The Office of the National Coordinator for Health Information Technology

A User's Guide to Understanding

The Draft Trusted Exchange Framework

What is the Trusted Exchange Framework?

Why did Congress require the Trusted Exchange Framework?

Who can use the Trusted Exchange Framework?

What are the benefits of the Trusted Exchange Framework?

How will the Trusted Exchange Framework work?

What use cases are covered under the Trusted Exchange Framework?

What fees can be charged under the Trusted Exchange Framework?

What privacy and security protections does the Trusted Exchange Framework guarantee?

When will it be implemented?

VISIT HTTPS://WWW.HEALTHIT.GOV/SITES/DEFAULT/FILES/DRAFT-TRUSTED-EXCHANGE-FRAMEWORK.PDF TO VIEW THE COMPLETE TRUSTED EXCHANGE FRAMEWORK DOCUMENT.

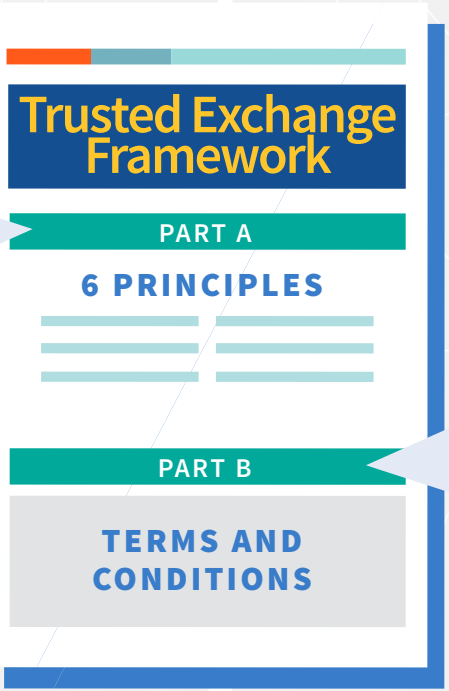
What is the Draft Trusted Exchange Framework?

Format of the Draft Trusted Exchange Framework

Part A—Principles for Trusted Exchange

General principles that provide guardrails to engender trust between Health Information Networks (HINs). Six (6) categories:

- **Principle 1 - Standardization:** Adhere to industry and federally recognized standards, policies, best practices, and procedures.
- **Principle 2 - Transparency:** Conduct all exchange openly and transparently.
- **Principle 3 - Cooperation and Non-Discrimination:** Collaborate with stakeholders across the continuum of care to exchange electronic health information, even when a stakeholder may be a business competitor.
- **Principle 4 - Security and Patient Safety:** Exchange electronic health information securely and in a manner that promotes patient safety and ensures data integrity.
- **Principle 5 - Access:** Ensure that patients and their caregivers have easy access to their electronic health information.
- **Principle 6 - Data-driven Accountability:** Exchange multiple records at one time to enable identification and trending of data to lower the cost of care and improve the health of the population.



Part B—Minimum Required Terms and Conditions for Trusted Exchange

A minimum set of terms and conditions for the purpose of ensuring that common practices are in place and required of all participants who participate in the Trusted Exchange Framework, including:

- Common authentication processes of trusted health information network participants;
- A common set of rules for trusted exchange;
- A minimum core set of organizational and operational policies to enable the exchange of electronic health information among networks.

Why did Congress require the Trusted Exchange Framework?

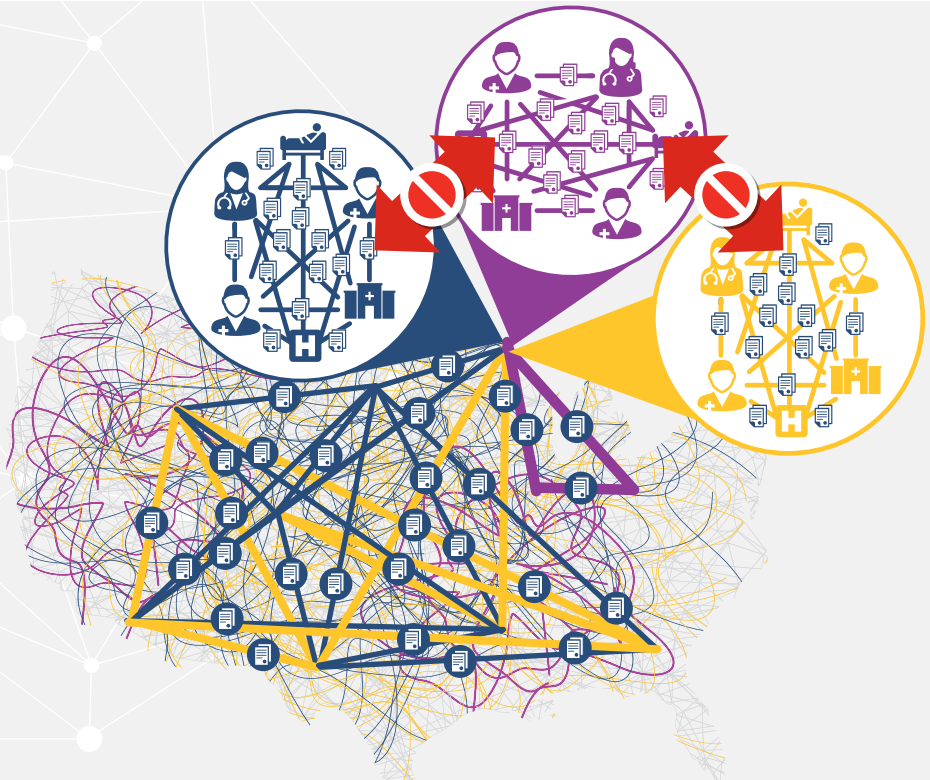
Need for the Trusted Exchange Framework – Complexity

Current Proliferation of Agreements

Many organizations have to join multiple Health Information Networks (HINs), and the HINs do not share data with each other.

Trusted exchange must be simplified in order to scale.

Each line color on the map represents a different network.
There are well over 100 networks in the U.S.



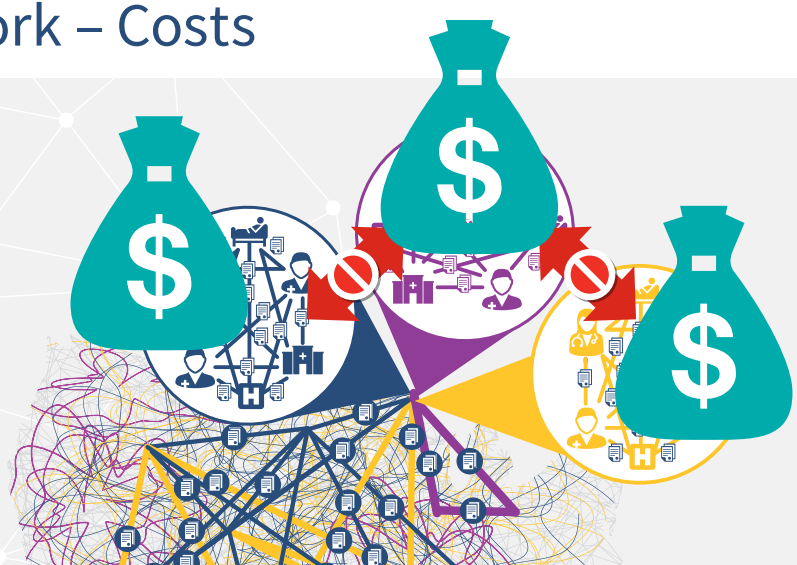
Why did Congress require the Trusted Exchange Framework?

Need for the Trusted Exchange Framework – Costs

Costs to healthcare providers due to lack of a Trusted Exchange Framework

Healthcare organizations are currently burdened with creating many costly, point-to-point interfaces between organizations.

The Trusted Exchange Framework will significantly reduce the need for individual interfaces, which are costly, complex to create and maintain, and an inefficient use of provider and health IT developer resources.



Proliferation of Interoperability Methods

Based on a pilot survey of roughly 70 hospitals:

Few hospitals used only one interoperability method.

- A majority of hospitals required three or more methods
- About three in 10 used five or more methods

Rated their own Interoperability as…

63% Not or a little bit interoperable

17% Somewhat interoperable

19% Largely or Fully interoperable

Why did Congress require the Trusted Exchange Framework?

Trusted Exchange Framework and Common Agreement

21st Century Cures Act - Section 4003(b)

"Not later than 6 months after the date of enactment of the 21st Century Cures Act, the National Coordinator shall convene appropriate public and private stakeholders to develop or support a trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information networks. The common agreement may include—

"(I) a common method for authenticating trusted health information network participants;

"(II) a common set of rules for trusted exchange;

"(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and

"(IV) a process for filing and adjudicating noncompliance with the terms of the common agreement."

21st Century Cures Act - Section 4003(c)

"Not later than 1 year after convening stakeholders…the National Coordinator shall publish on its public Internet website, and in the Federal register, the trusted exchange framework and common agreement developed or supported under paragraph B…"

Why did Congress require the Trusted Exchange Framework?

Goals of the Draft Trusted Exchange Framework

GOAL 1

Build on and extend existing work done by the industry

The Draft Trusted Exchange Framework recognizes and builds upon the significant work done by the industry over the last few years to broaden the exchange of data, build trust frameworks, and develop participation agreements that enable providers to exchange data across organizational boundaries.

GOAL 2

Provide a single "on-ramp" to interoperability for all

The Draft Trusted Exchange Framework provides a single "on-ramp" to allow all types of healthcare stakeholders to join any health information network they choose and be able to participate in nationwide exchange regardless of what health IT developer they use, health information exchange or network they contract with, or where the patients' records are located.

GOAL 3

Be scalable to support the entire nation

The Draft Trusted Exchange Framework aims to scale interoperability nationwide both technologically and procedurally, by defining a floor, which will enable stakeholders to access, exchange, and use relevant electronic health information across disparate networks and sharing arrangements.

GOAL 4

Build a competitive market allowing all to compete on data services

Easing the flow of data will allow new and innovative technologies to enter the market and build competitive, invaluable services that make use of the data.

GOAL 5

Achieve long-term sustainability

By providing a single "on-ramp" to nationwide interoperability while also allowing for variation around a broader set of use cases, the Draft Trusted Exchange Framework ensures the long-term sustainability of its participants and end-users.

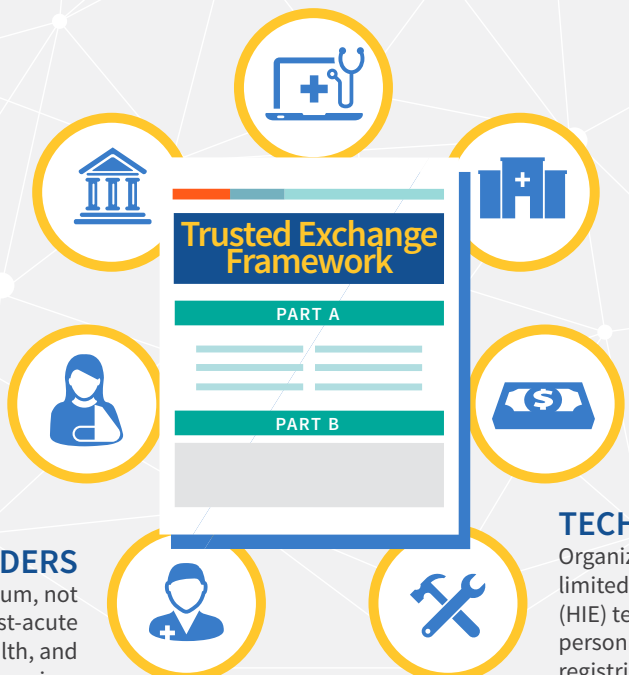
Who can use the Trusted Exchange Framework?

Stakeholders who can use the Trusted Exchange Framework

HEALTH INFORMATION NETWORKS

FEDERAL AGENCIES
Federal, state, tribal, and local governments

PUBLIC HEALTH
Public and private organizations and agencies working collectively to prevent, promote and protect the health of communities by supporting efforts around essential public health services



INDIVIDUALS
Patients, caregivers, authorized representatives, and family members serving in a non-professional role

PAYERS
Private payers, employers, and public payers that pay for programs like Medicare, Medicaid, and TRICARE

PROVIDERS
Professional care providers who deliver care across the continuum, not limited to but including ambulatory, inpatient, long-term and post-acute care (LTPAC), emergency medical services (EMS), behavioral health, and home and community based services

TECHNOLOGY DEVELOPERS
Organizations that provide health IT capabilities, including but not limited to electronic health records, health information exchange (HIE) technology, analytics products, laboratory information systems, personal health records, Qualified Clinical Data Registries (QCDRs), registries, pharmacy systems, mobile technology, and other technology that provides health IT capabilities and services

Who can use the Trusted Exchange Framework?

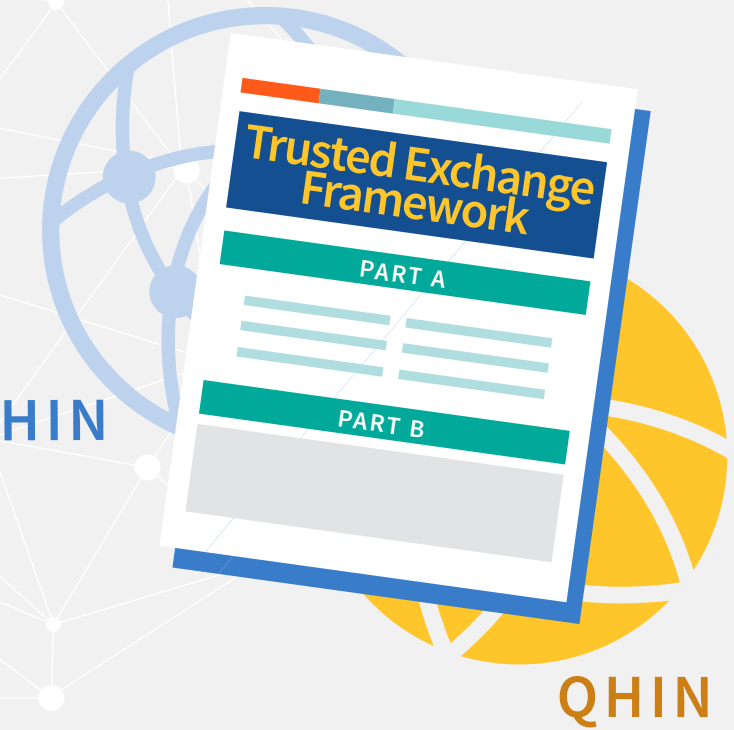
Defining Terms: Who is the Trusted Exchange Framework applicable to?

The Trusted Exchange Framework aims to create a technical and governance infrastructure that connects

Health Information Networks

together through a core of

Qualified Health Information Networks.



Who can use the Trusted Exchange Framework?

What is a Health Information Network?

Health Information Networks (HINs) are an Individual or Entity that:

1. Determines, oversees, or administers policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities;
2. Provides, manages, or controls any technology or service that enables or facilitates the exchange of electronic health information between or among two or more unaffiliated individuals or entities; or
3. Exercises substantial influence or control with respect to the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

Who can use the Trusted Exchange Framework?

What is a Qualified Health Information Network?

A Qualified Health Information Network (Qualified HIN) must meet ALL of the requirements of a HIN. In addition, it must also:

- Be able to locate and transmit ePHI between multiple persons and/or entities electronically;
- Have mechanisms in place to impose Minimum Core Obligations and to audit Participants' compliance;
- Have controls and utilize a Connectivity Broker service;
- Be participant neutral; and
- Have Participants that are actively exchanging the data included in the USCDI in a live clinical environment.

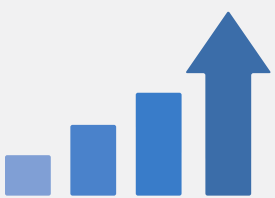
What are the benefits of the Trusted Exchange Framework?

Trusted Exchange Framework Benefits for HINs

For Qualified HINs and HINs the Trusted Exchange Framework will:

Give HINs and their participants access to more data on the patients they currently serve.

» This will enhance care coordination and care delivery use cases.



The Trusted Exchange Framework ensures that there is no limitation to the aggregation of data that is exchanged among Participants.

» This will allow organizations, including Health IT Developers, HINs, QCDRs, and other registries to use the Trusted Exchange Framework to obtain clinical data from providers and provide analytics services. (Note that appropriate BAs must be in place between the healthcare provider and analytics provider.)

What are the benefits of the Trusted Exchange Framework?

Trusted Exchange Framework Benefits for Providers

For Health Systems and Ambulatory Providers the Trusted Exchange Framework will:

Enable them to join one network and have access to data on the patients they serve regardless of where the patient went for care.

» This enables safer, more effective care, and better care coordination.

Enable them to eliminate one off and point-to –point interfaces

» This will allow providers and health systems to more easily work with third parties, such as analytics products, care coordination services, HINs, Qualified Clinical Data Registries (QCDRs), and other registries. (Note that appropriate BAs must be in place between the healthcare provider and analytics provider.)

What are the benefits of the Trusted Exchange Framework?

Trusted Exchange Framework Benefits for Patients

For Patients and Their Caregivers, the Trusted Exchange Framework will:

Enable them to find all of their health information from across the care continuum, even if they don't remember the name of the provider they saw.

» This enables patients and their caregivers to participate in their care and manage their health information.

How will the Trusted Exchange Framework work?

Recognized Coordinating Entity (RCE)

Recognized Coordinating Entity

The RCE is the entity selected by ONC that will enter into agreements with HINs that qualify and elect to become Qualified HINs in order to impose, at a minimum, the requirements of the Common Agreement set forth herein on the Qualified HINs and administer such requirements on an ongoing basis as described herein.

The RCE will act as a governance body that will operationalize the Trusted Exchange Framework by incorporating it into a single, all-encompassing Common Agreement to which Qualified HINs will agree to abide. In its capacity as a governance body, the RCE will be expected to monitor Qualified HINs compliance with the final TEFCA and take actions to remediate non-conformity and non-compliance by Qualified HINs, up to and including the removal of a Qualified HIN from the final TEFCA and subsequent reporting of its removal to ONC.

The RCE will also be expected to work collaboratively with stakeholders from across the industry to build and implement new use cases that can use the final TEFCA as their foundation, and appropriately update the TEFCA over time to account for new technologies, policies, and use cases.

READ MORE: How will it Work?

How will the Trusted Exchange Framework work?

Recognized Coordinating Entity (RCE)

2018 Selection

Process for Recognizing Entity

ONC will release an open, competitive Funding Opportunity Announcement (FOA) in spring 2018 to award a single multi-year Cooperative Agreement to a private sector organization or entity. The RCE will need to have experience with building multi-stakeholder collaborations and implementing governance principles in order to be eligible to apply for the Cooperative Agreement.

Expectations for Entity

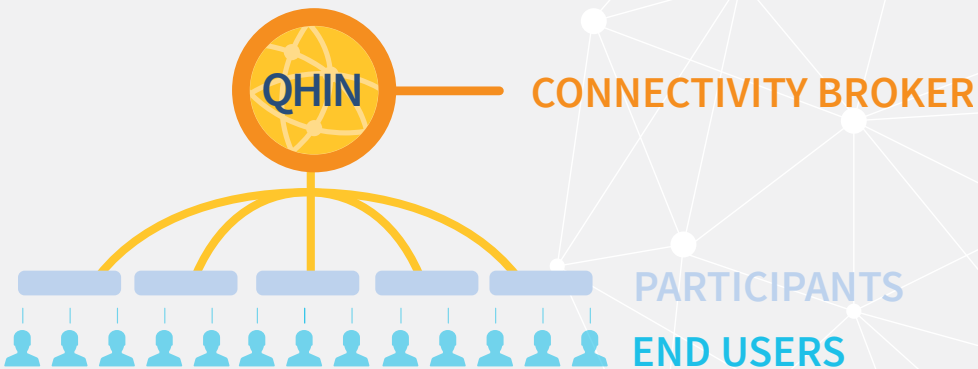
ONC will work with the RCE to incorporate the Trusted Exchange Framework into a single Common Agreement to which Qualified HINs and their participants voluntarily agree to adhere.

The RCE will have oversight, enforcement, and governance responsibilities for each of the Qualified HINs who voluntarily adopt the final TEFCA.

READ MORE: How will it Work?

How will the Trusted Exchange Framework work?

Structure of a Qualified Health Information Network



READ MORE: QHINs in Part B, Section 2

READ MORE: Connectivity Broker Capabilities in Part B, Section 3

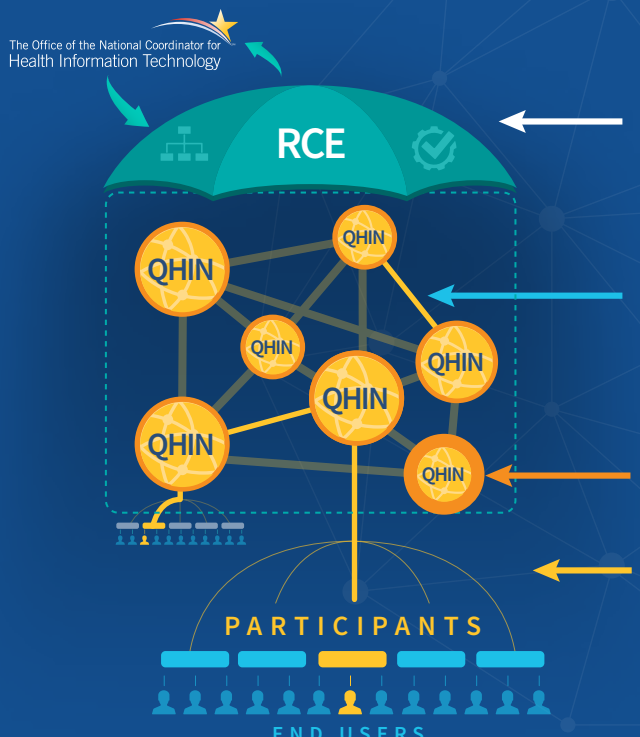
A **Qualified HIN (QHIN)** is a network of organizations working together to share data. QHINs will connect directly to each other to ensure interoperability between the networks they represent.

A **Connectivity Broker** is a service provided by a Qualified HIN that provides all of the following functions with respect to all Permitted Purposes: master patient index (federated or centralized); Record Locator Service; Broadcast and Directed Queries, and eHI return to an authorized requesting Qualified HIN.

A **Participant** is a person or entity that participates in the QHIN. Participants connect to each other through the QHIN, and they access organizations not included in their QHIN through QHIN-to-QHIN connectivity. Participants can be HINs, EHR vendors, and other types of organizations.

An **End User** is an individual or organization using the services of a Participant to send and/or receive electronic health info.

How will the Trusted Exchange Framework Work?



RCE provides oversight and governance for Qualified HINs.

Qualified HINs connect directly to each other to serve as the core for nationwide interoperability.

QHINs connect via connectivity brokers.

Each Qualified HIN represents a variety of networks and participants that they connect together, serving a wide range of end users.

READ MORE: QHINs in Part B, Section 2

READ MORE: Connectivity Broker Capabilities in Part B, Section 3

How will the Trusted Exchange Framework work?

Qualified HIN Requirements Clarifications

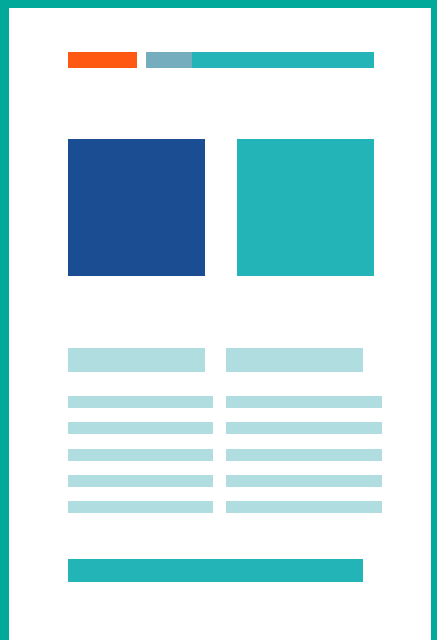
Included

- A minimum floor in the areas where there is currently variation between HINs that causes a lack of interoperability.
- Obligation to respond to Broadcast or Directed Queries for all the Permitted Purposes outlined in the Trusted Exchange Framework.
- Qualified HINs must exchange all of the data specified in the USCDI to the extent such data is then available and has been requested.
- Base set of expectations for how Qualified Health Information Networks connect with each other.

Not Included

- A full end-to-end agreement that would be a net new agreement.
- No expectation that every HIN will serve same constituents or use cases. (i.e. no requirement that Qualified HINs initiate Broadcast or Directed Queries for all of the Permitted Purposes outlined in the Trusted Exchange Framework)
- Not dictating internal technology or infrastructure requirements.
- No limitation on additional agreements to support uses cases other than Broadcast Query and Directed Query for the Trusted Exchange Framework specified permitted purposes.

TRUSTED EXCHANGE FRAMEWORK CONTENTS



What use cases are covered under the Trusted Exchange Framework?

Permitted Purposes

READ MORE: Part B, Section 1

What use cases are covered under the Trusted Exchange Framework?

Use Cases

Broadcast Query

Sending a request for a patient's Electronic Health Information (EHI) to all Qualified HINs to have data returned from all organizations who have it.

Supports situations where it is unknown who may have Electronic Health Information about a patient.

READ MORE: Broadcast and Directed Queries- Part B, Section 5.4 and Section 3

Directed Query

Sending a targeted request for a patient's Electronic Health Information to a specific organization(s).

Supports situations where you want specific Electronic Health Information about a patient, for example data from a particular specialist.

Population Level Data

Querying and retrieving Electronic Health Information about multiple patients in a single query.

Supports population health services, such as quality measurement, risk analysis, and other analytics.

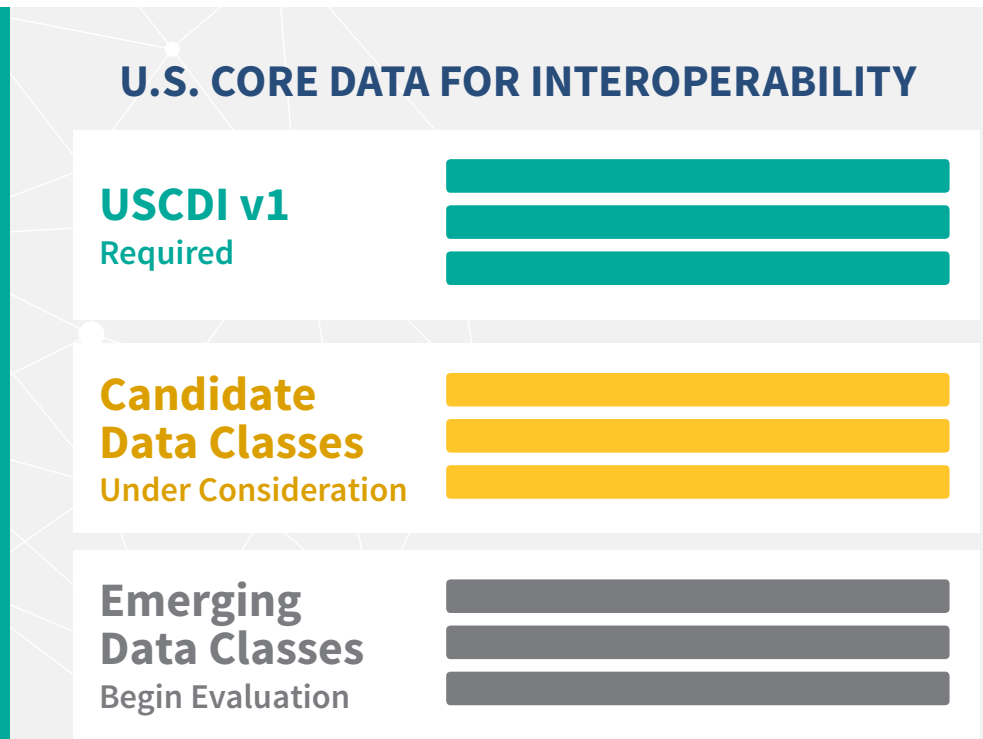
READ MORE: Population level data- Part B, Section 8

What use cases are covered under the Trusted Exchange Framework?

US Core Data for Interoperability (USCDI) Glide Path

The USCDI (https://www.healthit.gov/sites/default/files/draft-uscdi.pdf) 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 plus Clinical Notes and Provenance
2. Candidate Data Classes—Under consideration for USCDI v2
3. Emerging Data Classes– Begin evaluating for candidate status



What use cases are covered under the Trusted Exchange Framework?

Expansion of US Core Data for Interoperability (USCDI)

As the USCDI expands, Qualified HINs and their Participants will be required to upgrade their technology to support the data specified in the USCDI.

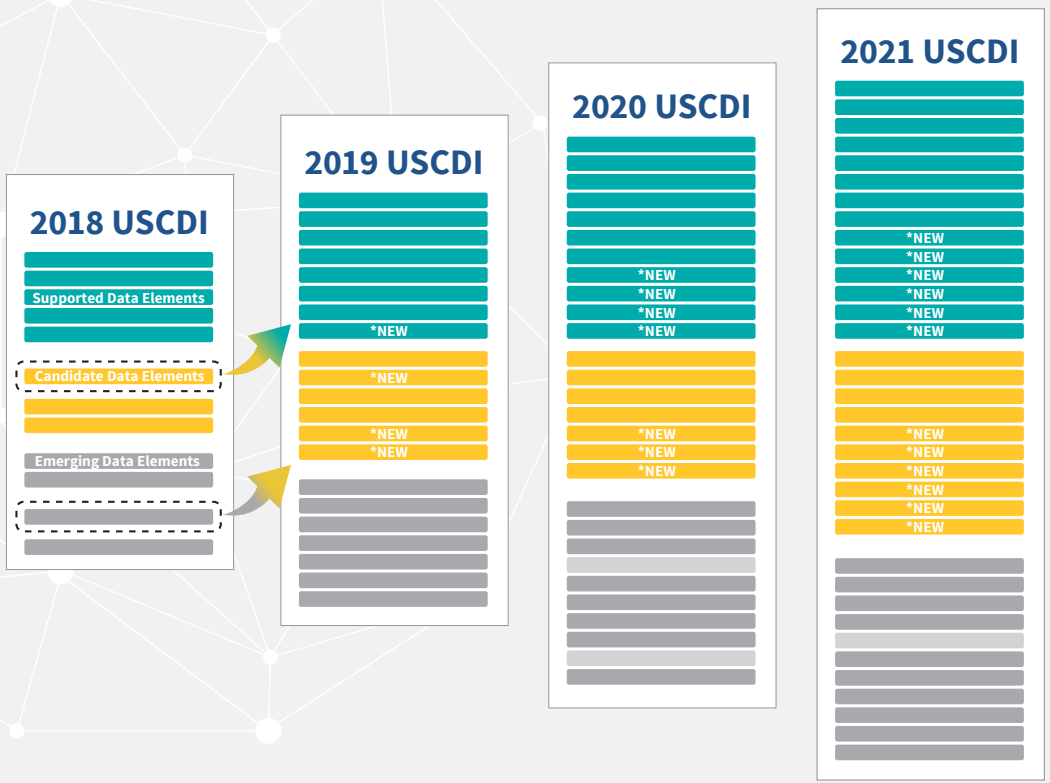
Some Candidates will be Accepted to USCDI

Some Candidates Require Further Work

Some Emerging Elements Become Candidates

Some Require Further Work

https://www.healthit.gov/sites/default/files/draft-uscdi.pdf



What fees can be charged under the Trusted Exchange Framework?

Attributable Costs and Services

Qualified HINs may, though they are not required to, charge attributable service costs to other Qualified HINs, provided they are reasonable and non-discriminatory.

Reasonable Allowable Costs: are costs that were actually incurred; are a direct cost or a reasonable allocation of indirect costs for the attributable services below; are based on objective and verifiable criteria; and are not variable depending on which Qualified HIN is being charged

Attributable Services may include:

- Developing or modifying interfaces or APIs to be able to exchange data in the USCDI;
- Developing or revising the Connectivity Broker required in the Trusted Exchange Framework; and
- Employing legal services necessary to review the Trusted Exchange Framework and amend participation and Business Associate agreements to meet the requirements of the Trusted Exchange Framework.

READ MORE: Fees- Part B, Section 5.3

What privacy and security protections does the Trusted Exchange Framework guarantee?

Definitions

Participant

A person or entity that participates in a Qualified HIN

READ MORE: Participant obligations- Part B, Section 9

End User

An individual or organization using the services of a Participant to send and/or receive electronic health info

READ MORE: End User obligations- Part B, Section 10

Individual

A patient or their authorized representative

READ MORE: Individuals- Part B, Section 6.1.1 and 7.2

What privacy and security protections does the Trusted Exchange Framework guarantee?

Privacy/Security: Identity Proofing

Identity proofing is the process of verifying a person is who they claim to be. The Trusted Exchange Framework requires identity proofing (referred to as the Identity Assurance Level (IAL) in SP 800-63A).

End Users and Participants

Each Qualified HIN shall require proof of identity for Participants and participating End Users at a minimum of IAL2 prior to issuance of credentials.

Individuals

Each Qualified HIN shall require its End Users and Participants to proof the identity for Individuals at a minimum of IAL2 prior to issuance of credentials. Individuals must provide strong evidence of their identity.

IAL 2 REQUIREMENT	DESCRIPTION
Evidence	» One (1) piece of SUPERIOR or STRONG evidence; OR » Two (2) pieces of STRONG evidence; OR » One (1) piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence
Validation	» Each piece of evidence must be validated with a process able to achieve the same strength as the evidence presented. » Validation against a third-party data service SHALL only be used for one piece of presented identity evidence.
Address Confirmation	» The Credential Service Provider (CSP) SHALL confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence.

READ MORE:
Part B, Section 6.2.4

What privacy and security protections does the Trusted Exchange Framework guarantee?

Privacy/Security: Identity Proofing - EXCEPTIONS

Qualified HINs, Participants, or End Users are responsible for proofing Individuals at the IAL2 level, HOWEVER:

Trusted Referee and Authoritative Source

In instances where the individual enrolling cannot meet the identity evidence requirements specified, organization staff may act as a trusted referee, allowing them to use personal knowledge of the identity of patients when enrolling patients as subscribers to assist in identity proofing the enrollee.

Individual presents for treatment

End Users and Participants must collect and validate Evidence of Identity

PREFERRED

Alternative Acceptable Forms of Identity Validation

- Personal Knowledge
- Previous Treatment

Sucessful Identity Proof

READ MORE: Part B, Section 6.2.4

Antecedent Event

Staff may also act as authoritative sources by using knowledge of the identity of the individuals (e.g., physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges) collected during an antecedent, in-person registration event.

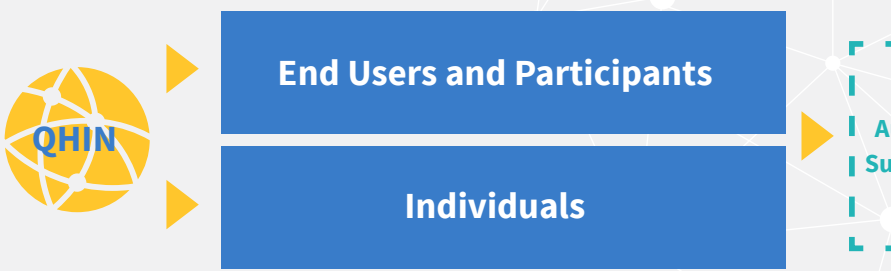
For example, IAL2 identity proofing for an Individual can be accomplished by two of the following:

1. Physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges,
2. Comparison to information from an insurance card that has been validated with the issuer, e.g., in an eligibility check within two days of the proofing event, and
3. Comparison to information from an electronic health record (EHR) containing information entered from prior encounters.

What privacy and security protections does the Trusted Exchange Framework guarantee?

Privacy/Security: Authentication

Digital authentication is the process of establishing confidence in a remote user identity communicating electronically to an information system. NIST draft SP 800-63B refers to the level of assurance in authentication as the Authenticator Assurance Level (AAL). Federal Assurance Level (FAL) refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).



Each Qualified HIN shall authenticate End Users, Participants, and Individuals at a minimum of AAL2, and provide support for at least FAL2 or, alternatively, FAL3.

Connecting to a Qualified HIN or one of its Participant will require **two-factor authentication**. A list of acceptable second factors (in addition to a username and password) can be found at https://pages.nist.gov/800-63-3/sp800-63b/sec4_aal.html.

READ MORE: Part B, Section 6.2.5

What privacy and security protections does the Trusted Exchange Framework guarantee?

Privacy/Security-Breach Notifications and CUI

Breach Notification Regulations

"The Qualified HIN shall comply with all applicable Breach notification requirements pursuant to 45 CFR §164.402 of the HIPAA Regulations which addresses Breach notification. The Qualified HIN further shall notify, in writing, the Recognized Coordinating Entity without unreasonable delay, but no later than fifteen (15) calendar days, after Discovery of the Breach in order to allow other affected parties to satisfy their reporting obligations. Upon receipt of such notice, the Recognized Coordinating Entity shall be responsible for notifying, in writing, other Qualified HINs affected by the Breach within seven (7) calendar days."

Controlled Unclassified Information (CUI)

"Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls" (32 C.F.R. § 2002.4(h))."

READ MORE: Breach Notification- Part B, Section 6.1.3 and 6.1.5

When will the Trusted Exchange Framework be implemented?

Timeline