The Office of the National Coordinator for Health Information Technology

Health IT Advisory Committee

# Trusted Exchange Framework Task Force
# First Meeting

Arien Malec, co-chair
Denise Webb, co-chair

February 20, 2018

# Membership

| Name | Organization | Role |
|---|---|---|
| Arien Malec | Change Healthcare | Co-Chair |
| Denise Webb | Marshfield Clinic Health System | Co-Chair |
| Carolyn Petersen | Mayo Clinic Global Business Solutions | HITAC Committee Member |
| Aaron Miri | Imprivata | HITAC Committee Member |
| John Kansky | Indiana Health Information Exchange | HITAC Committee Member |
| Sheryl Turney | Anthem Blue Cross Blue Shield | HITAC Committee Member |
| Sasha TerMaat | Epic | HITAC Committee Member |
| Steve Ready | Norton HealthCare | HITAC Committee Member |
| Cynthia Fisher | WaterRev, LLC | HITAC Committee Member |
| Anil Jain | IBM Watson | HITAC Committee Member |
| Kate Goodrich | CMS | HITAC Committee Member |
| David McCallie | Cerner | Public Member |
| Mark Savage | UC San Francisco | Public Member |
| Noam Arzt | HLN Consulting | Public Member |
| Grace Terrell | Envision Genomics, Inc. | Public Member |

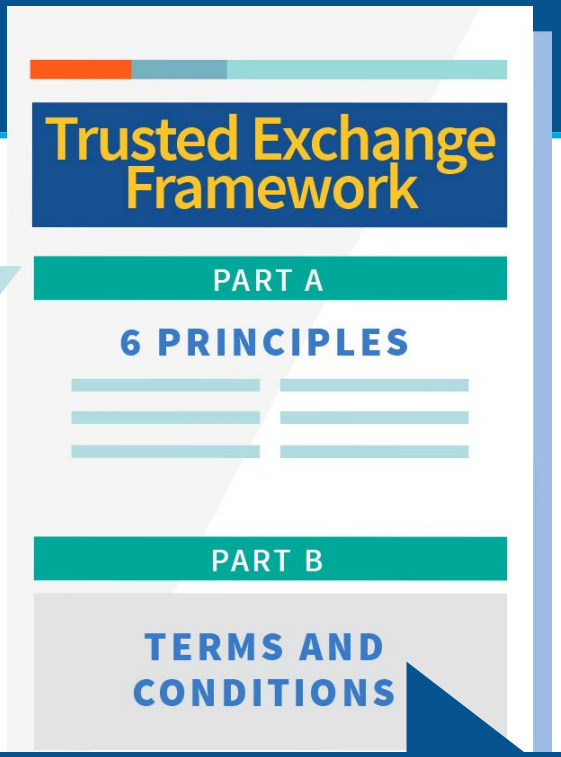
# Charge

- **Overarching charge:** The Trusted Exchange Framework Taskforce will develop and advance recommendations on Parts A and B of the Draft Trusted Exchange Framework to inform development of the final Trusted Exchange Framework and Common Agreement (TEFCA).
- **Detailed charge:** Make specific recommendations on the language included in the Minimum Required Terms and Conditions in Part B, including—
  - **Recognized Coordinating Entity:** Are there particular eligibility requirements for the Recognized Coordinating Entity (RCE) that ONC should consider when developing the Cooperative Agreement?
  - **Definition and Requirements of Qualified HINs:** Recommendations for further clarifying the eligibility requirements for Qualified HINs outlined in Part B.
  - **Permitted Uses and Disclosures:** Feedback on enhancing or clarifying the six (6) permitted purposes and three (3) use cases identified in Part B.
  - **Privacy/ Security:** Are there standards or technical requirements that ONC should specify for identity proofing and authentication, particularly of individuals?

The Office of the National Coordinator for Health Information Technology

# 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.

# Goals of the Draft Trusted Exchange Framework


### 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.

### 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.

### 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.

### Build a competitive market allowing all to compete on data services

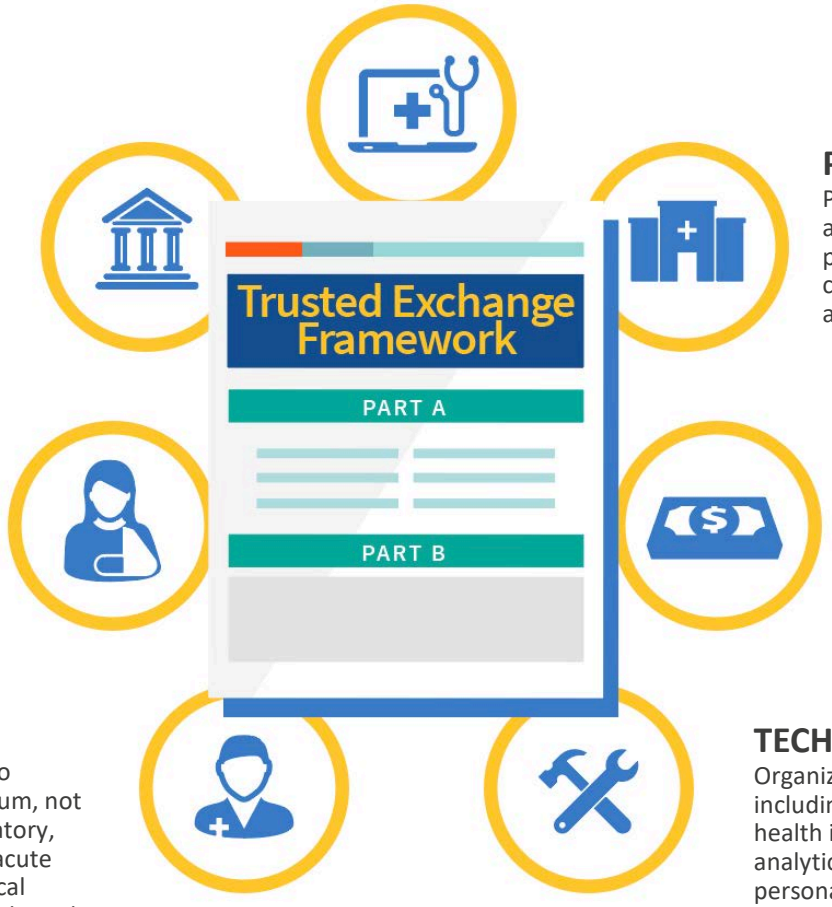
Easing the flow of data will allow new and innovative technologies to enter the market and build competitive, invaluable services that make use of the data.

### 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.

# 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

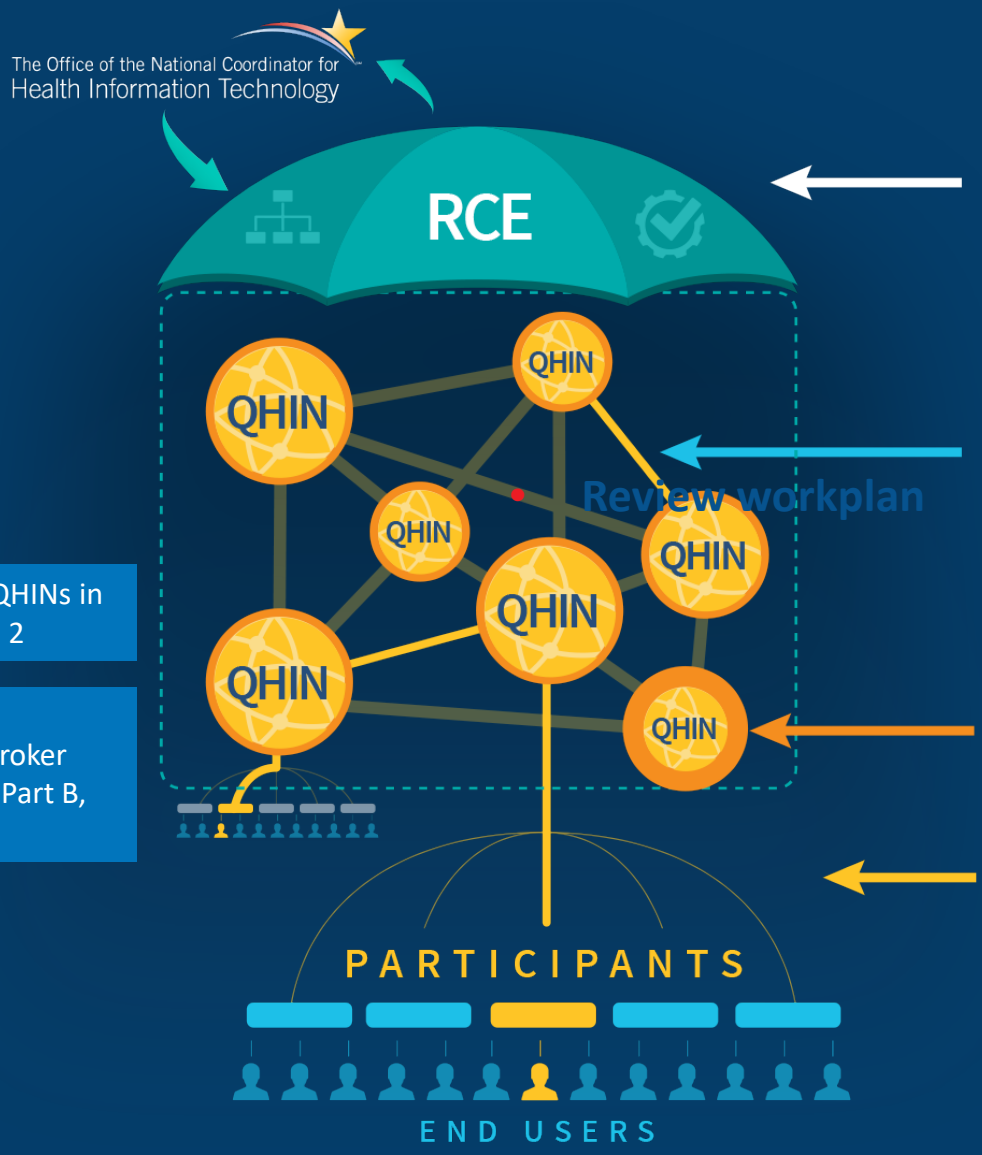
### PROVIDERS
Professional care providers who deliver care across the continuum, not limited to but including ambulatory, inpatient, long-term and post-acute care (LTPAC), emergency medical services (EMS), behavioral health, and home and community based services

### 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

The Office of the National Coordinator for Health Information Technology

# How will the Trusted Exchange Framework work?

# 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

# 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?

# 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?

# 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.**

# 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

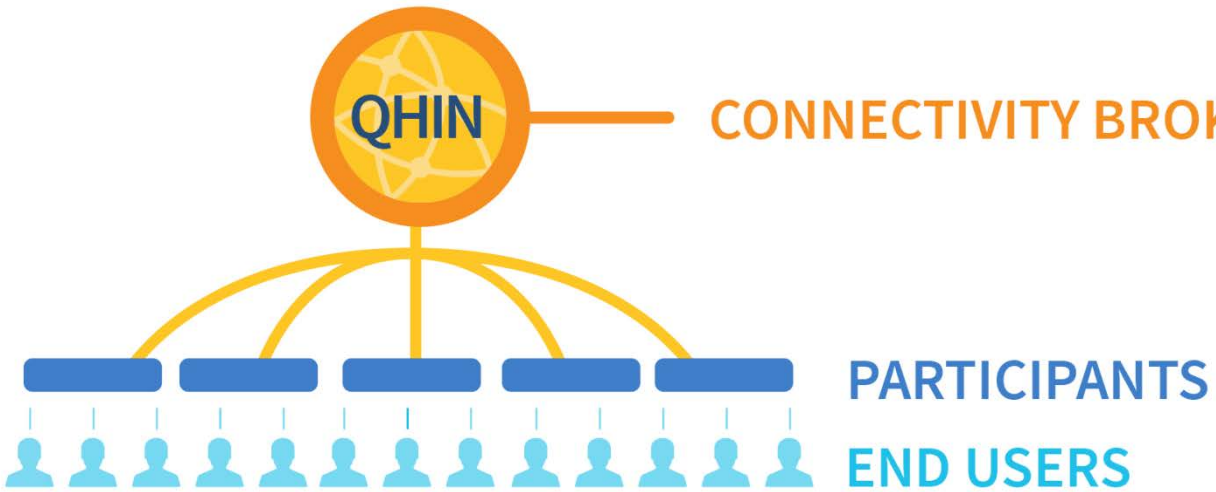
3. Exercises substantial influence or control with respect to the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

# 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.

# 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.

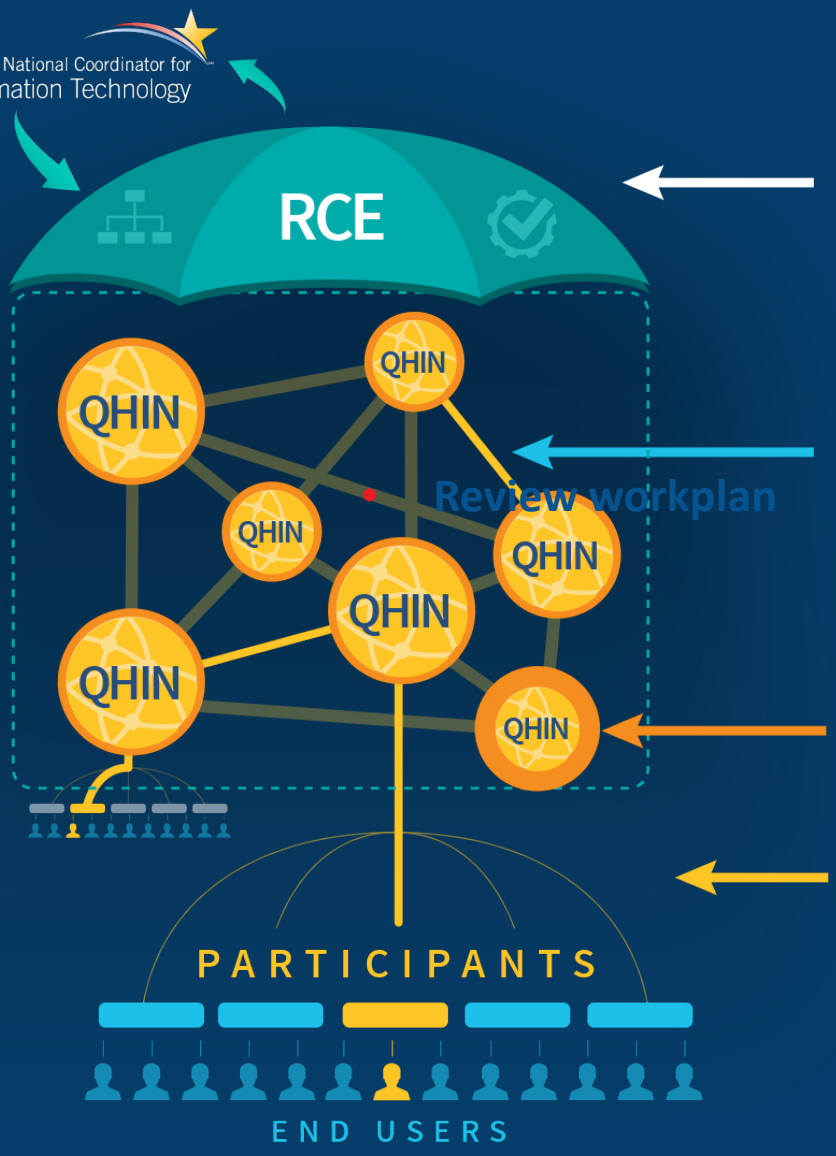
**A Connectivity Broker** is a service provided by a Qualified HIN that provides all of the following functions with respect to all Permitted Purposes: master patient index (federated or centralized); Record Locator Service; Broadcast and Directed Queries, and EHI return to an authorized requesting Qualified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

The Office of the National Coordinator for Health Information Technology

# What use cases are covered under the Trusted Exchange Framework?

# Permitted Purposes


READ MORE: Part B, Section 1

# 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.

## 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.

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

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

## Population Level Data

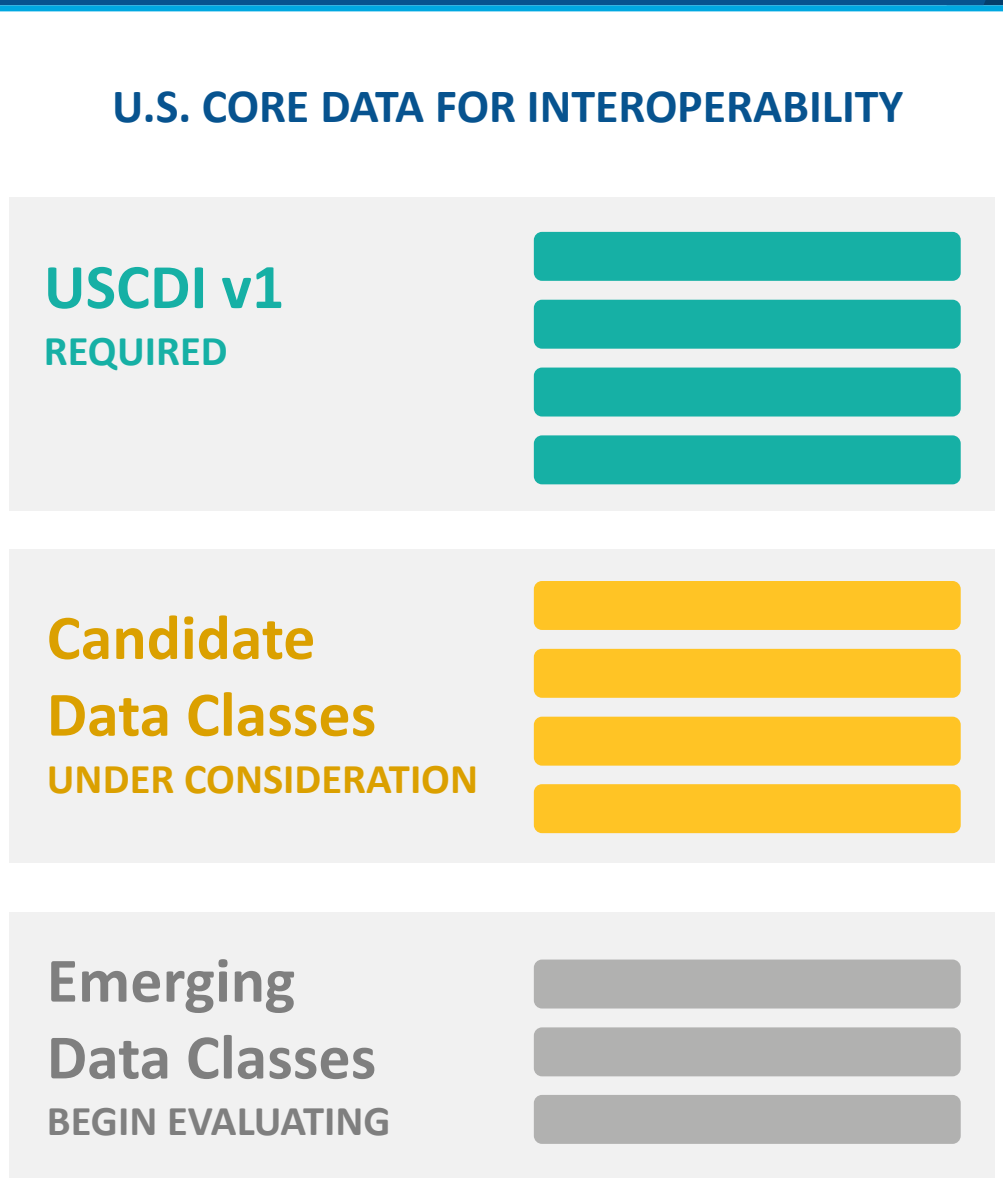
Querying and retrieving Electronic Health Information about multiple patients in a single query.

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

# US Core Data for Interoperability (USCDI) Glide Path

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.

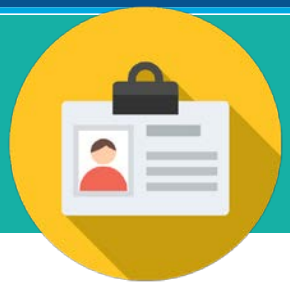
1. **USCDI v1— Required—CCDS plus Clinical Notes and Provenance**
2. **Candidate Data Classes—Under consideration for USCDI v2**
3. **Emerging Data Classes– Begin evaluating for candidate status**



The Office of the National Coordinator for Health Information Technology

# 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<br>• Two (2) pieces of STRONG evidence; OR<br>• One (1) piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence<br>READ MORE: Part B, Section 6.2.4 |
| **Validation** | • Each piece of evidence must be validated with a process able to achieve the same strength as the evidence presented.<br>• 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. |

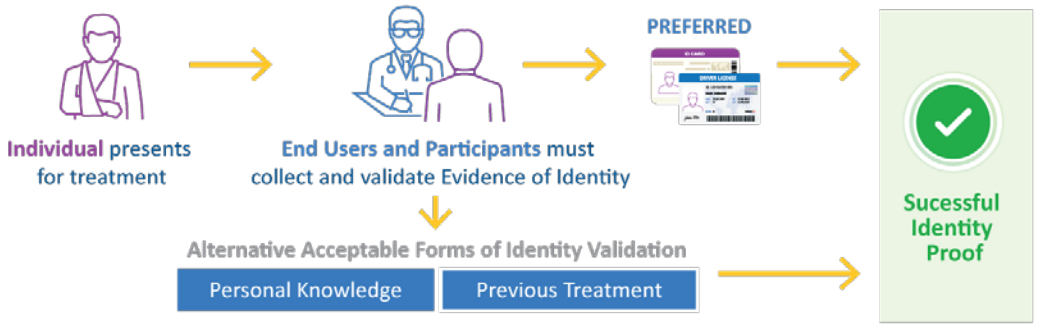
* Full IAL2 requirements can be found at www.nist.gov.

# 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.

**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.

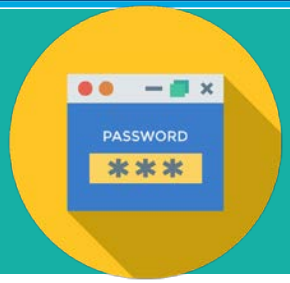



READ MORE: Part B, Section 6.2.4

**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.

# 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).


**End Users and Participants**

**Individuals**

**AAL 2 Authentication**

**Support for FAL2 or FAL3**

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

# Workplan

| Meeting Date | Discussion Items |
|---|---|
| February 20th, 2-3pm ET | Welcome, review of TEFCA, and review of Task Force project plan |
| February 23rd, 1-2pm ET | Recognized Coordinating Entity (RCE) eligibility requirements |
| February 26th, 2-3pm ET | Qualified HIN definition and eligibility requirements |
| March 2nd, 2-3pm ET | Permitted Uses and Disclosures |
| March 5th, 2-3pm ET | Privacy/Security<br>Begin drafting recommendations |
| March 9th | NO MEETING- Continue drafting recommendations |
| March 12th, 2-3pm ET | Review draft recommendations |
| March 16th, 2-3pm ET | Finalize recommendations |
| March 19th, 2-3pm ET | Send final recommendation to full committee for review |
| March 21st, 2-3pm ET | Present recommendations to full committee |

The Office of the National Coordinator for Health Information Technology

Health IT Advisory Committee

# Trusted Exchange Framework Task Force

@ONC_HealthIT @HHSONC HealthIT.gov