



GENERAL COMMITTEE MEETING

Thursday, May 16, 2019

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 857-232-0157, **Code:** 30-40-73

1. **Welcome and Introductions**
2. **Guest Speaker: John Rancourt,**
*Director, Interoperability Division, Office of Policy,
Office of the National Coordinator for Health IT*

TEFCA Draft 2 **Attachment 1**
3. **HIPAA FAQs Electronic Protected Health Information** **Attachment 2**
4. **Notification of Enforcement Discretion Regarding
HIPAA Civil Money Penalties** **Attachment 3**
5. **Cybersecurity Workforce** **Attachment 4**
6. **NIST Privacy Framework: Workshop**

Next Meeting: June 20, 3:00 pm - 4:00 pm



The Office of the National Coordinator for
Health Information Technology

A User's Guide to Understanding

Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2

This informational resource describes select proposals in the TEFCA but is not an official statement of any policy.
Please refer to the official version of the TEFCA.

VISIT WWW.HEALTHIT.GOV/TEFCA TO VIEW THE TEFCA DRAFT 2.



Cures Act Language

21st Century Cures Act - Section 4003(b)

“[T]he 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.”

“[T]he 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...”

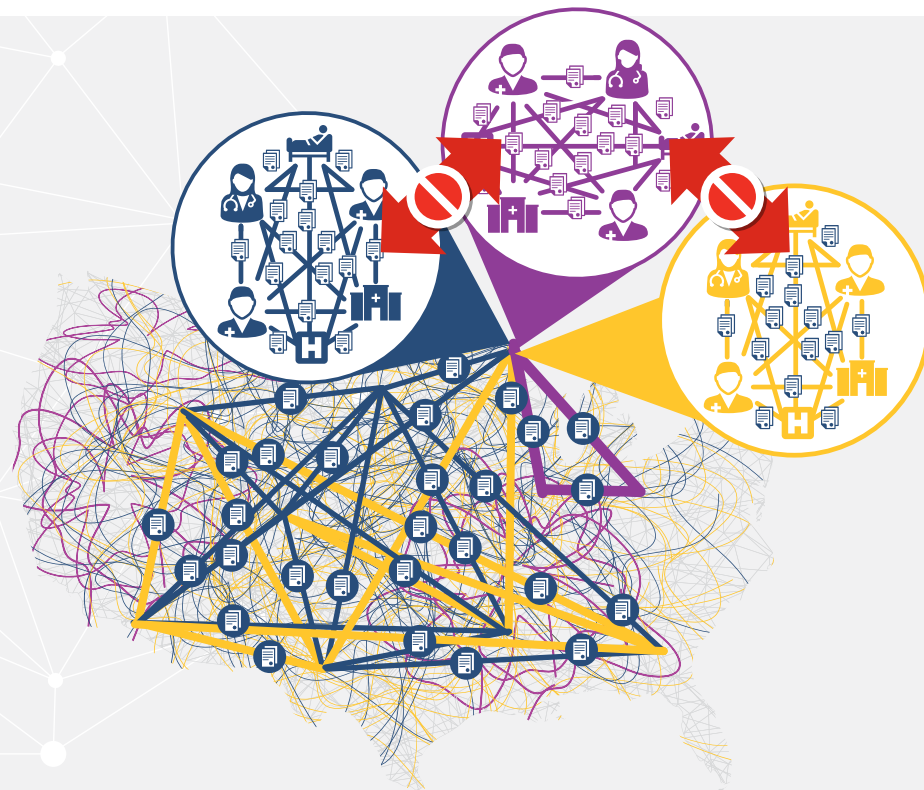


Current Complexity

Current Proliferation of Agreements

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

Trusted exchange must be simplified in order to scale.





Current Costs

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

The Trusted Exchange Framework and the Common Agreement would **reduce the need for duplicative network connectivity interfaces**, which are costly, complex to create and maintain, and an inefficient use of provider and health IT developer resources.



Proliferation of Interoperability Methods

A nationally representative survey by the American Hospital Association found¹ that:

Few hospitals used only one interoperability method.

- » 78% of hospitals use more than one electronic method to send records
- » 61% of hospitals use more than one electronic method to receive records
- » About 40% used five or more methods to send records

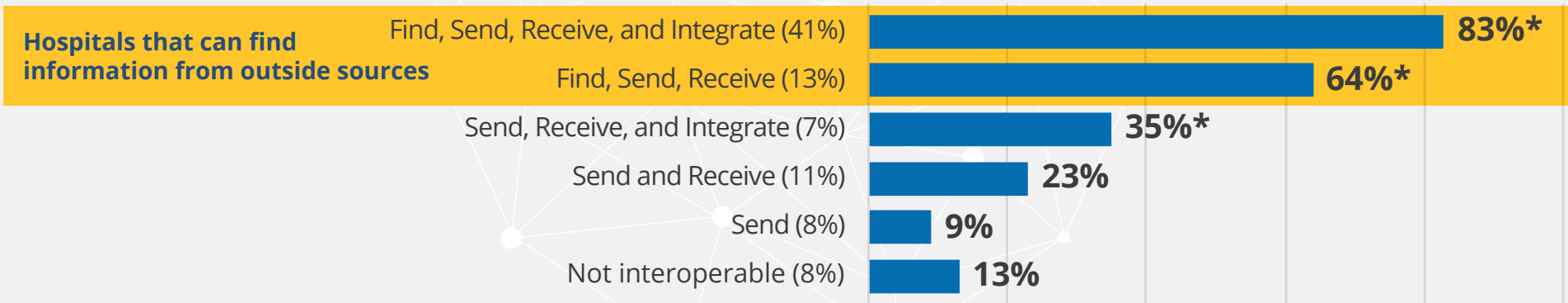
¹https://www.healthit.gov/sites/default/files/page/2018-12/Methods-Used-to-Enable-Interoperability-among-U.S.-NonFederal-Acute-Care-Hospitals-in-2017_0.pdf



Query Exchange is Critical for Care Coordination

Hospitals that query information from outside sources are significantly more likely to have the necessary information available at the point of care than those that do not¹.

HOSPITAL INTEROPERABILITY ACTIVITY(IES)



*Significantly different from send and received (p<0.05)

¹https://www.healthit.gov/sites/default/files/page/2018-11/Interop%20variation_0.pdf

■ Percent of Hospitals with Information Available at the Point of Care from Outside Providers

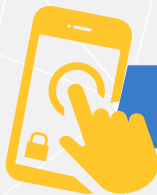


Goals



GOAL 1

Provide a single
“on-ramp” to
nationwide connectivity



GOAL 2

Electronic Health Information
(EHI) securely follows you
when and where it is needed



GOAL 3

Support nationwide
scalability



What is the Trusted Exchange Framework?

The **Trusted Exchange Framework** is a set of common principles that are designed to facilitate trust among Health Information Networks (HINs).



The Trusted Exchange Framework (TEF)

Principle 1 – Standardization: Adhere to industry and federally recognized standards, policies, best practices, and procedures.

Principle 2 – Transparency: Conduct all exchange and operations openly and transparently.

Principle 3 – Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange EHI, even when a stakeholder may be a business competitor.

Principle 4 – Privacy, Security, and Safety: Exchange EHI securely and in a manner that promotes patient safety, ensures data integrity, and adheres to privacy policies.

Principle 5 – Access: Ensure that individuals and their authorized caregivers have easy access to their EHI.

Principle 6 – Population-Level Data: Exchange multiple records for a cohort of individuals at one time in accordance with applicable law to enable identification and trending of data to lower the cost of care and improve the health of the population.



What is the Common Agreement?

The **Common Agreement** will provide the governance necessary to scale a functioning system of connected HINs that will grow over time to meet the demands of patients, clinicians, and payers.



Minimum Required Terms & Conditions (MRTCs): ONC will develop mandatory minimum required terms and conditions that Qualified Health Information Networks (QHINs) who agree to the Common Agreement would abide by.

Additional Required Terms & Conditions (ARTCs): In addition to the MRTCs, the Common Agreement will include additional required terms and conditions that are necessary for the day-to-day operation of an effective data sharing agreement. The Recognized Coordinating Entity (RCE) will develop the ARTCs and ONC will have final approval.

QHIN Technical Framework (QTF): Signatories to the Common Agreement must abide by the QHIN Technical Framework, which specifies functional and technical requirements for exchange among QHINs. The RCE will work with ONC and stakeholders to modify and update the QTF.



What is the QHIN Technical Framework?

The **QHIN Technical Framework (QTF)** describes the technical and functional requirements for EHI exchange among QHINs.



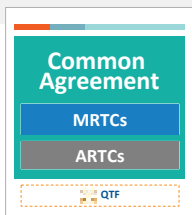
Functions included: Certificate Policy, Secure Channel, Mutual QHIN Server Authentication, User Authentication, Authorization & Exchange Purpose, Query, Message Delivery, Patient Identity Resolution, Record Location, Directory Service, Individual Privacy Preferences, Auditing, and Error Handling.

Technical detail: Focuses directly on information exchange between QHINs; for most interactions within a QHIN's network, the QHIN may determine how best to implement its responsibilities.

Functions enable: QHIN Broadcast Query, QHIN Targeted Query, and QHIN Message Delivery.



Framework Agreement Flow-Down



Common Agreement

The parties to the Common Agreement will be the RCE and one or more QHINs. The Common Agreement will include flow down clauses for the QHIN's agreements with its Participants and the Participant's agreements with its Participant Members.



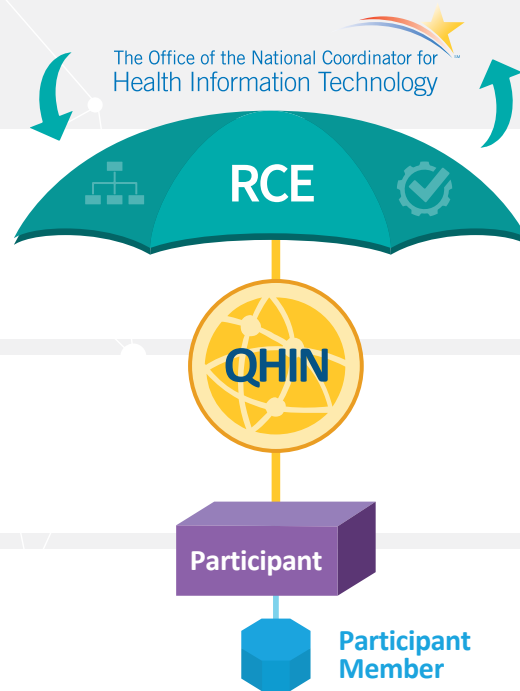
Participant-QHIN Agreement

An agreement between a Participant and a QHIN.



Participant Member Agreement

An agreement between a Participant and a Participant Member.





Summary of Key Changes

Exchange Purposes

Exchange Purposes Updated

Adopted a subset of payment and health care operations purposes, as defined in HIPAA.



QHIN Message Delivery (Push) Added

Included sending a patient's electronic health information (EHI) to a specific Qualified Health Information Network (QHIN) for delivery.



QHIN Technical Framework Added

Addressed the technical requirements for exchange among QHINs through development of the QHIN Technical Framework – Draft 1.



QHIN Definition Broadened

Application process added that allows a broader set of HINs to apply to be a QHIN.

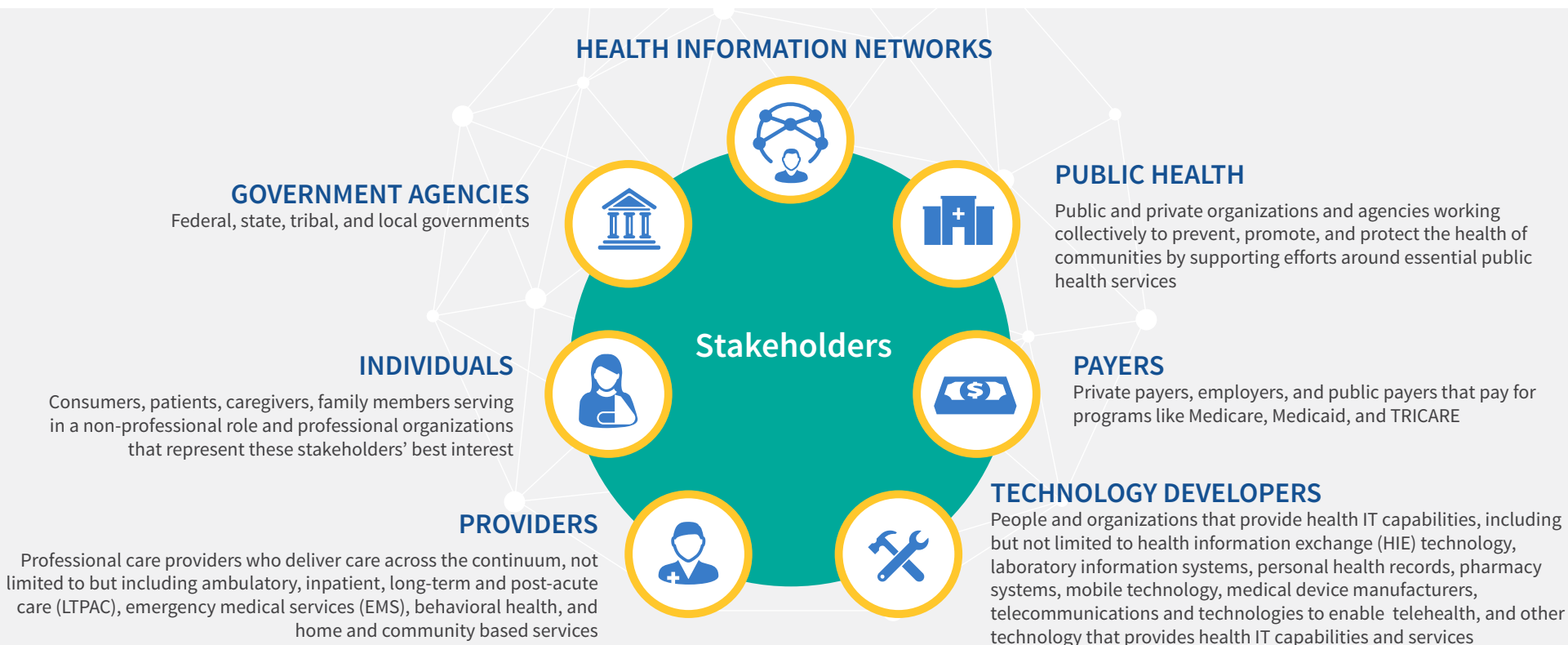


Timelines Extended

When a new version of the Common Agreement is published, entities that have signed a Framework Agreement would have 18 months to implement updates instead of 12.



Stakeholders who can use the TEFCA





Health Information Network (HIN)

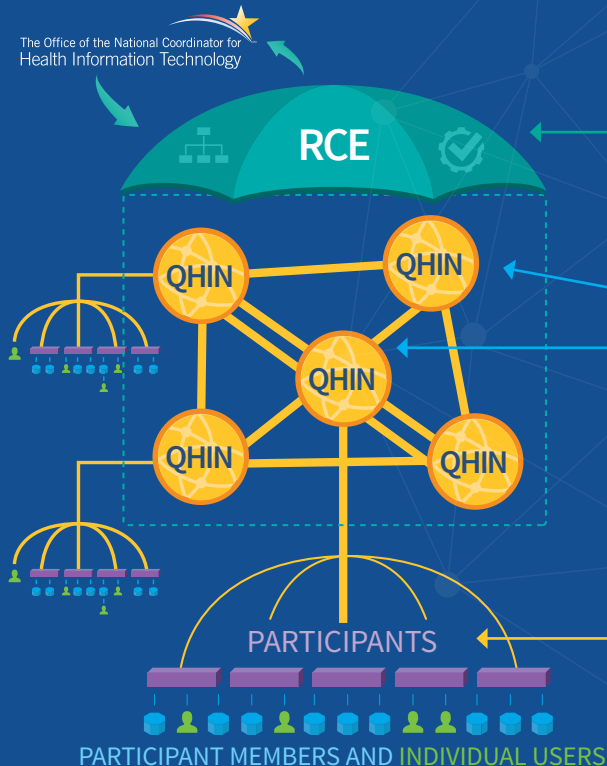
Health Information Network (HIN):
an individual or an entity that satisfies
one or both of the following:

- 1) Determines, oversees, administers, controls, or substantially influences 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; or
- 2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.





How Will the Common Agreement Work?



RCE provides oversight and governance for QHINs.

QHINs connect directly to each other to facilitate nationwide interoperability.

Each QHIN represents a variety of Participants that they connect together, serving a wide range of Participant Members and Individual Users.



Recognized Coordinating Entity (RCE)



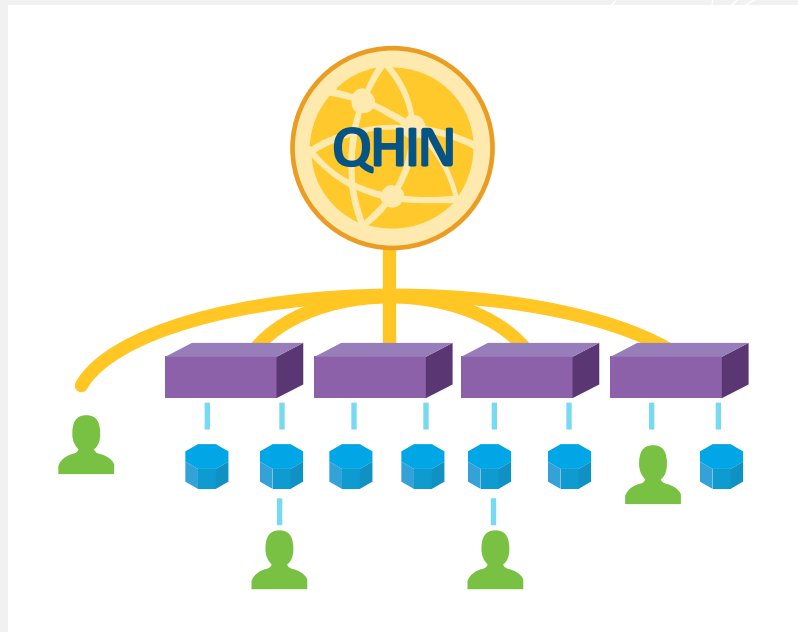
- ✓ Develop, update, implement, and maintain the Common Agreement.
- ✓ Identify, designate, and monitor QHINs.
- ✓ Modify and update the QHIN Technical Framework.
- ✓ Virtually convene public listening sessions.
- ✓ Develop and maintain a process for adjudicating QHIN noncompliance.
- ✓ Propose strategies to sustain the Common Agreement at a national level after the initial cooperative agreement period.

How the RCE is Selected

- » **ONC is releasing an open, competitive Notice of Funding Opportunity to award a single four-year cooperative agreement to a private sector organization to become the RCE.**
- » **A successful applicant would be a non-profit entity based in the United States. If awarded, the RCE may not be affiliated with a QHIN.**
- » **The Notice of Funding Opportunity is posted to Grants.gov.**



Structure of a Qualified Health Information Network



Participant

A natural person or entity that has entered into a Participant-QHIN Agreement to participate in a QHIN.



Participant Member

A natural person or entity that has entered into a Participant Member Agreement to use the services of a Participant to send and/or receive EHI.

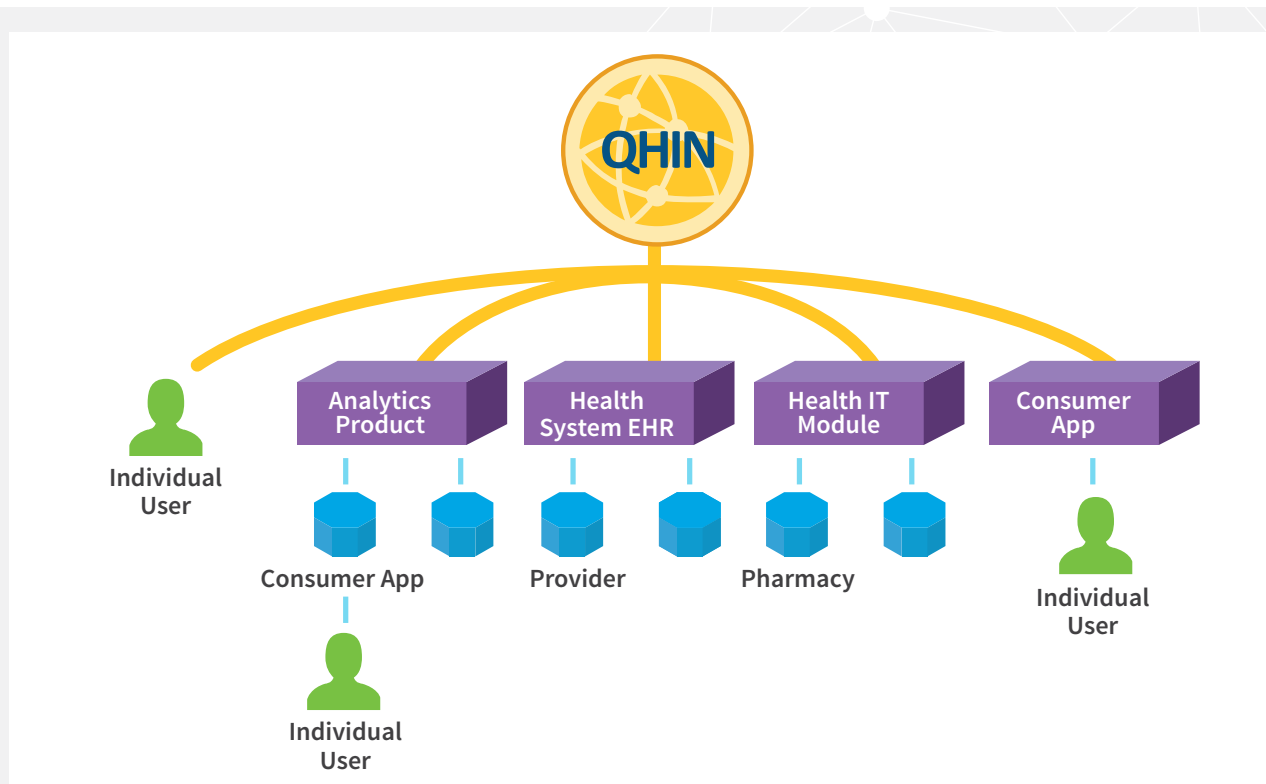


Individual User

An Individual who exercises their right to Individual Access Services using the services of a QHIN, a Participant, or a Participant Member.



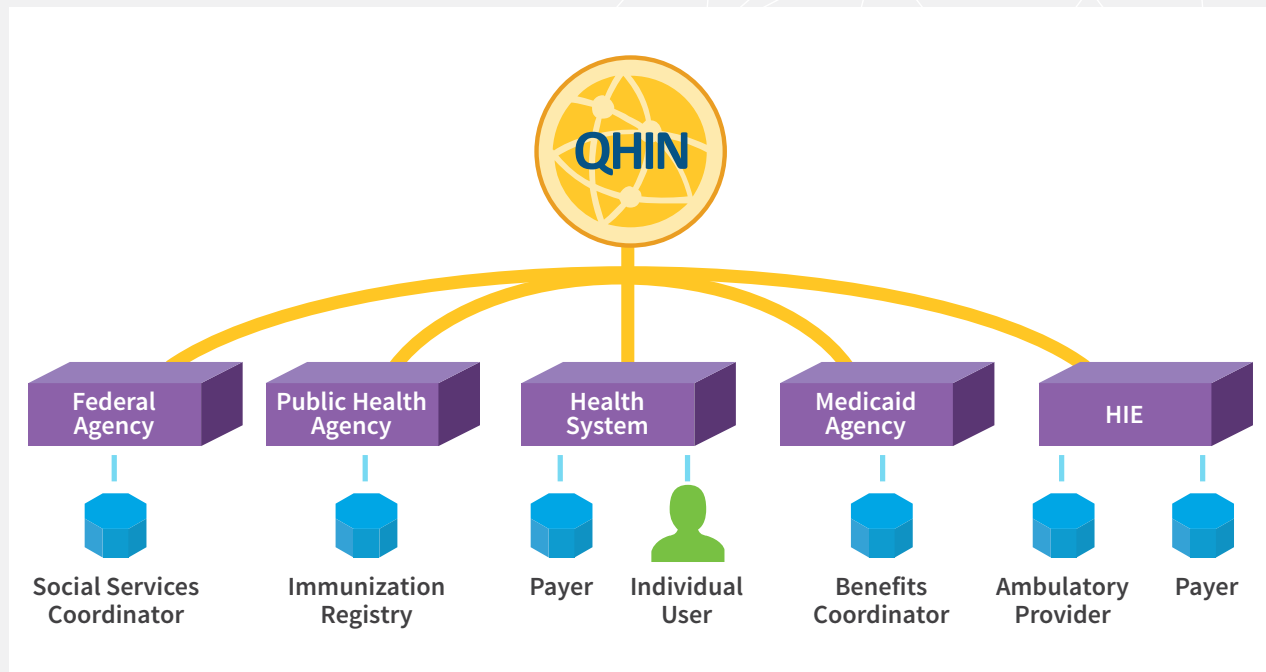
QHIN Example: Network of Health IT Developers



In this example, the QHIN supports a broad range of different health IT developer Participants. The users of the health IT developers' products are Participant Members. Individual Users connect directly to the QHIN, Participants, and Participant Members.



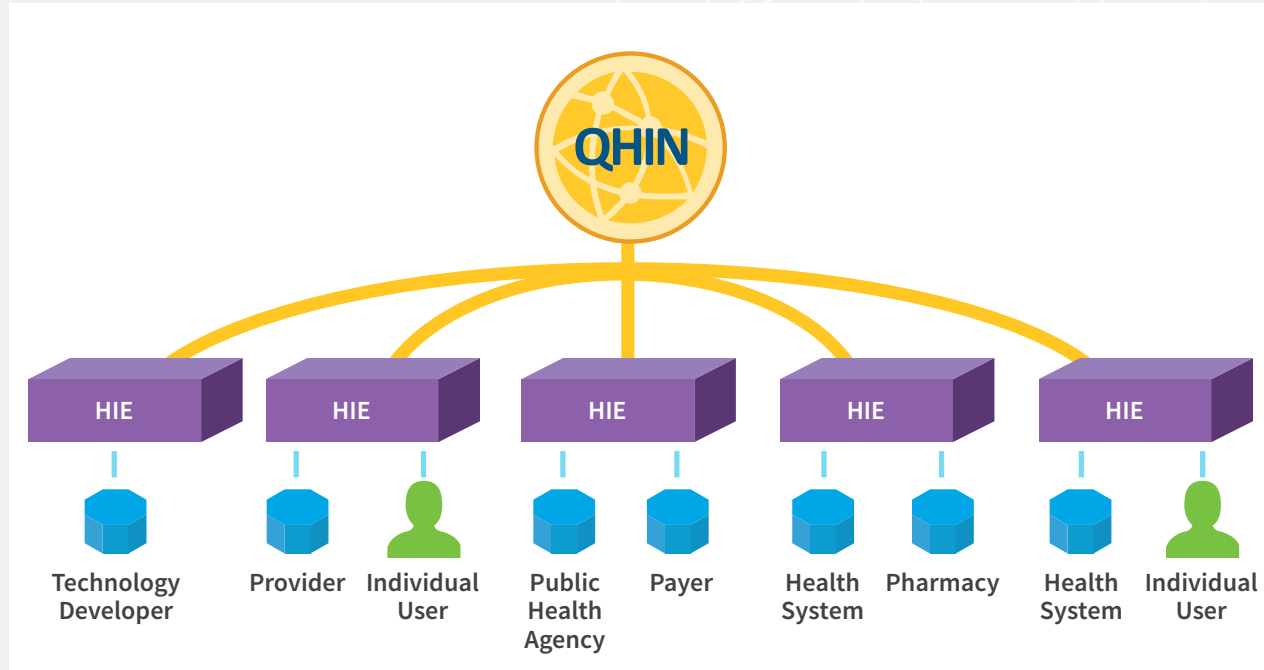
QHIN Example: Various Participants



In this example, the QHIN directly supports federal agencies, state agencies, health systems, and HIEs as Participants. The members of the federal/state agencies, health systems, and HIEs are Participant Members and Individual Users.



QHIN Example: Network of HIEs






In this example, the QHIN directly supports HIEs as Participants. Members of the HIEs are Participant Members and Individual Users.



QHIN Applicant Checklist

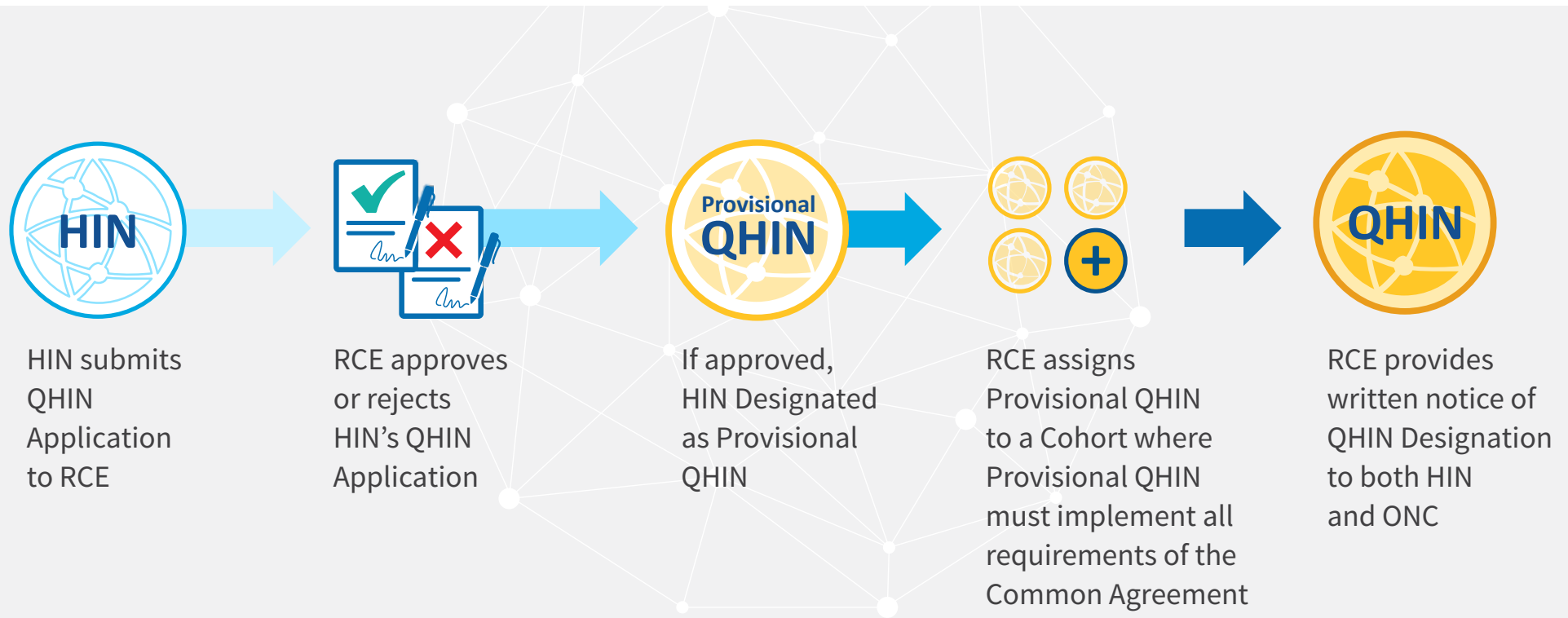
A HIN applying to be a QHIN must:

-  Operate an existing network with participants exchanging data in a live clinical environment
-  Meet applicable federal/state law
-  Submit a plan to meet all QHIN requirements





QHIN Application Process





QHIN Application Process

Step 1:

RCE solicits, collects, and evaluates QHIN Applications from HINs who wish to receive QHIN Designation. In order to apply for QHIN Designation, a HIN must meet certain prerequisites:



- i. The HIN already operates a network that provides the ability to locate and transmit EHI between multiple persons and/or entities electronically, on demand or pursuant to one or more automated processes.
- ii. Such persons and/or entities are already exchanging EHI in a live clinical environment using the network.
- iii. The HIN has provided reasonable evidence that exchange of EHI using its network is occurring in accordance with applicable law and the privacy, security, and patient safety requirements in the MRTCs.
- iv. The HIN has provided a reasonable plan in writing of how it will achieve within the required period all of the applicable requirements of the Common Agreement and the QHIN Technical Framework.

Step 2:

After receipt of a completed QHIN Application, the RCE approves or rejects each QHIN Application in writing and within a stated period.



Step 3:

If approved, the HIN and RCE must both execute the Common Agreement and the HIN receives Provisional QHIN status.



Step 4:

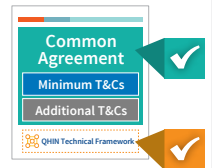
The RCE assigns the Provisional QHIN to a Cohort which has an applicable deadline by which the Provisional QHIN must become a Designated QHIN or be terminated from the Cohort.



A Cohort is a group of one or more Provisional QHINs that are attempting to be Designated by the RCE as QHINs. They have been assigned the same deadline for completing all required actions to be Designated a QHIN.

Step 5:

The Provisional QHIN asserts, and the RCE confirms, that all applicable requirements of the Common Agreement and QHIN Technical Framework have been met.



Step 6:

RCE provides written notice to the Provisional QHIN that it has been Designated a QHIN. The RCE also provides notice to ONC.





Exchange Purposes



**Only applies to HIPAA covered entities and business associates*



Exchange Purposes Definitions



TREATMENT*

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.



BENEFITS DETERMINATION

A determination made by any federal or state agency as to whether an Individual qualifies for federal or state benefits for any purpose other than health care.



QUALITY ASSESSMENT & IMPROVEMENT*

Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, patient safety activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment.



BUSINESS PLANNING AND DEVELOPMENT*

Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.



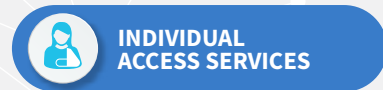
PUBLIC HEALTH*

A Use or Disclosure permitted under the HIPAA Rules and any other applicable law for public health activities and purposes.



UTILIZATION REVIEW*

The conduct of utilization review activities by a 1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan; or 2) health plan or provider to obtain or provide reimbursement for the provision of care. Utilization review activities include precertification and preauthorization of services, concurrent and retrospective review of services.



INDIVIDUAL ACCESS SERVICES

The services provided to satisfy an Individual's right to access pursuant to Applicable Law or any of the Framework Agreements, including the right of an Individual to: 1) obtain a copy of their EHI, and 2) direct that a copy of their EHI be transmitted to another person or entity designated by the Individual.

**Only applies to HIPAA covered entities and business associates*



Exchange Modalities



QHIN Broadcast Query

A QHIN's electronic request for a patient's EHI from all QHINs.



QHIN Targeted Query

A QHIN's electronic request for a patient's EHI from specific QHINs.



QHIN Message Delivery (Push)

The electronic action of a QHIN to deliver a patient's EHI to one or more specific QHINs.

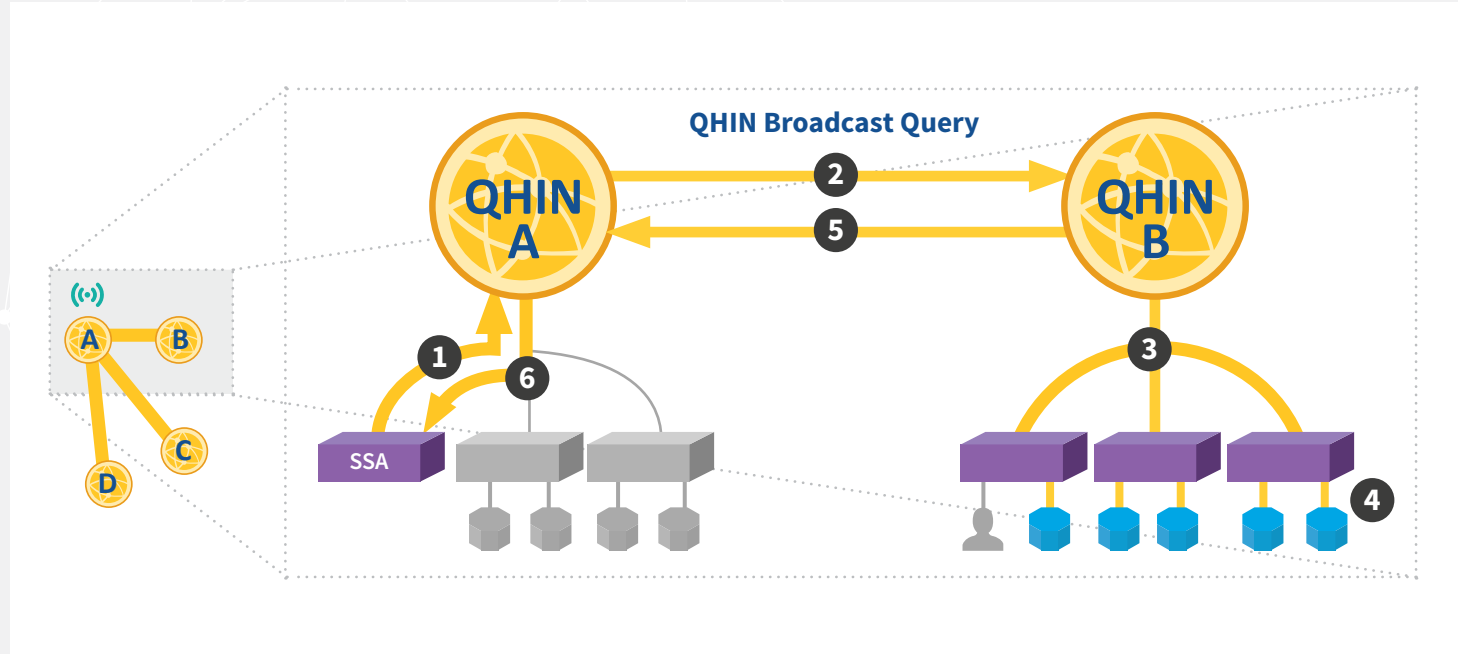


Exchange Purpose Example



BENEFITS DETERMINATION

- 1 Social Security Administration (SSA) (Participant) sends a request for medical records to QHIN A for the purpose of Benefits Determination
- 2 QHIN A initiates QHIN Broadcast Query to all connected QHINs
- 3 QHIN B, C, D execute their query methodology to request medical records from all appropriate Participants and their Participant Members
- 4 Participant Members and Participants respond with medical records
- 5 QHIN B, C, D send medical records to QHIN A
- 6 QHIN A sends medical records to SSA (Participant)

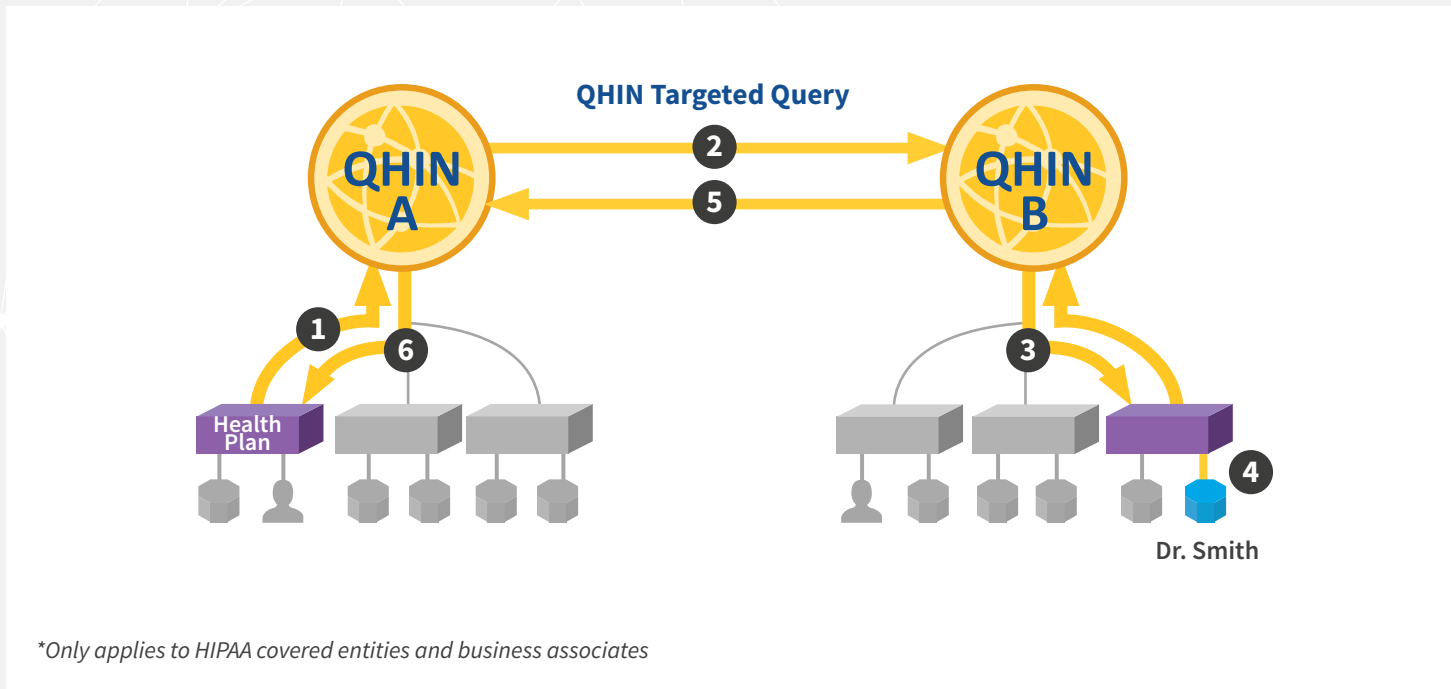




Exchange Purpose Example



- 1 Health Plan (Participant) sends a request for medical records from Dr. Smith to QHIN A for Quality Assessment & Improvement
- 2 QHIN A initiates QHIN Targeted Query to appropriate QHIN B
- 3 QHIN B executes its query methodology to request medical records from appropriate Participant, who requests from Dr. Smith (Participant Member)
- 4 Dr. Smith (Participant Member) responds with medical records, Participant sends medical records to QHIN B
- 5 QHIN B sends medical records to QHIN A
- 6 QHIN A sends medical records to Health Plan (Participant)



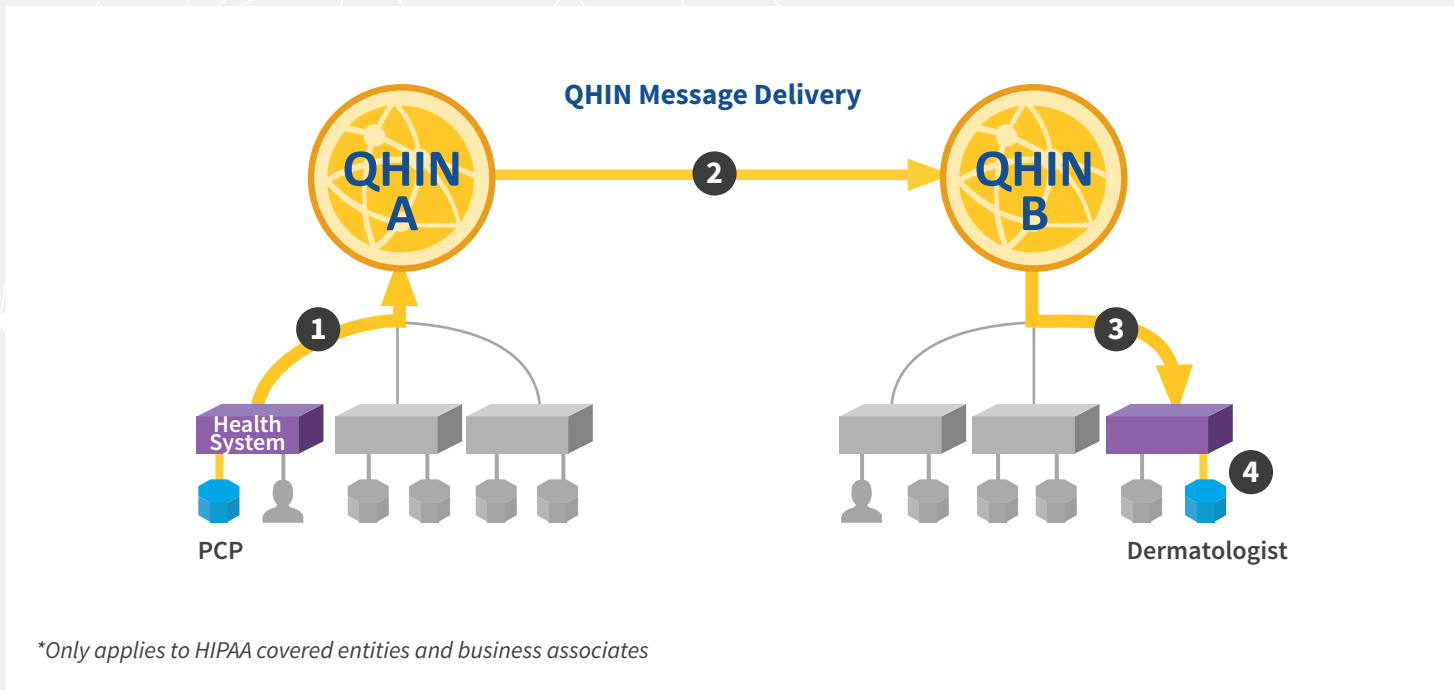


Exchange Purpose Example



TREATMENT*

- 1 Primary Care Provider (PCP) (Participant Member) refers patient to Dermatologist, and sends care summary to QHIN A for Treatment
- 2 QHIN A initiates QHIN Message Delivery to send care summary to the appropriate QHIN B
- 3 QHIN B sends care summary to the appropriate Participant
- 4 Participant delivers care summary to the Dermatologist (Participant Member)

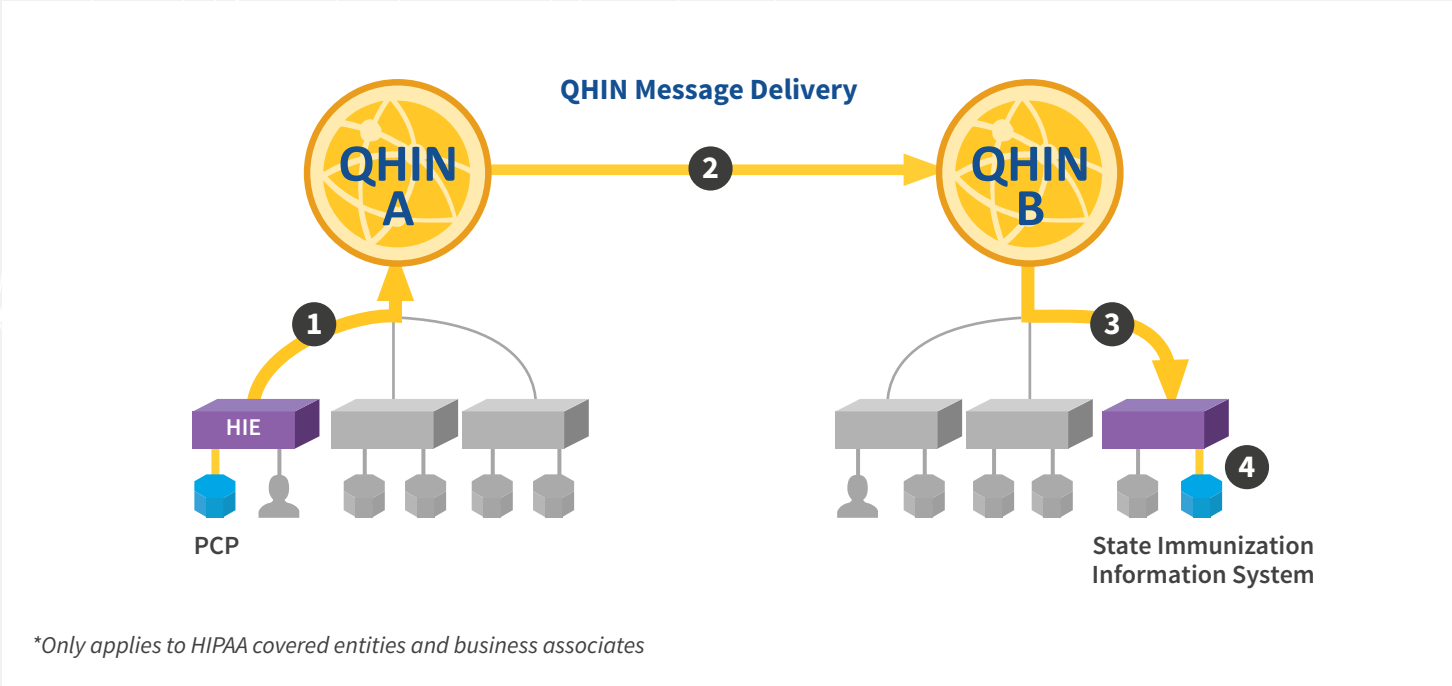




Exchange Purpose Example



- 1 Primary Care Provider (PCP) (Participant Member) provides an immunization to a patient and sends immunization record to QHIN A for Public Health
- 2 QHIN A initiates QHIN Message Delivery to send the immunization record to the appropriate QHIN B
- 3 QHIN B sends immunization record to the appropriate Participant
- 4 Participant delivers immunization record to the appropriate State Immunization Information System (Participant Member)



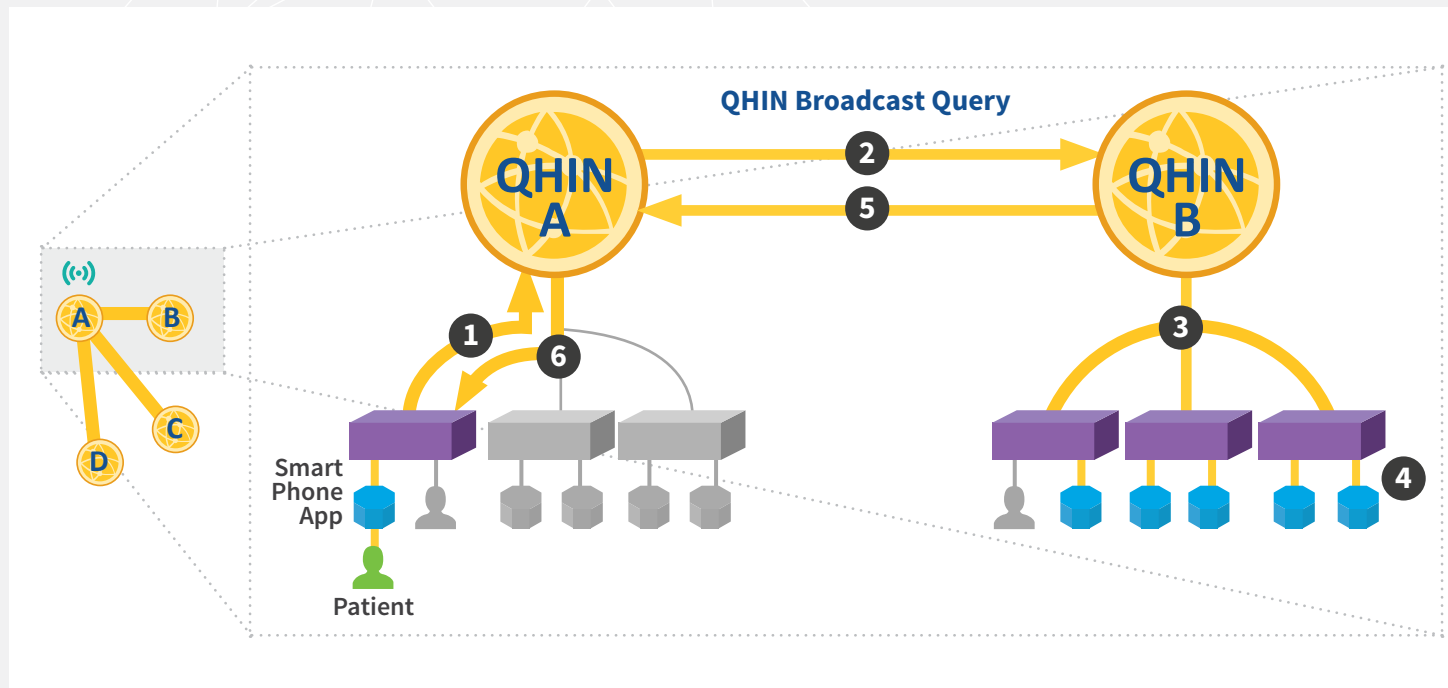


Exchange Purpose Example



INDIVIDUAL ACCESS SERVICES

- 1 Patient (Individual User) uses a smart phone app (Participant Member) to make a medical records request via the Participant to the QHIN for Individual Access Services
- 2 QHIN A initiates QHIN Broadcast Query to all connected QHINs
- 3 QHINs B, C, D execute their query methodology to request medical records from all appropriate Participants and their Participant Members
- 4 Participant Members and Participants respond with medical records
- 5 QHINs B, C, D send medical records to QHIN A
- 6 QHIN A sends medical records to Participant, who sends to smart phone app (Participant Member), who sends to Patient (Individual User)



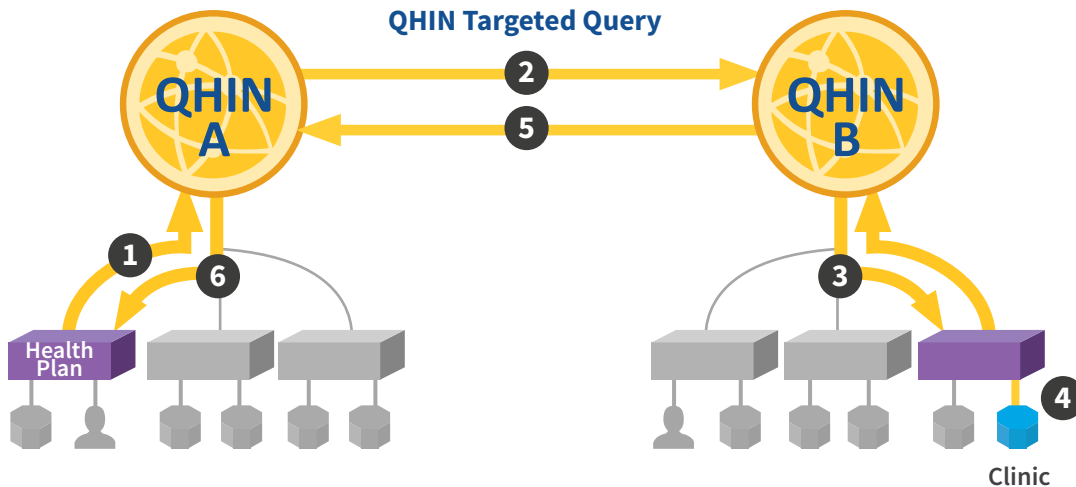


Exchange Purpose Example



UTILIZATION REVIEW*

- 1 Health Plan (Participant) sends a medical records request for a Clinic (Participant Member) to QHIN A for QHIN Targeted Query for Utilization Review
- 2 QHIN A initiates QHIN Targeted Query to QHIN B
- 3 QHIN B requests medical records from appropriate Participant, who requests from Clinic (Participant Member)
- 4 Clinic (Participant Member) responds with medical records, Participant sends medical records to QHIN B
- 5 QHIN B sends medical records to QHIN A
- 6 QHIN A sends medical records to Health Plan (Participant)



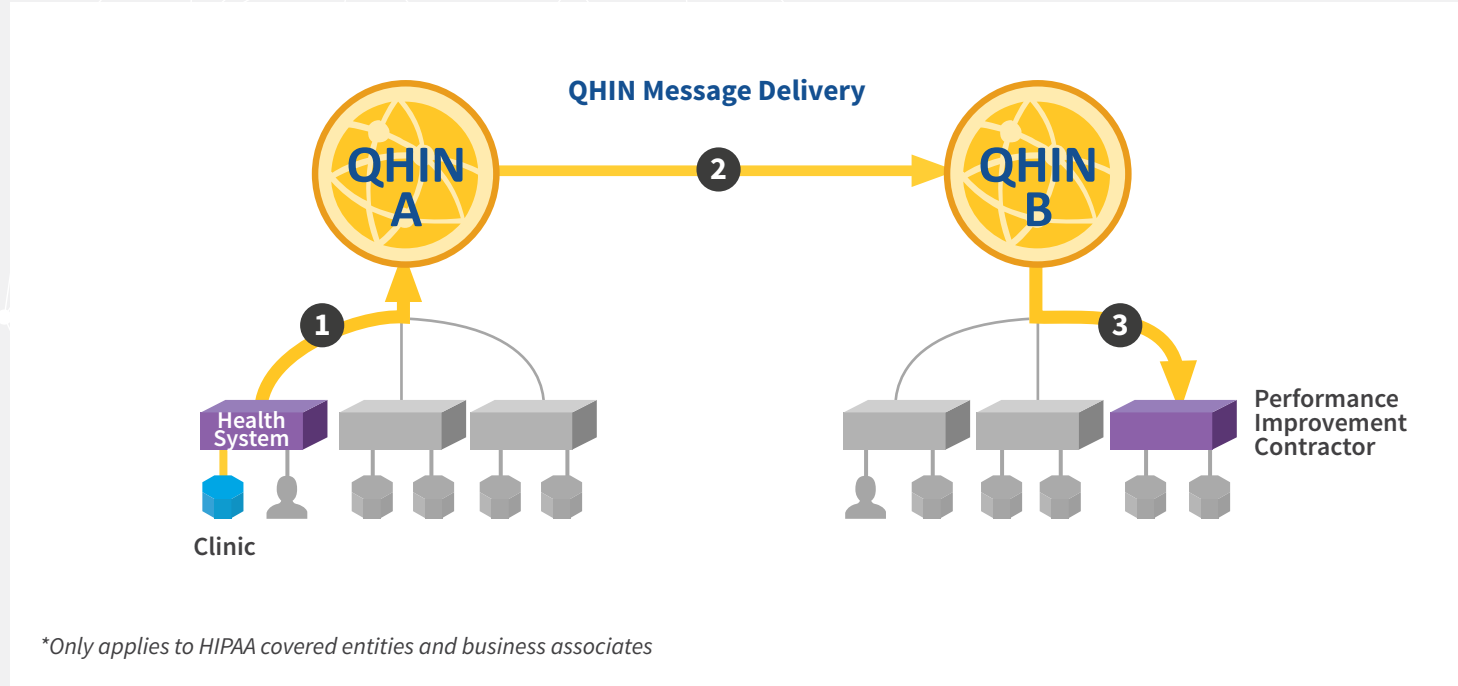
**Only applies to HIPAA covered entities and business associates*



Exchange Purpose Example



- 1 Clinic (Participant Member) sends medical records to QHIN A for QHIN Message Delivery for the purpose of business planning and development
- 2 QHIN A initiates QHIN Message Delivery to send medical records to QHIN B
- 3 QHIN B sends medical records to the Performance Improvement Contractor (Participant)





Minimum Privacy and Security Requirements



QHINs

QHINs must abide by the HIPAA Privacy and Security Rule as if it applies to EHI. They must also evaluate their security programs on an annual basis in accordance with NIST Special Publication 800-171. To the extent that the QHIN's risk analysis identifies any risks, vulnerabilities, or gaps in the QHIN's compliance with the HIPAA Rules or other Applicable Law, the QHIN shall assess and implement appropriate security measures consistent with industry standards and best practices that it determines would be reasonable and appropriate to ensure the confidentiality, integrity and availability of the EHI that it creates, receives, maintains or transmits, and provide documentation of such evaluation.

Participants and Participant Members

Participants and Participant Members, regardless of whether or not they are a Covered Entity or Business Associate, must take reasonable steps to promote the confidentiality, integrity, and availability of EHI. Participants, and Participant Members must review and modify such safeguards regularly to continue protecting EHI in a changing environment of security threats.

The reasonable steps include:

- » Maintaining reasonable and appropriate administrative, technical, and physical safeguards for protecting EHI;
- » Protecting against reasonably anticipated impermissible uses and disclosures of EHI;
- » Identifying and protecting against reasonably anticipated threats to the security or integrity of EHI; and
- » Monitoring workforce compliance.



Identity Proofing

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



QHIN

Each QHIN shall require proof of identity for Participants

Participants

Each Participant shall require proof of identity for Participant Members at a minimum of IAL2 prior to issuance of credentials.

Individual User

QHINS, Participants, and Participant Members shall require proof of identity for Individual Users at a minimum of IAL2 prior to issuance of credentials.

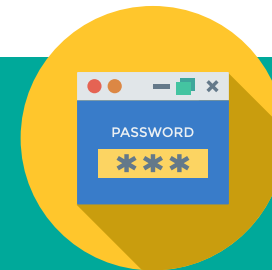
* Full IAL2 requirements can be found at www.nist.gov.

IAL 2 REQUIREMENT	DESCRIPTION
Evidence	<ul style="list-style-type: none"> » 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 FAIR evidence
Validation	<ul style="list-style-type: none"> » Each piece of evidence must be validated with a process able to achieve the same strength as the evidence presented.
Verification	<ul style="list-style-type: none"> » Verified by a process that is able to achieve a strength of STRONG



User 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). Federation 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).



QHIN

Each QHIN shall require Participants be authenticated at a minimum of AAL2 and provide support for at least FAL2 prior to the issuance of credential.

Participants

Each Participant shall require Participant Members be authenticated at a minimum of AAL2 and provide support for at least FAL2 prior to the issuance of credential.

Individual User

QHINS, Participants, and Participant Members shall require Individual Users to be authenticated at a minimum of AAL2 prior to issuance of credentials.





Other Privacy/Security Requirements

Breach Notification Regulations



QHINS, Participants, and Participant Members shall comply with Breach notification requirements pursuant to 45 CFR 164.400-414 of the HIPAA Rules regardless of whether or not they are a covered entity or business associate. Each QHIN further shall notify, in writing, the RCE and other QHINs to the extent that they or one of their Participants or Participant Members are affected by the Breach. Such notice shall be provided without unreasonable delay in accordance with Applicable Law. This does not modify or replace any obligation that an entity may have under the FTC Rule with respect to a breach of security.

No EHI Used or Disclosed Outside the United States

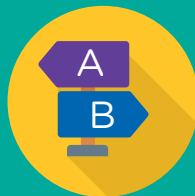


The MRTCs prohibit QHINs from Using or Disclosing EHI outside the United States, except to the extent that an Individual User requires his or her EHI to be Used or Disclosed outside of the United States. ONC seeks public comment on how the Common Agreement should handle potential requirements for EHI that needs to be sent, stored, maintained, or used outside the United States.



Other Privacy/Security Requirements

Meaningful Choice



QHINs, Participants, and Participant Members must provide Individuals with the opportunity to exercise Meaningful Choice, free of charge, by requesting that their EHI not be used or disclosed via the Common Agreement, except as permitted by Applicable Law. Participants and Participant Members are responsible for communicating this meaningful choice up to the QHIN who must then communicate the choice to all other QHINs within five (5) business days. This choice must be respected on a prospective basis.

Written Privacy Summary



QHINs, Participants, and Participant Members must publish and make publically available a written notice describing their privacy practices regarding the access, exchange, use, and disclosure of EHI. This notice should mirror ONC's Model Privacy Notice and include information explaining how an Individual can exercise their Meaningful Choice and who they may contact for more information about the entity's privacy practices.



Security Labeling

Currently, security labels can be placed on data to enable an entity to perform access control decisions on EHI such that only those appropriately authorized to access the EHI are able to access the EHI.



ONC is considering the inclusion of a new requirement regarding security labeling that states the following:

- » Any EHI containing codes from one of the SAMHSA Consent2Share sensitivity value sets for mental health, HIV, or substance use in [Value Set Authority Center \(VSAC\)](#) shall be labeled.
- » Any EHI for patients considered minors shall be electronically labeled.
- » The data holder responding to a request for EHI is obligated to appropriately apply security labels to the EHI.
- » At a minimum, EHI shall be electronically labeled using the confidentiality code set as referenced in the HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (DS4P IG), Part 1: CDA R2 and Privacy Metadata.
- » Labeling shall occur at the highest (document or security header) level.

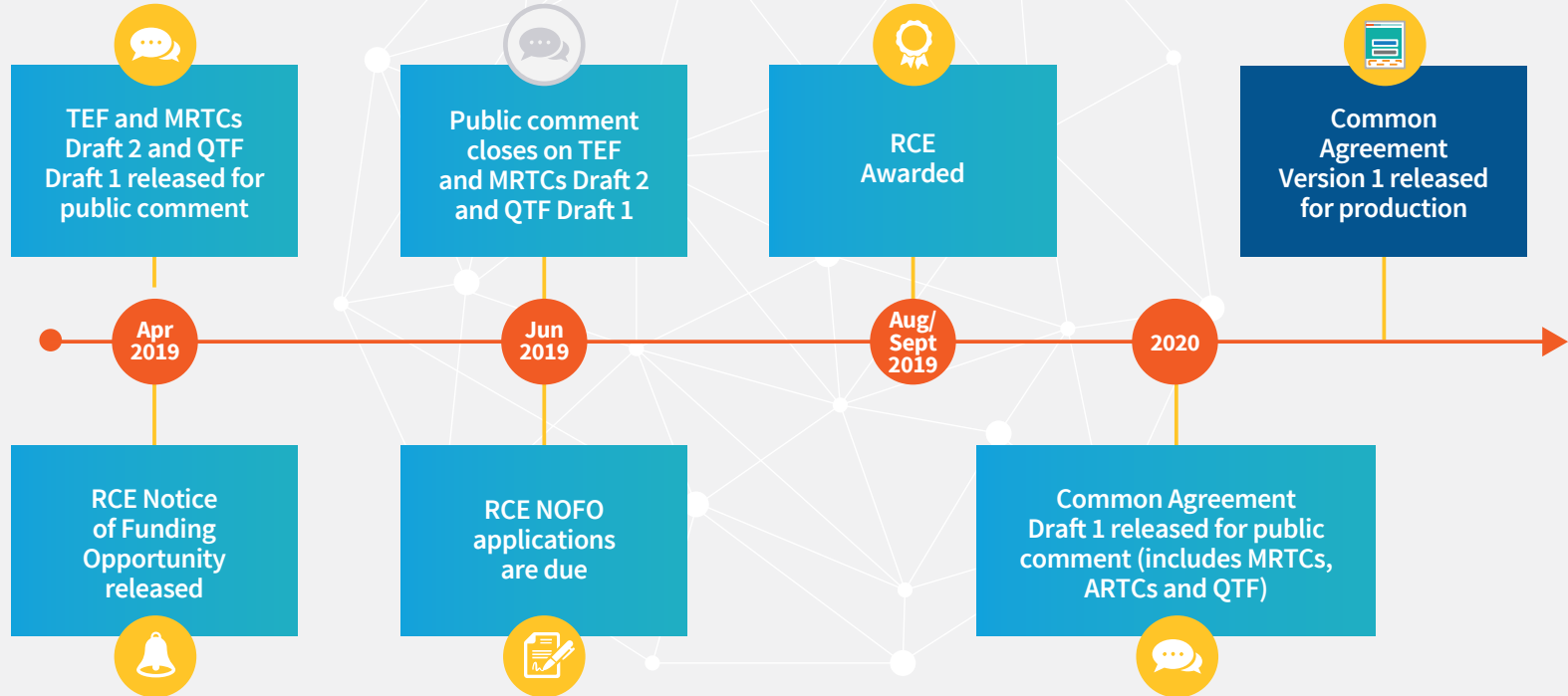


Update Process for the Common Agreement





Timeline



The HIPAA access right, health apps, & APIs

1. Q: Does a HIPAA covered entity that fulfills an individual's request to transmit electronic protected health information (ePHI) to an application or other software (collectively "app")¹ bear liability under the HIPAA Privacy, Security, or Breach Notification Rules (HIPAA Rules) for the app's use or disclosure of the health information it received?

A: The answer depends on the relationship between the covered entity and the app. Once health information is received from a covered entity, at the individual's direction, by an app that is neither a covered entity nor a business associate under HIPAA, the information is no longer subject to the protections of the HIPAA Rules. If the individual's app – chosen by an individual to receive the individual's requested ePHI – was not provided by or on behalf of the covered entity (and, thus, does not create, receive, transmit, or maintain ePHI on its behalf), the covered entity would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app. For example, the covered entity would have no HIPAA responsibilities or liability if such an app that the individual designated to receive their ePHI later experiences a breach.

If, on the other hand, the app was developed for, or provided by or on behalf of the covered entity – and, thus, creates, receives, maintains, or transmits ePHI on behalf of the covered entity – the covered entity could be liable under the HIPAA Rules for a subsequent impermissible disclosure because of the business associate relationship between the covered entity and the app developer. For example, if the individual selects an app that the covered health care provider uses to provide services to individuals involving ePHI, the health care provider may be subject to liability under the HIPAA Rules if the app impermissibly discloses the ePHI received.

2. Q: What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?

A: Under the individual right of access, an individual may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). For instance, an individual may request that their unencrypted ePHI be transmitted to an app as a matter of convenience. In such a circumstance, the covered entity would not be responsible for unauthorized access to the individual's ePHI while in transmission to the app. With respect to such apps, the covered entity may want to consider informing the individual of the potential risks involved the first time that the individual makes the request.

3. Q: Where an individual directs a covered entity to send ePHI to a designated app, does a covered entity's electronic health record (EHR) system developer bear HIPAA liability after completing the transmission of ePHI to the app on behalf of the covered entity?

A: The answer depends on the relationship, if any, between the covered entity, the EHR system developer, and the app chosen by the individual to receive the individual's ePHI. A business associate relationship exists if an entity creates, receives, maintains, or transmits ePHI on behalf of a covered entity (directly or through another business associate) to carry out the covered functions of the covered entity. A business associate relationship exists between an EHR system developer and a covered entity. If the EHR system developer does not own the app, or if it owns the app but does not provide the app to, through, or on behalf of, the covered entity – e.g., if it creates the app and makes it available in an app store as part of a different line of business (and not as part of its business associate relationship with any covered entity) – the EHR system developer would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app.

If the EHR system developer owns the app or has a business associate relationship with the app developer, and provides the app to, through, or on behalf of, the covered entity (directly or through another business associate), then the EHR system developer could potentially face HIPAA liability (as a business associate of a HIPAA covered entity) for any impermissible uses and disclosures of the health information received by the app. For example, if an EHR system developer contracts with the app developer to create the app on behalf of a covered entity and the individual later identifies that app to receive ePHI, then the EHR system developer could be subject to HIPAA liability if the app impermissibly uses or discloses the ePHI received.

4. Q: Can a covered entity refuse to disclose ePHI to an app chosen by an individual because of concerns about how the app will use or disclose the ePHI it receives?

A: No. The HIPAA Privacy Rule generally prohibits a covered entity from refusing to disclose ePHI to a third-party app designated by the individual if the ePHI is readily producible in the form and format used by the app. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). The HIPAA Rules do not impose any restrictions on how an individual or the individual's designee, such as an app, may use the health information that has been disclosed pursuant to the individual's right of access. For instance, a covered entity is not permitted to deny an individual's right of access to their ePHI where the individual directs the information to a third-party app because the app will share the individual's ePHI for research or because the app does not encrypt the individual's data when at rest. In addition, as discussed in Question 1 above, the HIPAA Rules do not apply to entities that do not meet the definition of a HIPAA covered entity or business associate.

5. Q: Does HIPAA require a covered entity or its EHR system developer to enter into a business associate agreement with an app designated by the individual in order to transmit ePHI to the app?

A: It depends on the relationship between the app developer, and the covered entity and/or its EHR system developer. A business associate is a person or entity who creates, receives, maintains or transmits PHI on behalf of (or for the benefit of) a covered entity (directly or through another business associate) to carry out covered functions of the covered entity. An app's facilitation of access to the individual's ePHI at the individual's request alone does not create a business associate relationship. Such facilitation may include API terms of use agreed to by the third-party app (i.e., interoperability arrangements).

HIPAA does not require a covered entity or its business associate (e.g., EHR system developer) to enter into a business associate agreement with an app developer that does not create, receive, maintain, or transmit ePHI on behalf of or for the benefit of the covered entity (whether directly or through another business associate).

However if the app was developed to create, receive, maintain, or transmit ePHI on behalf of the covered entity, or was provided by or on behalf of the covered entity (directly or through its EHR system developer, acting as the covered entity's business associate), then a business associate agreement would be required.

More information about apps, business associates, and HIPAA is available at <https://hipaaqportal.hhs.gov>

FACT SHEETS

President Donald J. Trump is Strengthening America's Cybersecurity Workforce to Secure Our Nation and Promote Prosperity

ECONOMY & JOBS

Issued on: May 2, 2019

“America built the internet and shared it with the world; now we will do our part to secure and preserve cyberspace for future generations.”

President Donald J. Trump

STRENGTHENING OUR CYBER WORKFORCE: President Donald J. Trump is supporting a strong cybersecurity workforce to defend our country and promote quality job opportunities.

- President Trump has signed an Executive Order directing the creation of programs to grow and strengthen our cybersecurity workforce to meet the challenges of the 21st century.
- The Executive Order will promote cybersecurity work within the Government, including through a new President's Cup Cybersecurity Competition.
- The Administration will develop a rotational program where Federal employees can expand their cybersecurity expertise through temporary reassignments to other agencies.
- The Executive Order encourages widespread adoption of the cybersecurity workforce framework created by the National Initiative for Cybersecurity Education (NICE).
 - The NICE Framework is a helpful reference for identifying, recruiting, developing, and retaining cybersecurity talent.
- The Executive Order aims to close cybersecurity skills gaps for the cyber-physical systems that our defense and critical infrastructure rely on.
- Federal agencies will identify cybersecurity aptitude assessments that they can use to reskill employees with potential in the cybersecurity field.

- The Administration will establish the Presidential Cybersecurity Education Awards, recognizing excellent elementary and secondary school educators teaching cybersecurity-related content.

GROWING THE WORKFORCE: Training and hiring cybersecurity workers is vital to protecting our Nation's defense systems and critical infrastructure.

- Government and private-sector action is urgently needed to grow and sustain our cybersecurity workforce, which is a strategic asset to our country.
- Our cybersecurity workforce is made up of dedicated individuals in the public and private sectors who operate the critical systems needed to run and defend our country.
- More than 300,000 cybersecurity job vacancies exist in America and it is critical for our economy and security that they be filled.
- The cybersecurity field offers well-paying jobs that provide incredible opportunities for Americans.
- An inadequate cybersecurity workforce jeopardizes our critical infrastructure, national defense, and modern economy.

PROTECTING OUR SECURITY: President Trump has committed his Administration to protecting and strengthening our Nation's cybersecurity.

- The President released a National Security Strategy that highlighted cybersecurity as a priority.
- Last year, President Trump unveiled our Nation's first cyber strategy in 15 years, which included the priority to develop a superior cybersecurity workforce.
- Multiple agencies have also released strategies emphasizing the importance of cybersecurity.
- In 2017, President Trump released an Executive Order to strengthen the cybersecurity of Federal networks and our critical infrastructure.