side launch includes authorization for data to be accessed by the third party via an access token. SMART Authorization scopes include population data which uses the Bulk Data Access FHIR IG for large groups of individuals as well as CDS Hooks that provide contextual information to the EHR for the provider side of the application.

The implementation specification includes OperationDefinitions, which define how the multiple patient export operations are invoked by clients, and the SMART Backend Services: Authorization Guide, which describes how a client can register with and obtain an access token from a server compliant with the implementation specification.[12]

Unfortunately, the Final Rule only mandates that these scopes must be available to the patient in a form serviceable by the implementation guide format from the basic data set. This means that the patient is getting a flat set of data that does not provide additional context to what the data actually means. This raw data does, however, give ISVs an opportunity to expand on their market value through data annotation and contextualization.

The Final Rule does, however, list data categories that are needed by Payer organizations through open APIs as represented by those elements in the USCDI.

The API certification criterion requires the use of the Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standard Release 4 and references several standards and implementation specifications adopted in § 170.213 and § 170.215 to support standardization and interoperability. This certification criterion will align industry efforts around FHIR Release 4 and advance interoperability of API-enabled "read" services for single and multiple patients.[13]

While access to data is the priority, ISVs will need to consider the patient perspective when determining how to make this data useful for the end-user.

---

[12] 45 CFR 170.215
[13] 85 FR 25645

From the application developer perspective, how useful the data is will depend on how effectively the application displays that information, as well as how the patient uses it. The presentation of data and how it is consolidated will play a major factor in application usability.

While there is no rule around how the data should be addressed, the common concern is that raw data might prove complicated and meaningless to the end user. The general consensus from industry players is that more frequent usage of the data from FHIR resources will lead to a natural refinement where developers begin to normalize and enrich the data around what information is necessary, useful, and meaningful for the end user.

The HIE typically serves as a broker in the healthcare community to achieve consensus around what data adds value to the patient and patient provider team. As there is no current API around this higher level knowledge, a critical consensus and agreement will be necessary to determine how the data is pushed out to the patient in a useful way.

Patient Matching and Identity Management - Payers, Providers, and ISVs

Two major models to serve as patient data exchange standards have been developed:

Federated Model - Payers and Providers

Allows patient access to any medical data from any original source via a one time record. The information can be sent via a document much like a background check.

The core challenge with this model is the current inability to pull what the patient specifically needs from the provider or payer that they are dealing with. More technical implementations like the Master Patient Index (MPI) specific to payer and provider organizations are required to do more sophisticated patient data extraction.

Consolidated Model - Payers

One ID and data lake that houses all of the patient's information they can access at any time. It serves as a storage center for the patient's information.This is similar to a driver's license that has all the patient's information in one place.

At the moment, payers likely have the ability to do patient matching as they calculate deductibles and benefits for patients across multiple providers. The need for HIEs to have this same viable approach to patient matching will be important as patient information can come from more than one payer.

While the ONC Rule has outlined the use of OpenID Connect 1.0 to facilitate the verification of the end user's identity in the OAuth2.0 authentication process, the Final Rule has no specification on what identifiers should be used to facilitate patient matching techniques.

Patient matching is a key component for driving interoperability between healthcare organizations. Though the Final Rule explicitly states that all patients should have access to all

claims and clinical information, as noted with the above mentioned models, there are still gaps in how vendors can consolidate patient information in a way that is conducive for compliance with the Final Rule.

At the moment, all a vendor has to do is provide technical means of providing patients with data from disparate providers and payers. It is the patient's responsibility to know their individual identity attribute.

With the end result of telling a patient what their medical information or prescriptions are agnostic of where they are coming from, the need for a standardized process towards data consolidation will be important as the push towards interoperability becomes a reality for the entire healthcare ecosystem.

Data consolidation that is enacted via vendor and HIE partnerships will allow all organizations in the healthcare community to push data towards the HIE where the HIE will serve as broker for the community health record.

A standardized approach towards data consolidation through an agreed upon broker for the community health record will allow patients to use apps via FHIR resources to download their care information and become a proactive part of their own care support through value based care.

Currently, some HIEs are working with payers to see what they currently use for patient matching and identify the best way to provide all of the required information for compliance. Enhance the existing memberID structure by adding a member-specific alphanumeric ID via Common Key Service can help the matching process after the initial match has been made.

It is important for the HIE to make sure they are not missing any data and to provide the patient with all the data they have available. As identity matching, authorization, and authentication develops more use cases through standardized FHIR resources, determining which organizations provide identity provisioning will become more clear.

Document Formatting - Payers

The new HITECH standard under the 21st Century Cures Act allows for more structure around key data components like the type of data that is sent in - specifically, data elements - as well as how the data is sent - in order, delineated through a stream, or through FHIR resources. This allows the form to be customized and sent in a much more user-friendly way, similar to how a claims form would be sent manually, except as an electronic submission.

We explained in the Proposed Rule that this definition of EHI includes, but is not limited to: Electronic protected health information and health information that is

created or received by a health care provider and those operating on their behalf; health plan; health care clearinghouse; public health authority; employer; life insurer; school; or university. In addition, we clarified that under our proposed definition, EHI includes, but is not limited to, electronic protected health information (ePHI) as defined in 45 CFR 160.103. We noted that EHI may also be provided, directly from an individual, or from technology that the individual has elected to use, to an actor covered by the information blocking provisions.[14]

This definition provides for an expansive set of EHI, which could include information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information.[15]

Da Vinci Project - Payers and Providers

The Da Vinci project has spearheaded the use of FHIR interoperability within the industry, with a bent towards the payer to provider collaborator aspect.

The core goal of the Da Vinci Project is to come up with standardized implementation guides with a focus on use cases and business challenges that would ensure better data flow between payers and providers. More specifically, members of the project ask the questions that point towards implementation guide standardization in order to create a more efficient backend data flow process that can truly impact care provider workflows. As a result of its close relationship with value-based care stakeholders, the HL7 Da Vinci Project is closely aligned with CMS rules.

Da Vinci's Approach Towards the Final Rule

A significant aspect of this project was the capability for various members of the HL7 community to invest resources into the development of FHIR workflows. Additionally, the ability to connect business challenges that occur between different groups (i.e., providers and payers) across the spectrum of organizations with different implementation capabilities is critically important as the implementations themselves continue to evolve.

When looking through the lens of the Da Vinci project, the core idea of how data flow and data equitability can be managed most effectively between payers and providers in accordance with the CMS rules is paramount.

[14] 85 FR 25803
[15] 84 FR 7513

The end result is an attempt to transform the healthcare industry away from large, transaction-based systems and into more nimble and modern API-based standards that ensure data liquidity for patients and patient-centered applications. This has helped to reduce the burden on providers and streamline care coordination, and will increasingly do so.

The CMS Interoperability and Patient Access final rule establishes policies that break down barriers in the nation's health system to enable better patient access to their health information, improve interoperability and unleash innovation, while reducing burden on payers and providers.[16]

Aid from federal partners and key industry players through beneficial regulations will help to accelerate the approach towards a more fully transformed and API-enabled healthcare IT ecosystem.

Critical Compliance Considerations - ISVs

As we noted before, from a compliance perspective, it is difficult to prescribe specifically what companies need to do as implementing interoperability in healthcare continues to evolve with new use cases being brought into the fold.

At the moment, developers and ISVs should understand and take into account several of the major regulatory and technical barriers that exist that are currently impeding the high level infrastructure of healthcare portability. Consistent rules that help to standardize specific processes along data flow will result in base standards and best practices that organizations can refer to when developing new app capabilities.

Other key considerations will need to include looking at the CMS and ONC regulations from a perspective that seeks to utilize a framework that enables organizations to free up data once authorization and authentication are granted to the end user.

Clinical Workflow - Payers and Providers

As a result of the shift towards value based care as well as the CMS emphasis on patient access to data, developers have the opportunity to innovate and provide real time access to ease workflows and administrative burden.

Prior Authorization - CMS - Payers and Providers

[16] *Interoperability and Patient Access Fact Sheet.* CMS. March 9th, 2020.

A more transparent clinical workflow takes into account prior authorization and what the actual benefits of the patient are during the clinical care process. What is happening upstream of this process includes:

- What is required to go from step 1 to step 2 in a prescribing event
    - What documentation requirements are necessary
        - Information about the patient's health status and benefit consumption status is during the health plan's year-long duration
        - When the prior authorization needs to be completed in the care cycle
    - What benefits are in place for the patient to receive the proper care

Electronic prior authorizations via FHIR also support the automation of data collection required for payer consideration. Unpacking the current workflows and enabling more data flow thanks to a combination of CMS patient access regulations as well as FHIR readiness on behalf of vendors, payers, and providers can serve to open up the walled up EHR data silos.

Electronic prior authorization transactions will additionally support the automation of the collection of data required for PA consideration, allowing a health IT developer to systemically pull data from a patient's medical record.[17]

Care Gap Quality Improvement

As with prior authorization, care quality relies on clinical workflows that can be made more efficient, with a more robust approach towards data flow. Once the gaps have been identified, the ability to share data across groups from payer to provider becomes essential.

The process for data exchange for quality measures (DEQM) is typically very burdensome and requires nurses and MAs (medical assistants) to determine whether certain data from status documents has been accounted for across multiple systems and file formats. The work, however, is extremely important as they have the ability to close gaps in healthcare that can lead to increased provider efficiency and a push towards VBC.

Based on the data reconciled and incorporated, the technology must be able to create a file formatted according to the standard specified in § 170.205(a)(4) using the Continuity of Care Document template and the standard specified in § 170.205(a)(5) on and after May 2, 2022.[18]

Da Vinci worked with Rush Health Systems and Cigna to leverage clinical data in order to augment HEDIS (Healthcare Effectiveness Data and Information Set) calculations to embark on FHIR efforts with the goal of transmitting clinical data at the point in time where it was necessary

[17] 85 FR 25685
[18] 85 FR 25942

for the workflow. Gaps in the care flow lead to lost opportunities to provide patient care for whatever benefits are required on behalf of the payer. This also detracts from the payers ability to become an interoperable entity and comply with stipulations of the Final Rule.

The technical implementation of the workflow from the Rush Health perspective involves:

1. Event notification and handoff between partners
2. Patient discharge and information sent to Rush Internal HIE
3. Follow up visit with care provider
4. Care provider attests medical reconciliation to the HIE
5. Rush checks to see if the patient is within the cohort of Cigna members

The technical implementation of the workflow from the Cigna perspective is:

1. Assemble patient level clinical quality measure (CQM) and supporting clinical evidence FHIR data element bundle
2. Data assigned to clinical database
3. Data fed through existing data pipelines to use as supplemental source for clinical quality analytics
4. Notification returns to Rush Health that Cigna has received particular member data

Foundational data sets for VBC success include member, provider, claims, and clinical data. Standardized interoperability between groups can lead to greater data flow discovery as well as uncovering missed opportunities where workflow simplification is possible.

Technological Implementation Clarification

While it is important for developers to understand and develop a FHIR API, the technology stack has no significance unless it is used in the context of the FHIR implementation guide that takes the user workflow into account. A consideration of key actors, roles, and workflow will need to be made prior to product development.

The true value of the product will be determined when an implementation guide is combined with USCDI to benefit a specific use case to solve a specific business problem once it has been identified.

FAST (FHIR At Scale Task Force)

Two critical hindrances to interoperability are the FHIR scalability gaps and barriers to FHIR adoption. The goal of FAST is to come up with solutions to technical barriers including:

- FHIR Endpoint Directory Services
- Patient and Provider Identity Management
- Security
- Exchange Process

- Testing, Conformance, and Certification
- Versioning
- Scaling

Addressing these issues in the right way at the start of development can lead to rapid deployment and rapid adoption of FHIR-based products in the marketplace. Da Vinci use cases like that above with Cigna and Rush Health are outliers that have nimble systems in place to enable FHIR readiness. Most organizations take much longer to adopt FHIR backend APIs due to the issues involving the technical barriers noted above. The lack of standardization and scalability in these areas slows adoption in the majority of the marketplace.

Often, different actors within the workflow are affected by different technical systems that act as barriers noted above. Actors on one side will make a request through systems to get corresponding information from the other side, whether it be patient identification or authorization and authentication.

The **ONC's FAST Tiger Team** plan is to work through specific use cases where the technical barrier friction is significant. From here, individual Tiger Team workstreams can focus on core capabilities that cut across use cases and solve for the technical problem where it is most acute.

The "Directory" Tiger Team currently deals with multiple endpoint locations as well as a lack of authoritative provider source information that can anchor FHIR endpoints. As noted above, there is no true authoritative location where data can be stored that is standardized across payers, providers, and vendors. The ideal future state is for there to be one authoritative national directory for an organization specific information: providers, payers, and applications. Note the federated model mentioned above in the "Patient Matching and Identity Management" section.

Thus, any action by an actor to restrict the public availability of URLs in support of patient access would be more than just likely to interfere with the access, exchange, or use of EHI; it would prevent such access, exchange, and use. Accordingly, as noted in § 170.404(b)(2), a Certified API Developer must publish FHIR service base URLs for certified API technology that can be used by patients to access their electronic health information.[19]

The "Security" tiger team focuses on scalable solutions around authorization and authentication processes.

Building a proof of concept that demonstrates the technical ability to implement user authorization and authentication at "point of request" while "granting" and maintaining credentials at scale are deliverables the tiger team is currently working on. Delivering national standards will be key here in order to comply with the Final Rule.

[19] 85 FR 25813

Current scaling solutions are a technical barrier, since they don't have the capacity to handle anticipated volume and response time requirements. Additionally, a lack of organizational experience using FHIR to handle data exchanges and endpoint discoverability serves as a hindrance to properly scaling FHIR resource processes.

Recommended future state for a properly scaled approach to the FHIR standard is a "mixed model" of interoperability (point to point, gateways, and intermediaries). Establishing minimum application performance requirements as well as supporting metadata for routing through intermediaries will be ideal future state steps towards reducing this technical burden.

Testing and Certification Tiger Teams' major deliverables involve coming up with the minimum level of conformance organizations need in order to participate in the scaled FHIR ecosystem. Additionally, they include testing the specifications that will lead to certification of an organization that assures compliance with respect to the FHIR task force. One of the most important aspects of the team, however, are the proofs of concepts that will ultimately test the scale across multiple organizations and stakeholders using FHIR products at various stages of maturity.

Current barriers to testing and certification include:

- Requirements: Documentation of requirements that provides a clear roadmap towards scalability success.

- Contingencies: Barriers towards integration of applicable FHIR implementation guides.

- Tooling: Independent FHIR development validation through automated tooling for conformance to current standards. See "Inferno".

- Versioning: Developing a successful testing and certification program that is nimble enough for continuous technological evolution.

- Timing: Encouraging the use of FAST Core Competency Requirements to test FHIR clients and servers on a regular basis during development as well as in use with key stakeholders in the industry.

Successful real world testing, according to ONC Final Rule stipulations, includes:

- *The certified health IT continues to be compliant to the full scope of the certification criteria to which it is certified, including the required technical standards and vocabulary codes set;*

- *The certified health IT is exchanging electronic health information in the care and practice settings for which it is intended for use; and*
- *Electronic health information is received by and used in the certified health IT.*[20]

While understanding the FAST approach can be extremely useful for the Health IT application developer, the content provided within this whitepaper only touches the surface of the totality of delivering FHIR solutions at scale. Individuals more interested in taking a deeper dive into the intricacies involved can join in on lively discussions as the project is ever evolving at the ONC Project Tracking portal for the taskforce.

Conclusion:

The Final Rule on Interoperability and Information Blocking from ONC and CMS is a huge leap forward in bringing out the inherent capabilities that exist across patient access, bulk data access, authorization, and authentication of healthcare IT systems.

Developers are advised to keep abreast of developments in the space as it evolves as a result of additional use cases, as well as the evolution of new technological standards, in particular the expansion of TEFCA, USCDI and FHIR.

While the ambiguities in the rule may seem like a major hindrance to compliance, understanding that they are there to make room for innovation is a perspective that can help product developers as they move to innovate within the marketplace.

The siloing of data has been an unfortunate byproduct of healthcare privacy rules. The emphasis on patient access from regulatory bodies and key industry players, however, will help to begin a new era - one that is focused on digital transformation. While the major conflicts between data sharing and data privacy in the healthcare industry remain intertwined, the early adoption of FHIR specific FHIR implementation guides, even at the smallest use case level, has shown how much more efficient a nimble, API-backed hospital administration can be.

Developing scalable FHIR standards that provide a nationalized framework around data transfer will begin a period of rapid deployment of technical interoperability implementations across numerous healthcare systems across the country. This will only serve as an impetus for developers to continue to innovate around products that help to better optimize patient care.

[20] 84 FR 7495

At A Glance: Final Rule Conditions of Certification

As the Final Rule is exhaustive in terms of its conditions of certifications, this chart may be helpful in providing organizations with some high-level guidance on what functionalities they should be prepared to implement in their systems.

Note: Many of these conditions of certification are interwoven amongst many areas and are subject to change over time as more technology is implemented. Developers are encouraged to consult with their legal counsel on the final word on their compliance obligations.

Organizational Role	SMART on FHIR for Patient Access	Bulk Data Access[21]	US Core	CARIN Blue Button[22]	Da Vinci PDEX	Da Vinci Drug Formulary	Data Segmentation For Privacy (C-CDA)	Quality Reporting Document Architecture
Payer	YES	YES	YES	YES	YES	YES	YES	YES
Provider	YES	YES	YES	YES	YES	N/A	YES	YES
EHR Vendor	YES	YES	YES	YES	YES	YES	YES	YES
HIE	YES	YES	YES	N/A	YES	N/A	YES	CMS DRAFT 2021[23]
Public Health Agency	YES	YES	YES	N/A	N/A	N/A	YES	CMS DRAFT 2021
Third Party Application	YES	YES	YES	YES	YES	YES[24]	YES[25]	N/A
Laboratory	YES	N/A	YES	N/A	YES	N/A	YES	YES
Medical Registry	YES	YES	YES	N/A	N/A	N/A	N/A	YES
Regulatory Agency	YES	YES	YES	YES	N/A	YES	YES	YES

[21] API Certification Guideline Criteria for the “Data Consistency and Raw Data” ambiguity. (pg. 10)
[22] Note “Application and Service Validation” ambiguity alongside “Right to Access” Rule. (pg. 9)
[23] CMS Implementation Guide for 2021
[24] Plan-level data only.
[25] “Security labeling is an essential technology to ensure patient’s privacy will be protected in the face of many new types of users and burgeoning new applications for health information.” Also See “CARIN Alliance”(pg.9) according to “Application and Service Validation” ambiguity.

GLOSSARY

Implementation guide (IG)

A set of rules or constraints on how a given set of FHIR resource types can be used to address a use case. This can be anything from implementing US Core Data in FHIR to creating basic reports. It includes associated documentation to support and clarify usage. These can range from profiles on resources to customized operations like bulk transfer of data.

The FHIR specification has created an ecosystem for national standards, vendor consortiums, clinical societies, and others to publish IGs that define how an organization develops an API and conforms the server to the implementation guide to solve a certain problem or meet a particular criterion.

Fast Healthcare Interoperability Resources (FHIR)

Standard for describing data formats and elements and an API for the exchange of electronic health records. The standard builds on previous HL7 data formats and provides an alternative to document-centric health record standardization by retrieving data elements via URL. The goal is to facilitate interoperability and make it easier for patients to access healthcare information through third-party applications via application programming interface (API) connectivity.

SMART on FHIR

SMART (Suitable Medical Applications, Reusable Technologies) on FHIR defines a way for health applications to connect to EHR systems according to clinical and contextual data. It uses appropriate security and authorization guarantees using OAuth2.0-based protocol from OpenID Connect to approve third party SMART apps for access to specific data sets from a service provider (EHR).