The Office of the National Coordinator for Health Information Technology

Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2

TABLE OF CONTENTS

Introduction to the Trusted Exchange Framework and Common Agreement (TEFCA)

April 19, 2019

TABLE OF CONTENTS

Executive Summary

For decades, many health care providers, health plans, and individuals have sought a health care system that enables a patient's Electronic Health Information (EHI)[1] to flow when and where it matters most. Even though most hospitals and clinicians use electronic health records (EHRs), connectivity across systems and networks remains fragmented and interoperable uses of EHI vary. Often these variations in interoperability are not due to technical issues, but rather caused by deficits in trust between organizations and by anti-competitive behavior that results in the holding of patient EHI. Congress recognized these gaps in the 21st Century Cures Act (Cures Act)[2], and laid out a path to promote nationwide interoperability.

The Office of the National Coordinator for Health Information Technology (ONC) leads implementation of key provisions under Title IV of the Cures Act, which includes defining the requirement for health IT developers of certified health IT to publish application programming interfaces (APIs) that can be used "without special effort" to drive individual, clinician, and payer access to clinical data; and the development of a comprehensive approach to address information blocking. Additionally, in section 4003 of the Cures Act, Congress directed ONC to "develop or support a trusted exchange framework, including a common agreement among health information networks (HINs) nationally."[3] In developing a Trusted Exchange Framework (TEF) and a Common Agreement that meets the industry's needs, ONC has focused on three high-level goals:

- Provide a single "on-ramp" to nationwide connectivity.
- Enable Electronic Health Information to securely follow the patient when and where it is needed.
- Support nationwide scalability.

The TEF and the Common Agreement will be distinct components that together aim to create technical and legal requirements for sharing EHI at a nationwide scale across disparate HINs. The TEF describes a common set of principles that facilitate trust between HINs. These principles serve as "rules of the road" for nationwide electronic health information exchange. 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 individuals, clinicians, and payers. The architecture will follow a "network of networks" structure, which allows for multiple points of entry and is inclusive of many different types of health care entities. Stakeholders have the option of participating at multiple levels of the TEF and Common Agreement exchange environment, as is appropriate for them.

ONC embarked on this work by holding stakeholder discussions, public listening sessions, and an initial comment period. In January 2018, ONC released the first draft of the Trusted Exchange Framework (TEF

[1] Capitalized terms are included in the MRTCs Draft 2, Section 1 (Appendix 2).
[2] Pub. L. 114–255 (Dec 13, 2016).
[3] Id.

Draft 1) for public comment. The TEF Draft 1 outlined the minimum set of principles, terms, and conditions to support the development of a Common Agreement that would enable data exchange across disparate health information networks.

ONC reviewed all of the public comments on the TEF Draft 1[4], and has now released an updated draft package for public comment. In particular, we look forward to receiving comments on the three complementary documents: the TEF Draft 2, the Minimum Required Terms and Conditions Draft 2 (MRTCs Draft 2), and the Qualified Health Information Network (QHIN) Technical Framework Draft 1 (QTF Draft 1).[5] The TEF sets forth the aspirational principles for trusted exchange that apply to a broad audience of HINs. The MRTCs constitute the required terms and conditions that would be binding for those who elect to sign the Common Agreement. The QTF would be incorporated by reference in the Common Agreement and details the technical components for exchange among QHINs. As they serve different purposes, ONC separated these parts into three appendices so that commenters could comment on each part in context. Your comments will help inform the final versions of the TEF and the Common Agreement.

ONC is concurrently issuing a Notice of Funding Opportunity (NOFO)[6] to select a Recognized Coordinating Entity (RCE) to develop, update, implement, and maintain the Common Agreement and the QTF.

The MRTCs Draft 2 requires support for a minimum set of Exchange Purposes for sending and receiving EHI. The proposed exchange modalities for exchanging EHI include QHIN Targeted Query, QHIN Broadcast Query, and QHIN Message Delivery, which will facilitate core use cases for interoperability, including Individuals' electronic access to and use of their EHI.

Under the MRTCs Draft 2, the Common Agreement will require strong privacy and security protections for all entities who elect to participate, including entities not covered by the Health Insurance Portability and Accountability Act (HIPAA). Establishing baseline privacy and security requirements is important for building and maintaining confidence and trust that EHI shared pursuant to the Common Agreement will be appropriately protected.

The Cures Act's focus on trusted exchange is an important step forward to advance an interoperable health system that empowers individuals to use their EHI to the fullest extent, enables providers and communities to deliver smarter, safer, and more efficient care, and promotes innovation and competition at all levels.

Capitalized terms in this document are defined in Section 1 of the MRTCs Draft 2 (Appendix 2).

---

[4] Public comments on TEF Draft 1 are available at: https://beta.healthit.gov/sites/default/files/page/2018-02/Copy%20of%20tefca%20draft_public_comments%20final.xlsx

[5] The MRTCs were previously referred to as "Part B" in TEF Draft 1.

[6] The Notice of Funding Opportunity (NOFO) for the Recognized Coordinating Entity (RCE) Cooperative Agreement is available at: https://www.healthit.gov/topic/onc-funding-opportunities/trusted-exchange-framework-and-common-agreement-recognized

Introduction

The U.S. health care system must evolve to ensure individuals have access to safe, effective, and efficient care. Such a transformation requires the interoperable exchange of EHI across the care continuum. The Cures Act's[7] focus on trusted exchange is an important next step toward advancing the establishment of an interoperable health system that:

- ***Empowers individuals to use their Electronic Health Information to the fullest extent;***
- ***Enables providers and communities to deliver smarter, safer, and more efficient care; and***
- ***Promotes innovation and competition at all levels.***

For EHI to move when and where it is needed most, networks that facilitate connectivity need to agree to the right mix of technical standards, policies, and legal terms and conditions. The TEF and the Common Agreement will provide the means to build on the industry's commitment to increase trust across networks, while promoting the privacy, security, and appropriate use of EHI.

In January 2018, ONC released the TEF Draft 1 for a public comment period. The TEF Draft 1 included two parts: "Part A — Principles for Trusted Exchange", and "Part B — Minimum Required Terms and Conditions for Trusted Exchange." ONC received more than 200 public comments from stakeholders across the industry, including individuals, health care systems, payers, purchasers, care providers (e.g., long-term and post-acute care, behavioral health, community-based and safety net providers, and emergency medical services), health IT developers, federal stakeholders, and other stakeholders that enable widespread health information exchange to occur. ONC reviewed those comments and engaged with federal partners in the development of Draft 2, including the HHS Office for Civil Rights, the Department of Veterans Affairs, the Department of Defense, the Social Security Administration, the National Institute of Standards and Technology, and the Centers for Medicare & Medicaid Services. Additionally, ONC's federal advisory committee, the Health Information Technology Advisory Committee (HITAC), created a Task Force to review TEF Draft 1 and provide recommendations.[8]

The modified draft ONC released for public comment on April 19, 2019 is broken into three parts that are included as Appendices to this document. These parts are:

(i) **The TEF Draft 2 (Appendix 1):** formerly "Part A — Principles for Trusted Exchange";
(ii) **The Minimum Required Terms and Conditions (MRTCs) Draft 2 (Appendix 2):** formerly "Part B — Minimum Required Terms and Conditions for Trusted Exchange;" and
(iii) **The QHIN Technical Framework Draft 1 (Appendix 3)**

---

[7] Pub. L. 114–255 (Dec 13, 2016).
[8] The HITAC TEF Task Force recommendations are available at: https://www.healthit.gov/topic/federal-advisory-committees/recommendations-national-coordinator-health-it.

An "On-Ramp" for Data Exchange

Currently, there are more than 100 regional health information exchanges[9] and multiple national level organizations that support health information exchange. While these organizations have made significant progress in advancing interoperability, connectivity across HINs is still limited due to variations in the participation and data use agreements that govern data exchange. This results in fragmentation and gaps in interoperability. It also means that HINs, health care providers, health plans, and individuals participate in multiple forms of data exchange, which can be extremely costly and burdensome, in order to access all of an individual's data. According to a recent survey of about 70 hospitals, a majority of respondents indicated that they required three or more methods for exchanging data and about three in 10 hospitals used five or more methods to be interoperable.[10] Continuing with the status quo is not enough to ensure all stakeholders have efficient methods for engaging in health information exchange.

The TEF and the Common Agreement seek to scale health information exchange nationwide and ensure that HINs, health care providers, health plans, individuals, and many more stakeholders can access real-time, interoperable health information. A single network that comprehensively addresses all use cases for all users is not feasible for a variety of reasons, including, technical limitations, security concerns, variations in use cases, and resource limitations. However, establishing a Common Agreement that enables existing and future networks to share EHI with each other without having to join multiple networks is feasible and achievable.

The industry has done significant work to broaden the exchange of data, build trust frameworks, and develop participation agreements that enable providers to exchange data across organizational boundaries. A national exchange agreement must leverage what is working well to encourage and facilitate growth. Such an agreement must also create a balance between being overly prescriptive and unintentionally adding burden that impedes interoperability, while also minimizing the current variations that prohibit data flow. To that end, once finalized, the TEF and the Common Agreement will build on existing trust frameworks, infrastructure, and capabilities. These efforts will enable participating HINs to work together to provide an on-ramp to EHI regardless of what health IT developer an organization uses, health information exchange or network they contract with, or how far across the country an individual's records are located.

To develop a TEF and a Common Agreement that meet the needs of the industry, ONC has focused in on three high-level goals:

- **Provide a single "on-ramp" to nationwide connectivity:** Currently, many health systems and providers are in a position where they must join multiple networks that do not connect with one another in order to receive the information they need to care for their patients. These gaps prevent data from flowing and can have serious health consequences to patients. This is also financially costly to providers that must spend resources to connect to multiple networks.

[9] Julia Adler-Milstein, Sunny C. Lin, and Ashish K. Jha. The Number Of Health Information Exchange Efforts Is Declining, Leaving The Viability Of Broad Clinical Data Exchange Uncertain. Health Affairs Vol. 35 No. 7: July 2016. https://doi.org/10.1377/hlthaff.2015.1439

[10] Jordan Everson, PhD. "Measuring the Interoperability Network" Presented at ONC Annual Meeting, November 30, 2017. Washington, D.C.

Providers and individuals need a way to connect to one network, which then becomes a gateway to all other networks that have EHI on individuals and populations. The TEF and the Common Agreement seek to provide a single "on-ramp" to allow all types of health care stakeholders to join any network they choose and be able to participate in nationwide exchange.

- **Enable EHI to securely follow the patient when and where it is needed:** The TEF and the Common Agreement are designed to ease the flow of EHI, providing patients and their health care providers with secure access to their information when and where they need it most. This will help empower patients to play a more active role in managing and shopping for their care. It will also provide the foundation for improved care coordination and quality improvement among health care providers. Further, the TEF and the Common Agreement would apply appropriate safeguards that help ensure EHI is exchanged in a safe and secure environment for appropriate purposes. Addressing these gaps, which currently exist in exchange environments, would spur greater trust and confidence in electronic exchange among both providers and patients.

- **Support nationwide scalability:** The TEF and the Common Agreement aim to scale interoperability nationwide. This will be done by defining a floor of legal and technical requirements, which will enable stakeholders to access, exchange, and use relevant EHI across disparate networks. In order for this to happen, HINs must agree on a minimum set of principles, terms, and conditions that enable trust. HINs, providers, users, health IT developers, and other stakeholders may build on the minimum required terms and conditions in the TEF and the Common Agreement to create valuable services for the unique constituencies they serve. Consistent ''rules of the road'' for nationwide electronic exchange will minimize the current legal and technical policy variations that prohibit EHI from flowing as it should and allow for a more innovative, efficient, and extensible electronic marketplace.

What are the Trusted Exchange Framework (TEF) and the Common Agreement?

The TEF and the Common Agreement are distinct components that aim to create a technical and legal infrastructure for broadly sharing EHI across disparate HINs to enable nationwide data exchange. ONC will maintain the TEF and will work with an industry-based Recognized Coordinating Entity (RCE) to develop, update, implement, and maintain the Common Agreement. The RCE will establish a process to continuously identify new standards and use cases to add to the Common Agreement and will convene virtual public listening sessions to allow the industry to provide objective and transparent feedback around the development of updates to the Common Agreement. ONC will have final approval of the Common Agreement and all subsequent updates.

The Trusted Exchange Framework (TEF)

To support the Cures Act's goal of advancing health information exchange among health information networks, the TEF creates a common set of principles that are designed to facilitate trust between HINs and by which all HINs should abide in order to enable widespread data exchange. These principles are standardization; transparency; cooperation and non-discrimination; privacy, security, and patient safety; access; and data driven accountability. These principles are non-binding, but are the foundational concepts that guide the development of the Common Agreement to support the ability of stakeholders to access, exchange, and use relevant EHI across disparate HINs and sharing arrangements.

The Common Agreement

ONC intends to select and work with an industry-based entity, known as the RCE, to develop, update, implement, and maintain a Common Agreement, the terms of which will be subject to ONC approval. This Common Agreement would be based on the TEF noted above and would be comprised of three parts:

- **Minimum Required Terms and Conditions (MRTCs):** ONC will develop the MRTCs, which will consist of mandatory minimum required terms and conditions with which Qualified Health Information Networks (QHINs) may voluntarily agree to comply. The MRTCs are not a full end-to-end trust agreement. Rather, the MRTCs focus on the areas of variation among currently existing trust agreements that impede nationwide interoperability. The Common Agreement would include the MRTCs, as well as additional required terms and conditions developed by the RCE.

- **Additional Required Terms and Conditions (ARTCs):** In addition to the MRTCs, the Common Agreement would include additional required terms and conditions that are necessary for an effective data sharing agreement. These may include provisions that govern interactions between the RCE and the QHINs. For example, ARTC provisions would cover determination of fee schedules and compliance; QHIN Application, Onboarding, and Designation requirements; a process for surveilling and testing QHIN compliance with the Common Agreement; an arbitration process for adjudicating non-compliance; and an audit-appropriate process for accepting and investigating complaints, and for suspending and potentially terminating a non-compliant QHIN. The RCE will develop the ARTCs and will ensure that the ARTCs do not conflict with the MRTCs. ONC will have final approval of the Common Agreement.

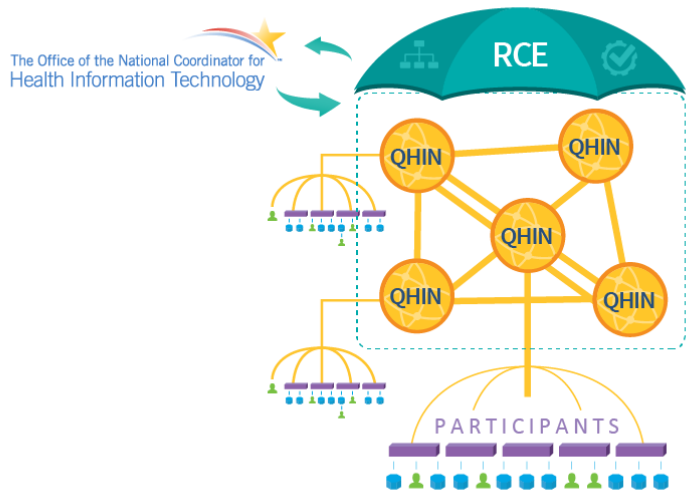
- **Qualified Health Information Network (QHIN) Technical Framework (QTF):**[11] Commenters, including the HITAC recommended that ONC refrain from naming particular standards or implementation mechanisms in the Common Agreement. To that end, the RCE will work with ONC to develop the QTF, which will be incorporated by reference in the Common Agreement. Where the Common Agreement will include and detail the underlying policies and expectations for exchange among QHINs, the QTF will focus on the technical components for exchange among QHINs, including, but not limited to identity proofing and authentication, and utilization of Connectivity Services. ONC developed the QTF Draft 1 and will work with the RCE and external stakeholders to modify and update Draft 1 per public comment.

[11] The QHIN Technical Framework Draft 1 can be found in Appendix 3 of this document.

Structure of the Trusted Exchange Framework and the Common Agreement

The TEF and the Common Agreement follow a “network of networks” structure, which allows for multiple points of entry and is inclusive of many different types of health care stakeholders. Such stakeholders include, but are not limited to:

- Health information networks
- Health information exchanges
- Individuals
- Providers
- Federal agencies
- Public health agencies
- Health plans and other payers
- Health IT developers



Stakeholders have the option of fulfilling the responsibilities for and participating as a QHIN, a Participant, a Participant Member, or an Individual User, each of which is explained in more detail below.

Recognized Coordinating Entity (RCE)

In order to meet the goals of the Cures Act, build on existing work done by the industry, and scale interoperability nationwide, ONC believes that an industry-based entity is well suited to implement and monitor compliance with the Common Agreement on behalf of ONC. Public comment generally favored this approach, and there was strong agreement that the RCE should be a not-for-profit, neutral entity that is broadly trusted, transparent, free of conflicts of interest, and can ensure a level playing field for all stakeholders.

Therefore, through a Cooperative Agreement,[12] ONC will seek eligible applicants to become the RCE and receive funding from ONC to do the following:

1. Develop a Common Agreement that includes the MRTCs and ARTCs, for ONC approval and publication to HealthIT.gov and in the Federal Register.

2. Virtually convene public listening sessions that will allow industry stakeholders to provide objective and transparent feedback to the RCE.

3. Identify and monitor QHINs that voluntarily agree to sign and adopt the Common Agreement.

4. Implement an ONC-approved process to adjudicate QHIN noncompliance with the Common Agreement, up to and including removal from ONC’s public directory on HealthIT.gov.

---

[12] The Notice of Funding Opportunity (NOFO) for the Cooperative Agreement was released with the TEF Draft 2 and MRTCs Draft 2 and can be found here.

5. Implement a process to update the Common Agreement, as needed, for ONC final approval and publication to HealthIT.gov and in the Federal Register.

6. Modify and update the QHIN Technical Framework Draft 1, for ONC approval, to detail proposed technical components for exchange among QHINs as required by the latest version of the MRTCs.

7. Propose strategies that an RCE could employ to sustain the Common Agreement at a national level after the expiration of the term of the Cooperative Agreement.

The Cooperative Agreement will be a four (4) year award and will include requirements for the RCE to demonstrate a commitment to transparent, fair, and nondiscriminatory data exchange through organizational policies and governing structures. Specifically, to avoid conflict of interest, ONC will require the RCE to meet and maintain certain independence criteria through the term of the Cooperative Agreement, such that once an applicant is awarded to be the RCE it may not be affiliated with a QHIN as long as it is the RCE. Additionally, the RCE will employ organizational policies that prevent conflicts of interest. ONC intends to work closely with the chosen RCE, and will be continually involved in implementation of the Common Agreement throughout the duration of the term of the Cooperative Agreement.

Qualified Health Information Networks (QHIN)

The TEF Draft 1 introduced the concept of a QHIN, which is an entity with the technical capabilities to connect Participants on a nationwide scale. A QHIN must meet the definition of a Health Information Network (HIN) and satisfy all of the conditions of the Common Agreement and accompanying QTF. These include utilization of Connectivity Services[13] for sending and receiving EHI, responding to requests for EHI for all of the Exchange Purposes described in the Common Agreement, and adhering to all privacy and security requirements.

In order to apply for QHIN Designation, a HIN must also meet certain prerequisites, including already operating a network that provides the ability to locate and transmit EHI between multiple persons or entities electronically, with existing persons or entities exchanging EHI in a live clinical environment; and providing the RCE with a written plan of how it will achieve all of the requirements of the Common Agreement within a specified time period. A HIN must submit a QHIN Application to the RCE that documents that it meets these prerequisites, and the RCE must certify in writing that the HIN in question has satisfied these requirements. Once the RCE has approved a QHIN Application, the HIN becomes a Provisional QHIN and is assigned to a Cohort to complete the remainder of the requirements in the Common Agreement and QTF. A Provisional QHIN is only Designated a QHIN once the RCE has confirmed and documented that the Provisional QHIN in question has satisfied the requirements of the Common Agreement and the QTF. [14] The RCE will also be responsible for monitoring QHINs on an ongoing basis and adjudicating noncompliance with the Common Agreement up to and including removal of the QHIN from ONC's public directory on HealthIT.gov, when necessary. ONC requests public comment on this proposed process.

[13] QHINs may contract with one or more external entities that provide Connectivity Services.

[14] More details on this process can be found in Section 2.1 of the MRTCs Draft 2.

A QHIN's ability to operate successfully and efficiently is crucial to ensuring all Individuals and providers have appropriate and real-time access to EHI. Therefore, it is critical that QHINs fully understand the breadth and scope of their responsibilities before applying for QHIN Designation. Ensuring their capabilities and compliance to the Common Agreement through testing, rigorous on-boarding, and monitoring will be critical to ensure continuity of services among Participants and Participant Members. Organizations that apply to be a QHIN should do so with an understanding of the infrastructure and personnel necessary to support interoperability at a nationwide scale.

Participants, Participant Members, and Individual Users

The TEF and the Common Agreement seek to serve many different stakeholders across the country who have unique needs and constituencies. As such, the TEF, MRTCs, and QTF do not dictate the internal requirements or business structures of QHINs, but rather provide QHINs flexibility to provide different services and support different stakeholders. Not all QHINs must be composed of the same types of Participants and Participant Members, and depending on its internal structure, there could be several different amalgamations of Participants and Participant Members within and across QHINs. Entities should consider what makes the most sense for their internal business model when determining which QHIN they want to join.

- **Participants:** Participants may include persons or entities that have entered into a contract to participate in a QHIN. Some examples of Participants could include, but are not limited to, a HIN, a health system, a health IT developer, a payer, or a federal agency.
- **Participant Members:** Participant Members may include persons or entities that use the services of a Participant to send and receive EHI. For example, if a QHIN is composed of health information exchanges, the health information exchange would be the Participant, and those who use the health information exchange services, (such as health systems, ambulatory providers, health IT developers, payers, and others) are the Participant Members. Alternatively, a health IT developer could be a direct Participant of a QHIN, in which case, the Participant Members may be the provider practice that uses the health IT developer's software or services.
- **Individual Users:** An Individual User represents an actual person who is the subject of the EHI, such as a patient, health plan member, or a patient representative. Individual Users may have a Direct Relationship with the QHIN, Participant, or Participant Member, depending on the structure of the QHIN to which they belong, but they are not themselves considered Participants or Participant Members.

What can the Common Agreement be used for?

The Common Agreement requires that QHINs support a minimum set of exchange modalities and Exchange Purposes for sending and receiving EHI. These modalities and purposes facilitate core use cases for interoperability such as Individuals' electronic access to and use of their EHI. ONC received a number of public comments on the proposed exchange uses included in TEF Draft 1 and we have made modifications consistent with this feedback. We request comment on these updates.

Exchange Modalities

TEF Draft 1 required that QHINs support three types of exchange modalities for exchanging EHI — Targeted Query, Broadcast Query, and Population-Level Data Exchange. Commenters were supportive of the inclusion of both Targeted Query, which allows for queries to a known location, and Broadcast Query, which supports situations where the location of the EHI is unknown.

However, commenters expressed concern regarding the relative maturity of Population-Level Data Exchange. While important for modern health care delivery and to the Cures Act's long term goals for quality measurement, risk analysis, research, and public health, the industry is still working to mature this use case in a network exchange context. Therefore, this use case has been removed from the MRTCs. Given the nature and development of the technical specifications to support this use case, it is anticipated that most population-level queries (i.e., a data request for a population of one party's patients) would occur using APIs. It is further expected that these data use relationships and the associated service levels would be established through mutual contracts consistent with the HIPAA Privacy and Security Rules.

Additionally, ONC received a number of requests from commenters to include a "push-based" exchange modality in the TEF and the Common Agreement. Commenters noted that push transactions play a vital role in supporting transitions of care and public health use cases and would be necessary to fully support required Public Health reporting. Therefore, ONC has included QHIN Message Delivery, which supports instances where a QHIN sends EHI to one or more QHINs for delivery. We request comment on the inclusion of QHIN Message Delivery and its definition.

The three exchange modalities included in the MRTCs Draft 2 are as follows:

- **QHIN Targeted Query:** a QHIN's electronic request for EHI (sometimes referred to as a "pull") from specific QHINs in the context of the Common Agreement to the extent permitted by the Common Agreement and Applicable Law.

- **QHIN Broadcast Query:** a QHIN's electronic request for EHI in the context of the Common Agreement that requests EHI from all other QHINs to the extent permitted by the Common Agreement and Applicable Law.

- **QHIN Message Delivery:** the electronic action of a QHIN to deliver EHI to one or more QHINs, or to send EHI to one or more QHINs for delivery to one or more Participants or Individuals (sometimes referred to as a "push"). Notwithstanding the foregoing, QHIN Message Delivery does not include responses to any QHIN Query.

While QHINs must have the capability to perform Broadcast Query, Targeted Query, and Message Delivery, they may use different exchange modalities for different situations. For example, a provider following-up with a patient who has been hospitalized may only want EHI from the specific hospital visit, whereas a provider seeing a new patient may want EHI from all providers the individual has seen. QHINs should provide as much flexibility to their Participants and Participant Members as possible to support broad interoperability for multiple use cases. We request comment on these exchange modalities and their definitions.

Exchange Purposes

The TEF Draft 1 included Treatment, Payment, Health Care Operations, Public Health, Individual Access (as those terms are defined by the HIPAA Privacy Rule), and Benefits Determination, as required Exchange Purposes.[15, 16] However, many commenters felt that requiring the full Payment and Health Care Operations Exchange Purposes were too burdensome to implement immediately. Therefore, the Common Agreement will initially require exchange for only a subset of activities in Payment (Utilization Review) and Health Care Operations (Quality Assessment and Improvement, and Business Planning and Development) as defined in the HIPAA Privacy Rule. The requirements to exchange for purposes of Treatment, Public Health, and Benefits Determination will remain the same as proposed in TEF Draft 1. The Exchange Purpose described as Individual Access in TEF Draft 1 has been modified to Individual Access Services, which includes the HIPAA Privacy Rule right for an individual to view or obtain a copy of his or her Protected Health Information from Covered Entities. The Individual Access Services Exchange Purpose now includes a corresponding requirement for non-HIPAA entities that elect to participate in the Common Agreement. We request comment on the scope of these Exchange Purposes.

QHINs, Participants, and Participant Members have a duty to respond to all requests for EHI they receive for any of the Exchange Purposes with the EHI they have available. However, Participants and Participant Members that only provide Individual Access Services are only required to respond to requests for Individual Access Services.

Phased Approach

Over time, ONC intends to phase in new exchange modalities and Exchange Purposes in the Common Agreement to support additional use cases. A phased approach will allow the industry and potential signatories to adequately prepare to incorporate the necessary standards into their architectures, as well as resolve some of the variation in standards and policies that exist today. ONC intends to work with the National Institute of Standards and Technology (NIST) and the industry on pilots focusing on use cases of the TEF and the Common Agreement.

As ONC phases in new requirements, QHINs, Participants, and Participant Members are in no way limited from voluntarily offering additional exchange modalities and services or from entering into point-to-point or one-off agreements between organizations that are different from the Common Agreement's MRTCs, provided that such agreements do not conflict with the policies of the Common Agreement. ONC

[15] We note that TEF Draft 1 used the term "permitted purposes." In this draft and going forward, this term will now be replaced with "Exchange Purposes."
[16] See 45 CFR 164.501 Definitions

structured the initial requirements to address the areas of greatest need while also allowing existing HINs and trusted exchange networks to vary as appropriate to meet more specialized use cases that are specific to their own Participants and Participant Members. The TEF and the Common Agreement do not limit the ability of HINs to innovate and build additional services that would provide value to their users and support their long-term sustainability.

The Common Agreement's Relationship to HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[17] Privacy Rule and HIPAA Security Rule serve as the foundation for federal protection of the privacy and security of most individually identifiable health information.[18] However, the HIPAA Rules apply only to organizations defined in the Rules as Covered Entities and Business Associates.

The Cures Act emphasizes the need to improve patients' access to their EHI.[19] Many non-HIPAA entities, such as developers of smartphone apps, offer useful and efficient services to individuals who elect to use them as a means to access their EHI. These services allow individuals to play a greater role in managing their own health and shopping for coverage or care. It is essential that individuals have trust in these organizations and the use of these technologies that can ultimately enhance the quality of their care.

Individuals, health care providers, health plans, and networks may not be willing to exchange data through the Common Agreement if smartphone app developers and other non-HIPAA entities present privacy or security risks because they are not obligated to abide by the HIPAA Rules. In order to meet the goals of the Cures Act as well as to help address these concerns and encourage robust data exchange that will ultimately improve the health of patients, the Common Agreement requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. This will bolster data integrity, confidentiality, and security, which is necessary given the evolving cybersecurity threat landscape.

Federal agencies that are not subject to HIPAA may elect to be a Participant or Participant Member. In these instances, such agencies would not be required to comply with the HIPAA Rules referenced in the Common Agreement. However, they must comply with all privacy and security requirements imposed by applicable federal law.

Establishing baseline privacy and security requirements shared by all QHINs, Participants, and Participant Members is important for building and maintaining confidence and trust that EHI shared pursuant to the Common Agreement is appropriately protected.

---

[17] Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996).
[18] ONC is working with the HHS Office for Civil Rights (OCR) to ensure that where applicable, electronic health information exchange, as proposed in the Common Agreement, does not conflict with relevant provisions of the HIPAA Rules.
[19] Section 4006 of the 21st Century Cures Act.

Agreement Structure

The Common Agreement is an agreement between QHINs and the RCE; however, it will include the responsibility of a QHIN to ensure that Participants and Participant Members abide by certain mandatory minimum obligations. To implement these obligations, data sharing agreements between QHINs and Participants (Participant-QHIN Agreements), and Participants and Participant Members (Participant Member Agreements), respectively, will need to incorporate these mandatory minimum obligations.

ONC recognizes that this overall approach may necessitate modifications to existing data sharing agreements and trust frameworks. Such changes are necessary to meet Congress' objectives under the Cures Act and will enable more robust exchange of EHI.

Participants and Participant Members that are Covered Entities or Business Associates must amend existing Business Associate Agreements (BAAs), or enter into or amend other types of data use agreements to address the mandatory minimum obligations.[20] Additionally, Individual Users have exchange rights and obligations; however, they would not be expected to sign a data sharing agreement.

In addition, we note that the MRTCs do not supplant any responsibilities of Covered Entities and Business Associates to comply with the HIPAA Rules, and the Common Agreement does not prohibit entities from entering into additional agreements to exchange data for uses that are outside the scope of the Common Agreement.

What Privacy and Security Requirements are Included in the Common Agreement?

The MRTCs Draft 2 includes provisions that address QHIN, Participant, and Participant Member privacy and security practices in order to ensure all connections within a QHIN's network are trusted and secure. There are MRTC provisions that address meaningful choice, written privacy summaries, data integrity, identity proofing, access control, user authentication, and auditing consistent with industry best practices. We request comment on all aspects of privacy and security as addressed in the MRTCs, and particularly on the proposed policies below.

[20] Where other statutes or regulations require use of specific standards for particular purposes or use cases, the Common Agreement would not alter these other regulations, and should not be construed as altering any organization's compliance requirements for these other regulations.

Meaningful Choice and Written Privacy Summary

Given the anticipated increased access in EHI exchange through the Common Agreement, it is critical that Individuals have the opportunity to understand and make informed choices about where, how, and with whom their EHI is shared. Therefore, the MRTCs Draft 2 requires that QHINs, Participants, and Participant Members provide Individuals with the opportunity to exercise Meaningful Choice to request that their EHI not be Used or Disclosed via the Common Agreement, except as required 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. This choice must be respected on a prospective basis.

Additionally, all QHINs, Participants, and Participant Members who provide Individual Access Services must publish and make publicly 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 an explanation of how an Individual can exercise their Meaningful Choice and who they may contact for more information about the entity's privacy practices.

Breach Notification Requirements

The MRTCs Draft 2 requires that QHINs, Participants, and Participant Members comply with the Breach notification requirements pursuant to the HIPAA Breach Notification Rule at 45 CFR §164.400-414, regardless of whether or not they are a Covered Entity or Business Associate. Further, each QHIN shall notify the RCE, as well as other QHINs, Participants, Participant Members, and Individual Users who may have been affected by the Breach without unreasonable delay and in accordance with Applicable Law. Where applicable, actors in the Common Agreement may be subject to the Federal Trade Commission Health Breach Notification Rule, which applies to a vendor of personal health records (PHRs), a PHR-related entity, or a third-party service provider for a vendor of PHRs or a PHR-related entity. The Breach notification requirements of the Common Agreement do not supplant any HIPAA or FTC breach reporting requirements or responsibilities.

Minimum Security Requirements

The MRTCs Draft 2 requires that QHINs comply with the HIPAA Privacy and Security Rules as it pertains to EHI. Also, QHINs must evaluate their security program for the protection of Controlled Unclassified Information (CUI), and develop and implement an action plan to comply with the security requirements of the most recently published version of the NIST Special Publication 800-171 (Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations). A CUI category includes EHI. This Publication provides principle guidelines to federal government-wide requirements for CUI, and entities which handle EHI are required to demonstrate the security controls and be compliant with the NIST 800-171 requirements of the most recent publication.

In addition, as part of its ongoing security risk analysis and risk management program, QHINs shall review the most recently published version of the HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework. The NIST Cybersecurity Framework is guidance that was developed with industry for organizations to better manage and reduce cybersecurity risks. Additionally, it was designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders. The NIST Cybersecurity Framework is based on existing standards, guidelines, and practices.

To the extent the QHIN's risk analysis identifies any risks, vulnerabilities, or gaps in the QHIN's compliance with the HIPAA Privacy and Security Rules or other Applicable Law, the QHIN would be required to 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 any such evaluation. This evaluation would not be required for Participants and Participant Members. QHINs are to evaluate their security program on at least an annual basis.

Participants and Participant Members must comply with the HIPAA Privacy and Security Rules and Applicable Law, when applicable. However, regardless of whether they are a Covered Entity or Business Associate, Participants and Participant Members must take reasonable steps to promote the confidentiality, integrity, and availability of EHI, including 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. ONC is requesting public comment regarding appropriate security controls for Participants or Participant Members in the Common Agreement, specifically regarding EHI received from federal agencies.

No EHI Used or Disclosed Outside the United States

ONC seeks public comment on how the Common Agreement should handle potential requirements for EHI that may be used or disclosed outside the United States. For example, there are federal agencies and other multinational entities that have employees receiving care outside the United States, and their health care providers may want to request the patients' health care records that are located within the United States. Currently, the MRTCs Draft 2 does not permit QHINs to Use or Disclose EHI outside the United States, except to the extent that an Individual User requests his or her EHI to be Used or Disclosed outside of the United States. ONC requests comment on reasonable applicability of similar limitations to preserve the security and privacy of EHI sent, stored, maintained, or used by Participants and Participant Members while also preserving the rights of each individual with respect to that EHI.

Security Labeling

ONC received a significant number of comments requesting that ONC focus its efforts on addressing security labeling, especially for sensitive protected data (e.g., HIV/AIDs, substance abuse, or mental health). Currently, security labels can be placed on data to enable an entity to perform access control decisions on EHI such that only those persons appropriately authorized to access the EHI are able to do so. 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 electronically labeled;
- Any EHI of patients considered to be minors shall be electronically labeled;
- The data holder responding to a request for EHI is obligated to appropriately apply electronic security labels to the EHI;
- At a minimum, such 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; and
- Labeling shall occur at the highest (document or security header) level.

While the DS4P Implementation Guide[21] was included as an optional criterion in the 2015 Edition of certification criteria, ONC recognizes that the use of the DS4P IG has yet to reach wide adoption. Therefore, we have limited the proposed requirement to four (4) of the most commonly requested sensitive data categories. ONC is requesting public comment regarding the use of confidentiality codes and security tags and/or reasonable alternatives that would ultimately promote the ability to exchange sensitive data under the Common Agreement.

Major Updates to Draft 2 of the TEF and MRTCs

	TEF Draft 1	TEF and MRTCs Draft 2
QHIN Technical Framework (QTF)	• Standards were included in the TEF itself.	• Added the QTF, which details technical and functional components for exchange among QHINs. • The QTF would be incorporated by reference in the Common Agreement.
Timelines	• QHINs have *12 months* to update agreements and technical requirements.	• QHINs have *18 months* to update agreements and technical requirements.
Exchange Modalities	• Targeted Query • Broadcast Query • Population-Level Data Exchange	• Targeted Query (now referred to as QHIN Targeted Query) • Broadcast Query (now referred to as QHIN Broadcast Query) • QHIN Message Delivery
Exchange Purposes	• Treatment • Payment • Health care Operations • Public Health • Benefits Determination • Individual Access	• Treatment • Quality Assessment and Improvement • Business Planning and Development • Utilization Review • Public Health • Benefits Determination • Individual Access Services
QHIN Prerequisites	A QHIN must meet all 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.	A HIN that intends to apply for QHIN Designation must meet the following prerequisites: • Be a HIN that already operates a network that provides the ability to locate and transmit EHI between multiple persons and/or entities electronically; • Such persons and/or entities are already exchanging EHI in a live clinical environment using the network; • The HIN has provided reasonable evidence that exchange of EHI using its network is occurring in accordance with Applicable Law; and • The HIN has provided a reasonable plan in writing of how it will achieve all of the applicable requirements of the Common Agreement within the required period.

[21] HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, May 2014
https://www.hl7.org/implement/standards/product_brief.cfm?product_id=354

	TEF Draft 1	TEF and MRTCs Draft 2
Fees	• QHINs must use reasonable and non-discriminatory criteria if it charges any fees to another QHIN. • QHINs *may* charge other QHINs to respond to queries for Treatment, Payment, and Health care Operations. • QHINs *may not* charge other QHINs to respond to queries for Individual Access, Public Health, or Benefits Determination. • QHINs *may not* impose any other fee on the Use or further Disclosure of the EHI once it is accessed by another QHIN.	• QHINs must use reasonable and non-discriminatory criteria if it charges any fees to another QHIN. • QHINs *may not* charge another QHIN any amount to exchange EHI for Individual Access Services. • QHINs *may not* impose any other fee on the Use or further Disclosure of the EHI once it is accessed by another QHIN. *Any additional requirements around fees will be specified in the ARTCs, which will be developed by the RCE and approved by ONC.

What are the Next Steps?

On April 19, 2019, ONC released TEF Draft 2, the MRTCs Draft 2, the QTF Draft 1, and the Notice of Funding Opportunity (NOFO) for the RCE Cooperative Agreement. ONC is accepting public comment on TEF Draft 2, the MRTCs Draft 2, and the QTF Draft 1 for a period of 60 days. Comments are due on June 17, 2019. Entities interested in applying for the RCE Cooperative Agreement must submit their application by June 17, 2019.

ONC will consider comments received on or prior to the comment deadline. ONC will update and release a Final TEF, while working with the RCE and industry stakeholders to modify and update the MRTCs Draft 2 and the QTF Draft 1. When combined, the MRTCs, ARTCs, and QTF will form the Common Agreement Draft 1. ONC and the RCE will release the Common Agreement Draft 1 for a round of public comment. Subsequently, ONC and the RCE will work with industry stakeholders to release Version 1 of the Common Agreement. See table below.

Key Steps for the Trusted Exchange Framework and Common Agreement

This table clarifies the process and versioning of major documents related to the Trusted Exchange Framework and the Common Agreement. It also summarizes the responsible entities and opportunities for public involvement.

Major Document	Responsible Entity and Related Action	Timing of Step
Draft Trusted Exchange Framework (including Part A, Principles for Trusted Exchange, and Part B, Minimum Required Terms and Conditions)	ONC developed and released for public comment	Completed 1/5/18
Trusted Exchange Framework (TEF) – Draft 2 (includes Principles for Trusted Exchange)	ONC developed and is releasing for public comment	April 19, 2019
Minimum Required Terms and Conditions (MRTCs) – Draft 2 (previously called TEF Part B)	ONC developed and is releasing for public comment	April 19, 2019
QHIN Technical Framework – Draft 1	ONC developed and is releasing for public comment	April 19, 2019
Notice of Funding Opportunity – Trusted Exchange Framework and Common Agreement – Recognized Coordinating Entity (RCE) Cooperative Agreement	ONC publishing with a 60-day application period	April 19, 2019
Trusted Exchange Framework (TEF) – FINAL (includes Principles for Trusted Exchange)	ONC publishes final document	Future Step

Major Document	Responsible Entity and Related Action	Timing of Step
Common Agreement – Draft 1 (includes MRTCs developed by ONC and ARTCs developed by RCE and approved by ONC	RCE develops, ONC approves, then RCE releases for public comment	Future Step
QHIN Technical Framework – Draft 2	RCE develops, ONC approves, then RCE releases for public comment	Future Step
Common Agreement – FINAL Version 1	RCE develops, ONC approves, then RCE releases for production. This version will be published in the Federal Register.	Future Step
QHIN Technical Framework – FINAL Version 1	CE develops, ONC approves, then RCE releases for production	Future Step

Appendix 1:
The Trusted Exchange Framework (TEF)

DRAFT 2

April 19, 2019

TABLE OF CONTENTS

Overview

The 21st Century Cures Act[22] (Cures Act) directs the Office of the National Coordinator for Health Information Technology (ONC) to "develop or support a trusted exchange framework, including a common agreement among health information networks (HINs) nationally." In January 2018, ONC released the first draft of the Trusted Exchange Framework (TEF Draft 1) for public comment. The TEF Draft 1 included two parts: "Part A — Principles for Trusted Exchange," and "Part B — Minimum Required Terms and Conditions for Trusted Exchange."

This Draft of the TEF (TEF Draft 2) includes only "Part A — Principles for Trusted Exchange." ONC also released a revised draft of "Part B — Minimum Required Terms and Conditions for Trusted Exchange," which is now entitled the Minimum Required Terms and Conditions (MRTCs) (Appendix 2).

The Trusted Exchange Framework (TEF) Draft 2 describes a common set of principles that facilitate trust between HINs. These principles serve as "rules of the road" for nationwide electronic health information exchange. Broad adherence to these principles will minimize variation in technical and legal policies that restrict the secure flow electronic health information (EHI) where and when it is needed and allow for a more innovative, efficient, and extensible electronic marketplace. This would also support the ability of patients and health care providers to access EHI when and where it is needed most and help provide the foundation for improved care coordination and quality improvement.

ONC is accepting comments on the TEF Draft 2.

The six principles are:

- **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 Patient 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 seamless 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.

Each principle is described in detail below and includes lettered sub-principles.

[22] Pub. L. 114–255 (Dec 13, 2016).

Principles for Trusted Exchange

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

1) Adhere to applicable standards for EHI and interoperability that have been adopted by the U.S. Department of Health & Human Services (HHS), approved for use by ONC, or identified by ONC in the Interoperability Standards Advisory (ISA).[23,24]

HINs should adhere to federally adopted standards for EHI and interoperability. Specifically, HINs should first look to use standards adopted by HHS, then those approved by ONC through the proposed standards version advancement process as part of the ONC Health IT Certification Program (Certification Program), and finally, those identified in the ISA. In instances where none of the above references include applicable standards, HINs should then consider voluntary consensus or industry standards that are readily available to all stakeholders, thereby supporting robust and widespread adoption. Consistent adherence to these standards will ensure improved usability and access to EHI.

2) Implement technology in a manner that makes it easy to use and that allows others to connect to data sources, innovate, and use data to support better, more person-centered care; smarter spending; and healthier people.

HINs should use standards-based technology to exchange EHI with other HINs. To minimize variation in how standards are implemented, such technology should be implemented in accordance with authoritative best practices published by an applicable standards development organization (SDO). By doing so, it will make it easier for HINs to connect to each other and with their users.

HINs should, to the extent possible, ensure that the data exchanged within their own network and with other HINs meets minimum quality standards by using testing and onboarding programs to verify minimum quality levels. HINs may consider using tools, such as ONC's C-CDA scorecard tool for testing the technical conformance of C-CDAs or the Patient Demographic Data Quality Framework (PDDQ) to evaluate the quality of patient demographic data.[25,26] They may also consider developing tools to test the quality of data exchange using Health Level Seven (HL7®) Fast Healthcare Interoperability Resources (FHIR®) APIs.

---

[23] Note: The HIPAA and ACA administrative simplification electronic data interchange provisions are implemented by HHS through the Division of National Standards (DNS) at CMS, which adopts certain transactions standards that are required to be used when electronic data are exchanged in support of covered administrative transactions. These transactions include: health care claims or equivalent encounter information; eligibility for a health plan; enrollment and disenrollment in a health plan; health care electronic funds transfers (EFT) and remittance advice; referral certification and authorizations; health care claims status; coordination of benefits; health plan premium payments; and Medicaid pharmacy subrogation. HIPAA covered entities must use the adopted standards, generally either an ASC X12N or NCPDP standard (for certain pharmacy transactions) in conducting transactions.

[24] ONC, Interoperability Standards Advisory (ISA), available at: https://www.healthit.gov/isa/

[25] ONC, Consolidated-Clinical Document Architecture (C-CDA_ Scorecard, available at: https://sitenv.org/ccda-smart-scorecard/

[26] ONC, Patient Demographic Data Quality Framework (PDDQ), available at: https://www.healthit.gov/playbook/pddq-framework/

These types of testing programs can help ensure that high quality data is exchanged both within and across HINs.

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

A. Make terms, conditions, and contractual agreements that govern the exchange of EHI easily and publicly available.

All parties desiring to exchange EHI through a HIN should know, prior to engaging with a HIN, the responsibilities of being a participant in a HIN and the protections that have been put in place to ensure that privacy and security requirements are followed. HINs should make these and other terms and conditions for participating in their network easily and publicly available via their website; meaning they are accessible to the general public.

B. Specify and have all HINs agree to the uses and disclosures for exchanging EHI.

Because HINs are often either business associates of covered entities or a business associate subcontractor of a business associate, their Business Associate Agreements (BAAs) specify the uses and disclosures for which their HIN may be used to exchange EHI. While some HINs currently support all of the uses and disclosures specifically addressed in the HIPAA Privacy Rule, others may only support use and disclosure of electronic protected health information (ePHI) for treatment purposes. When HINs have varying, allowable uses and disclosures in their own data use agreements, the full exchange of EHI between those HINs is limited. Therefore, HINs should specify the minimum set of uses and disclosures they support. These should be specified in the HINs legal agreement with their participants, made open and transparent consistent with Principle 2.A, and clearly communicated when EHI is requested or sent between participants and HINs.

C. Publish, keep current, and make publicly available the HIN's privacy practices.

Ensuring that participants of HINs understand the privacy practices of each HIN will help to build trust that EHI will be protected and will not be used in ways that they do not expect. Consequently, HINs and their participants should ascribe to the following privacy practices:

(a) HINs should comply with all applicable laws regarding the use and disclosure of EHI.
(b) HINs should clearly specify the minimum set of uses and disclosures for exchanging EHI and, for non-treatment purposes, limit the use of EHI to the minimum amount required.
(c) HINs should not impede the ability of individuals to access their EHI and direct it to designated third parties, as required by the HIPAA Privacy Rule.
(d) HINs should provide a method by which individuals can exercise meaningful choice regarding the exchange of EHI about them and ensure that such individual's choice is honored on a prospective basis, consistent with applicable law.

These privacy practices are critical to effective data exchange. To further promote transparency, HINs should publish and make publicly available a written notice in plain language, similar to ONC's Model

Privacy Notice[27] that describes their privacy practices regarding the access, exchange, use, and disclosure of EHI.

D. When necessary, conduct any arbitration processes with other HINs in an equitable, transparent manner.

It may be necessary to address behavior that violates data sharing agreements among HINs. When a violation of one of these agreements occurs, HINs should ensure that an arbitration process for addressing such violations is clearly defined in their respective agreements and subsequently followed. Such arbitration processes should be equitable and transparent to all parties, particularly prior to signing an agreement and binding an entity to such processes.

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.

A. Do not seek to gain competitive advantage by limiting access to individuals' EHI.

HINs should not treat individuals' EHI as an asset that can be restricted in order to obtain or maintain a competitive advantage. For example, HINs should not withhold health information requested for treatment, payment, and health care operations purposes from health care providers or health plans that are outside of their preferred referral networks or outside of a value-based payment arrangement, such as by establishing internal policies and procedures and knowingly making misleading claims regarding privacy laws or regulations as a pretext for not sharing EHI. Likewise, HINs should not implement technology in a manner that limits the sharing of EHI. HINs should practice data reciprocity (e.g., have a willingness to share EHI themselves as opposed to only participating in an exchange relationship only for the purpose of receiving health information from others). In addition, fees and other costs should be reasonable and should not be used to interfere with, prevent, or materially discourage the access, exchange, use, or disclosure of EHI within a HIN or between HINs.

While HINs must comply with applicable laws (including the applicable HIPAA Rules), they should not use contract provisions or proprietary technology implementations to unduly limit connectivity with other HINs such as by preventing the appropriate flow of health information across technological, geographic, or organizational boundaries for health and care, safety, quality measurement, or payment.

HINs should not use methods that discourage or impede appropriate health information exchange with competitors. This includes throttling the speed with which data is exchanged purely for competitive reasons, limiting the data elements that are exchanged with health care organizations that may be their competitor or a competitor of one of their participants, or by requiring burdensome testing requirements designed to unfairly deter or discourage connections that do not benefit the HIN.

[27] ONC Model Privacy Notice, available at: https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf.

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.

A. Ensure that EHI is exchanged and used in a manner that promotes safe care, including consistently and accurately matching EHI to an individual.

Certain health plans and health care providers, and their business associates must follow the HIPAA Rules to safeguard individual ePHI. However, EHI is increasingly collected, shared, or used by new types of organizations beyond the traditional health care organizations covered by the HIPAA Rules. Privacy and security should be a foundation for all health care stakeholders, including those that are not subject to HIPAA.

Ensuring the integrity of EHI is paramount to providing safe care. When EHI is exchanged, safe care begins with correctly matching the data to an individual so that care is provided to the right individual based on the right information. Sophisticated algorithms that use demographic data for matching are the primary method for connecting data to an individual. To support accurate matching, HINs should agree upon and consistently share a core set of demographic data each time that EHI is requested. Likewise, participants of HINs should ensure that the core set of demographic data is consistently captured for all individuals so that it can be exchanged in a standard format and used to accurately match data.

In addition to the importance of the integrity of demographic data, overall EHI integrity is a key component of promoting patient safety in electronic exchange. Where possible, standard nomenclatures should be used and exchanged in a data format that is consumable by a receiving system, such as a C-CDA or via FHIR APIs. Further, clinicians should update individuals' EHI in their EHR to ensure that medications, allergies, and problems are up to date prior to exchanging such data with another organization. To the extent possible, HINs should utilize testing and onboarding processes for their participants that seek to establish a high level of data quality.

B. Ensure providers and organizations participating in data exchange have confidence that individuals have the opportunity to exercise meaningful choice, if and when it is needed, prior to the exchange of EHI.

When required by federal or state law, a HIN's ability to appropriately and electronically capture an individual's meaningful choice to exchange or use their EHI will engender trust amongst other entities seeking to exchange with that network.

The HIPAA Privacy Rule generally does not require covered entities to get an individual's consent or authorization before using or disclosing ePHI for treatment, payment, and health care operations purposes. While the Privacy Rule generally permits covered health care providers to give individuals the choice as to whether their health information may be disclosed to other covered entities or that covered entity's business associate for those purposes, some federal and state laws require health care providers to obtain an individual's written consent before they disclose or exchange an individual's EHI to other people and organizations, even for treatment and payment purposes. For example, for some health conditions such as human immunodeficiency virus (HIV), mental health, or genetic testing, state laws generally impose a more stringent standard (e.g., requiring consent from the individual) than HIPAA. Additionally, under 42 CFR Part 2, subject to certain exceptions, federally assisted "Part 2 programs" (certain substance use disorder treatment programs) are required to obtain an individual's consent to disclose or re-disclose health information related to substance use disorder information, such as treatment for addiction.

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

A. Do not impede or put in place any unnecessary barriers to the ability of individuals to access and direct their EHI to designated third parties, and to learn how information about them has been access or disclosed.

HINs who maintain EHI should (1) enable individuals to easily and conveniently access their EHI; (2) enable individuals to direct their EHI to any desired recipient they designate; and (3) ensure that individuals have a way to learn how their information is shared and used. This principle is consistent with the HIPAA Privacy Rule, which requires covered entities to provide PHI to individuals in the form and format in which they request it, if it is readily producible in that form and format. This means that if it is stored electronically, individuals can request it and access it electronically at virtually no cost.

Under the HIPAA Privacy Rule, covered entities are also required to transmit an individual's PHI to a third party when directed by the individual. Covered entities may not impose limitations through internal policies and procedures that unduly burden the individual's right to get a copy or to direct a copy of their health information to a third party of their choosing.[28] The HIPAA Privacy Rule also requires a covered entity to have Notices of Privacy Practices available to inform individuals about how PHI is use and disclosed by the entity, as well as the individual's rights with respect to their PHI.

Much like the HIPAA law provisions on individuals' access to their health information are important, for purposes of this Principle, HINs should not limit third party applications from accessing individuals' EHI via an API when the application complies with the applicable data sharing agreement requirements and the individual has directed the entity to disclose a copy of ePHI to the application. Likewise, it is also important for individuals to be able to obtain information about how their EHI has been used and disclosed. As the Fair Information Practice Principles (FIPPs) of the Nationwide Privacy and Security Framework on openness and transparency states, "[p]ersons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format."[29] HINs should commit to following this principle and should provide such opportunities electronically whenever possible, particularly when an individual makes the request electronically.

---

[28] See 45 CFR 164.524

[29] *Nationwide Privacy and Security Framework for EHI Exchange of Individually Identifiable Health Information*, http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf (December 15, 2008) quoted Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973): http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

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.

A. Enable participants to request and receive multiple patient records, based on a patient or member panel,[30] at one time.

Health systems and providers may want to use HINs to decrease the number of discreet interfaces they have to build to exchange EHI with other covered entities or with their own business associates for allowed uses and disclosures. For example, a provider may want to use a HIN to share EHI from their EHR to a qualified clinical data registry (QCDR), a qualified entity (QE), another HIN, or a health IT developer providing care coordination or quality measurement services. Payers, including employer-sponsored group health plans may wish to work with HINs to connect to EHI to obtain information that would better support operations, including using analytics for services such as assessing individuals' risk, population health analysis, and quality and cost analysis. These population level requests are fundamental to providing accountability for health care systems across the country.

Supporting these types of use cases necessitates the ability to exchange multiple records at one time (i.e., population level or "bulk transfer"), rather than potentially performing hundreds of data pulls or pushes for a panel of patients. Given the nature and development of the technical specifications to support this use case, it is anticipated that most population-level queries (i.e., a data request for a population of one party's patients) would occur using APIs. Further, these data use relationships and the associated service levels would be established through mutual contracts consistent with the HIPAA Privacy and Security Rules.

The standards to support this use case are not yet mature enough for widespread implementation. As updated and new standards become available, HINs should provide the ability for their participants to both pull and push population level records. This decreases the amount of time a clinician's resources are devoted to such activity and makes more time available for providing efficient and effective care.

Conclusion

The TEF Draft 2 supports the Cures Act's goal of advancing nationwide interoperability and is a key component of HHS' and the Administration's broader strategy to facilitate nationwide interoperability. HINs must agree on a minimum set of principles that enable trust in order to facilitate interoperability and the exchange of EHI necessary to support the entire care continuum. The TEF Draft 2 establishes a uniform set of principles that all HINs should adhere to allow for the trusted and secure electronic exchange of health information. Adherence to these principles will help improve the flow of EHI, providing patients with secure access to their information when and where they need it most. This will empower patients to play a more active role in managing and shopping for their care and improve the efficiency and quality of care delivered.

[30] A patient or member panel is a list of individuals assigned to a provider, health system, payer, etc.

Appendix 2:
Minimum Required Terms & Conditions (MRTCs)

DRAFT 2

April 19, 2019

TABLE OF CONTENTS

Overview

Congress charged ONC with ensuring full network-to-network exchange of EHI through a Trusted Exchange Framework and Common Agreement. This section provides a set of MRTCs to ensure that signers of the Common Agreement agree to common practices that will engender trust, support nationwide interoperability, and align to the principles and objectives contained in the TEF. The MRTCs do not make up a full end-to-end trust agreement; rather, they focus on standardizing areas of variation among currently existing trust agreements that impede nationwide interoperability.

The Recognized Coordinating Entity (RCE) will combine these MRTCs, as well as Additional Required Terms and Conditions (ARTCs), developed by the RCE and approved by ONC, into a full data sharing agreement known as the Common Agreement with which QHINs may voluntarily agree to be bound.

The following MRTCs do not contradict the HIPAA Rules and are designed to help promote, for example:

- Common authentication processes of trusted HIN participants;
- A common set of rules for trusted exchange; and
- A minimum core set of organizational and operational policies to enable the exchange of EHI among HINs.

The Common Agreement will also include an agreed upon process for filing claims that may arise with respect to the Common Agreement and adjudicating noncompliance with the Common Agreement. Such processes will be described in the ARTCs. ONC is accepting comments on the MRTCs Draft 2.

1. Definitions

2015 Edition: the 2015 Edition certification criteria adopted at 45 CFR § 170.315.

AALs: the Authentication Assurance Levels described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017).

Additional Required Terms and Conditions (ARTCs): the terms and conditions, written by the RCE and approved by ONC, which are in addition to the MRTCs.

Applicable Law: all applicable federal or state laws and regulations then in effect.

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 (for example, Social Security disability benefits) to the extent permitted by Applicable Law. Disclosure of PHI for this purpose may require an authorization that complies with 45 CFR § 164.508 if the conditions of 45 CFR 154.512(k)(6) are not met.

Breach: has the meaning assigned to such term at 45 CFR § 164.402 regarding PHI as if it applied to EHI and arises from an act or omission of a QHIN, Participant or Participant Member in the context of any of the Framework Agreements that involves the EHI that was exchanged, Used, or Disclosed pursuant to any of the Framework Agreements. The foregoing does not modify or replace any obligation that a person or entity may have under the FTC Rule with respect to a breach of security as defined in the FTC Rule.

Business Associate: has the meaning assigned to such term at 45 CFR § 160.103.

Business Associate Agreement: a contract, agreement or other arrangement that satisfies the requirements of 45 CFR § 164.504(e), as applicable.

Business Planning and Development: conducting business planning and development activities of a Covered Entity as described in subsection (5) of the definition of health care operations at 45 CFR § 164.501.

Cohort: a group of one or more Provisional QHINs specified in writing by the RCE that are attempting to be Designated by the RCE as QHINs by the same Cohort Deadline.

Cohort Deadline: the date established by the RCE for a completion of all Onboarding and other actions necessary for the Provisional QHINs in the Cohort to be Designated by the RCE as QHINs.

Common Agreement: an agreement in the form published by ONC and signed by the RCE and a Provisional QHIN (which shall become a QHIN only upon Designation by the RCE as further described in Section 2 below). The Common Agreement shall consist of (a) the Minimum Required Terms and Conditions, (b) the Additional Required Terms and Conditions, and (c) such other terms as the RCE and the QHIN mutually agree upon; provided, however, that in the event of any conflict or inconsistency between or among Applicable Law, the MRTCs, the ARTCs, and any other terms and conditions, the following shall be the order of precedence to the extent of such conflict or inconsistency: (i) Applicable Law, including the HIPAA Rules, (ii) the MRTCs, (iii) the ARTCs, and (iv) any other terms and conditions agreed to by the parties.

Connectivity Services: the technical services utilized by a QHIN to perform QHIN Broadcast Query, QHIN Targeted Query, and QHIN Message Delivery consistent with the requirements of the then applicable QHIN Technical Framework pursuant to the Common Agreement with respect to all Exchange Purposes.

Controlled Unclassified Information (CUI): has the meaning assigned to such term at 32 CFR § 2002.4(h).

Covered Entity: has the meaning assigned to such term at 45 CFR § 160.103.

Data: one or more elements of EHI (unless otherwise expressly specified).

Designation (including its correlative meanings “Designate”, “Designated”, and “Designating”): the RCE’s written confirmation to ONC that a Provisional QHIN has satisfied all the requirements of both the Common Agreement and the QHIN Technical Framework before the Provisional QHIN may become a QHIN.

Direct Relationship: a relationship between (a) an Individual and (b) a QHIN, Participant, or Participant Member, that arises when the QHIN, Participant or Participant Member, as applicable, offers services to the Individual in connection with one or more of the Framework Agreements and the Individual agrees to receive such services.

Disclosure (including its correlative meanings "Disclose", "Disclosed", and "Disclosing"): has the meaning assigned at 45 CFR § 160.103 with respect to EHI instead of PHI.

Discovery: for purposes of determining the date on which a Breach was discovered, the term Discovery shall be determined consistent with 45 CFR § 164.404(a)(2) and it shall apply to Discovery of Breaches of EHI.

Electronic Health Information (EHI): Electronic Protected Health Information, and any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in "electronic media," as defined at 45 CFR § 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Electronic Protected Health Information (ePHI): has the meaning assigned to such term at 45 CFR § 160.103.

Exchange Purposes: Use or Disclosure for Treatment, Utilization Review, Quality Assessment and Improvement, Business Planning and Development, Public Health, Individual Access Services, and Benefits Determination, each to the extent permitted under Applicable Law.

For the avoidance of doubt, EHI may be requested, exchanged, retained, aggregated, Used or Disclosed for an Exchange Purpose under Sections 2.2,1, 7.1, 8.1 below only for an Exchange Purpose of a Covered Entity or other health care provider that is acting in accordance with Applicable Law; provided, however, that this requirement shall not apply to Individual Access Services or Benefits Determination. For example: (a) EHI requested for Business Planning and Development may be disclosed and used only for activities conducted by or on behalf of a Covered Entity or other health care provider in accordance with Applicable Law.

FALs: the Federation Assurance Levels described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017).

Fees: any present or future obligation to pay money or provide any other thing of value charged by a QHIN. Fees may include, but are not limited to, one-time membership fees, ongoing membership fees, testing fees, ongoing usage fees, transaction fees, and data analytics fees.

Framework Agreement: any one of the Common Agreement, the Participant-QHIN Agreement, and the Participant Member Agreement, as applicable.

FTC Rule: the Health Breach Notification Rule promulgated by the Federal Trade Commission set forth at 16 CFR Part 318.

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.

HIPAA: the Health Insurance Portability and Accountability Act of 1996 codified at 42 U.S.C. § 300gg, 29 U.S.C. § 1181 *et seq.* and 42 U.S.C. §1320d *et seq*. and the Health Information Technology for Economic and Clinical Health Act (HITECH) codified at 42 U.S.C. § 17921 et seq.

HIPAA Rules: the regulations set forth at 45 CFR Parts 160, 162, and 164 and as amended.

Identity Assurance Level 2: IAL 2 described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017).

Individual: one or more of the following —

1) An individual as defined at 45 CFR 160.103;
2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, maintained, Disclosed or Used;
3) A person who, in accordance with Applicable Law, acts on behalf of a person described in paragraphs (1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g);
4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraphs (1) or (2) of this section; or
5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraphs (1) or (2) of this section or the individual's estate under Applicable Law.

Individual Access Services: with respect to the Exchange Purposes definition, the services provided to satisfy an Individual's right to access and to obtain a copy of the Individual's EHI and to direct that it be sent to a third party pursuant to:

1) Applicable Law;
2) Any of the Framework Agreements;
3) 45 CFR §164.524(a) as if it applied to all EHI;
4) 45 CFR §164.524(c)(2) as if it applied to all EHI; and
5) 45 CFR §164.524(c)(3)(ii) if the Individual wants the EHI sent to a third party.

Individual User: an Individual who exercises his or her right to Individual Access Services using the services of a QHIN, a Participant, or a Participant Member. An Individual User is neither a Participant nor a Participant Member.

Information Blocking: has the meaning assigned to such term in 45 CFR Part 171 and any applicable regulations promulgated thereunder that are then in effect.

Meaningful Choice: an Individual's choice with respect to the Use or Disclosure of EHI in the context of the applicable Framework Agreement that is: (i) made with advance knowledge as provided by the written privacy summary described in Sections 6.1.5, 7.6, or 8.6, as applicable; (ii) not used as a condition for receiving medical treatment or for discriminatory purposes; and (iii) revocable on a prospective basis if an Individual gives written notice to a QHIN, Participant, or Participant Member.

Minimum Information: all of the following information in plain language and in a conspicuous format that must be received by an Individual before he or she grants the approval required under Section 2.2.2, Section 7.2 or Section 8.2 below:

1) the person or entity that will be taking such action;
2) the specific purpose(s) for which such action may be taken;
3) how long such action may be taken;
4) whether EHI may be Disclosed to any third party (and, if so, to whom and for what purpose);
5) whether EHI may be Used by a third party (and, if so, identifying the third party and the Uses);
6) whether the QHIN, Participant, Participant Member, and any third party to which any of them may Disclose the EHI (including any agents or subcontractors of any of them) are required to comply with the HIPAA Rules;
7) whether EHI may be sold or licensed;
8) any material benefits or risks of such action; and
9) whether the privacy and security measures set forth in the MRTCs will apply to the EHI that is the subject of such action (including whether they will apply to any recipient of the EHI).

For purposes of this definition, information in all capital letters shall not be used to satisfy the requirement that the Minimum Information be conspicuous.

Minimum Necessary Requirements: refers to the provision in the HIPAA Rules that, under certain circumstances, requires a Covered Entity or a Business Associate to make reasonable efforts when Using or Disclosing PHI or when requesting PHI from another Covered Entity or Business Associate to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure or request. See 45 CFR §164.502(b) and §164.514(d).

Minimum Required Terms and Conditions (MRTCs): the terms and conditions included in this document.

NIST Special Publication 800-63: Special Publication 800-63 (Revision 3), Digital Identity Guidelines published by the National Institute of Standards and Technology.

NIST Special Publication 800-171: Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations published by the National Institute of Standards and Technology.

Onboarding: all implementation and other actions necessary for a QHIN, a Participant, or Participant Member to become operational in the live environment of the Framework Agreements to which it is a party. For a QHIN, the Onboarding requirements shall be set forth in the Common Agreement. For a Participant, the Onboarding requirements shall be set forth in the Participant-QHIN Agreement. For a Participant Member, the Onboarding requirements shall be set forth in the Participant Member Agreement.

ONC: Office of the National Coordinator for Health Information Technology.

ONC's Model Privacy Notice (MPN): the template maintained by ONC that assists health technology developers who collect digital health data to provide clear and transparent notice of their privacy and security practices to their users.

ONC's Interoperability Standards Advisory (ISA): a public list of the standards and implementation specifications, published by ONC, that can best be used to address specific interoperability needs. The ISA reflects the results of ongoing dialogue, debate, and consensus among industry stakeholders, and documents known limitations, preconditions, and dependencies as well as other helpful information about the listed standards and implementation specifications.

Patient Demographic Data Quality (PDDQ) Framework: the PDDQ Framework published by ONC intended to assist health care organizations in evaluating and improving their organization's patient demographic data quality by creating, implementing, and innovating processes and procedures for managing patient demographic data.

Participant: a natural person or an entity, regardless of whether the person or entity is a Covered Entity or a Business Associate, that has entered into a Participant-QHIN Agreement to participate in a QHIN. Without limitation of the foregoing, a health information exchange, health IT developer, health care system, payer, or federal agency could each be a Participant.

Participant Member: a natural person or entity, regardless of whether the person or entity is a Covered Entity or Business Associate, that has entered into a Participant Member Agreement to use the services of a Participant to send and/or receive EHI, but not an Individual exercising his or her right to Individual Access Services.

Participant Member Agreement: an agreement between a Participant and one or more Participant Members. In the event of any conflict or inconsistency between or among Applicable Law, the Participant-Member Agreement, and any other terms and conditions, the following shall be the order of precedence to the extent of such conflict or inconsistency: (i) Applicable Law including the HIPAA Rules, (ii) the Participant-QHIN Agreement, and (iii) any other terms and conditions agreed to by the parties.

Participant Member Obligations: all of the mandatory minimum obligations of Participant Members set forth in Section 8 below or elsewhere in the Participant Member Agreement.

Participant Obligations: all of the mandatory minimum obligations of Participants set forth in Section 7 below or elsewhere in the Participant-QHIN Agreement.

Participant-QHIN Agreement: an agreement between a QHIN and one or more Participants. In the event of any conflict or inconsistency between or among Applicable Law, the Participant-QHIN Agreement, and any other terms and conditions, the following shall be the order of precedence to the extent of such conflict or inconsistency: (i) Applicable Law including the HIPAA Rules, (ii) the Participant-QHIN Agreement, and (iii) any other terms and conditions agreed to by the parties.

Protected Health Information (PHI): has the meaning assigned to such term at 45 CFR § 160.103.

Provisional QHIN: a Health Information Network that has signed a Common Agreement that has also been signed by the RCE after approval as described in Section 2 below. A Provisional QHIN has not yet completed all of the requirements of the Common Agreement and the QHIN Technical Framework and has not been Designated by the RCE as a QHIN.

Public Health: with respect to the definition of Exchange Purposes, a Use or Disclosure permitted under the HIPAA Rules and any other Applicable Law for public health activities and purposes, including a Use or Disclosure permitted under 45 CFR §164.512(b) and 45 CFR §164.514(e).

QHIN Application: the written application of a HIN that wishes to become a QHIN that: (a) certifies which of the Common Agreement and QHIN Technical Framework requirements the HIN already satisfies with sufficient detail to allow the RCE to easily confirm such representations, and (b) describes the HIN's plan to satisfy all other requirements of the Common Agreement and the QHIN Technical Framework within a stated period after signing the Common Agreement.

QHIN Broadcast Query: a QHIN's electronic request for an Individual's EHI in the context of the Common Agreement that requests EHI from all other QHINs to the extent permitted by the Common Agreement and Applicable Law.

QHIN Message Delivery: the electronic action of a QHIN to deliver an Individual's EHI to one or more QHINs without an obligation to further transmit it, or to send EHI to one or more QHINs for delivery to one or more Participants or Individuals (sometimes referred to as a "push"). Notwithstanding the foregoing, QHIN Message Delivery does not include responses to any QHIN Query.

QHIN Targeted Query: a QHIN's electronic request for an Individual's EHI (sometimes referred to as a "pull") from specific QHINs in the context of the Common Agreement to the extent permitted by the Common Agreement and Applicable Law.

QHIN Technical Framework: the document approved by ONC pursuant to the Common Agreement that includes: (1) technical requirements, functional requirements, privacy and security related considerations required for the exchange of EHI between QHINs; (2) internal-QHIN functional requirements; (3) technical, privacy, and security flow down requirements from the QHIN to the Participants and/or Participant Members (if any); and, (4) operational considerations that enable the exchange of EHI between QHINs.

QHIN Query: includes both a QHIN Targeted Query and a QHIN Broadcast Query.

Qualified Health Information Network (QHIN): a Health Information Network that is a party to a Common Agreement signed by the RCE and has been Designated a QHIN by the RCE after satisfying all the conditions of the Common Agreement and the QHIN Technical Framework.

Quality Assessment and Improvement: the conduct of quality assessment and improvement activities described in subsection (1) of the definition of health care operations set forth at 45 CFR § 164.501.

Recognized Coordinating Entity (RCE): the entity selected by ONC that will enter into agreements with QHINs in order to impose, at a minimum, the requirements of the Common Agreement and the QHIN Technical Framework on the QHINs and administer such requirements on an ongoing basis.

Trusted Exchange Framework (TEF): the Trusted Exchange Framework published in the Federal Register and on ONC's website.

Treatment: has the meaning assigned to such term at 45 CFR § 164.501.

United States: means all of the United States of America and its territories and possessions and any other location in which any Federal agency or Federal governmental entity operates.

Use: has the meaning assigned at 45 CFR § 160.103 with respect to EHI instead of PHI.

US Core Data for Interoperability (USCDI): a standardized set of health data classes adopted by the Department of Health and Human Services and published by ONC to support nationwide electronic health information exchange.

Utilization Review: the conduct of utilization review activities, described in subsection (2)(v) of the definition of payment at 45 CFR § 164.501.

2. Initial Application, Onboarding, Designation and Operation of QHINs

2.1 Initial Application, Onboarding, and Designation.

2.1.1 QHIN Application. A HIN that wishes to become a QHIN shall begin the process by first delivering to the RCE a completed QHIN Application. The HIN shall promptly make its personnel available to respond to any reasonable questions that the RCE may have about the QHIN Application and promptly provide such further information and documentation that the RCE may reasonably request to process the QHIN Application. If applicable, the HIN shall also make available information relating to personnel of the HIN's vendors and persons or entities that currently use its network in order to address reasonable requests of the RCE.

2.1.2 Timing of Review by RCE. The RCE shall use commercially reasonable efforts to approve or reject each QHIN Application in writing within a stated period after receipt of a completed QHIN Application and all responses to its questions and requests for additional information and documentation, if any, that the RCE has submitted to the HIN. Despite the expiration of the stated period for review by the RCE, a QHIN Application shall not be deemed approved by the RCE unless and until the RCE issues a written notice of approval to the HIN that submitted it.

2.1.3 Requirements for Approval of a QHIN Application. No QHIN Application shall be approved by the RCE unless the HIN certifies in writing and the RCE has confirmed and documented that the HIN in question has satisfied all applicable requirements of the Common Agreement and the QHIN Technical Framework only to the extent they are prerequisites to the RCE signing the Common Agreement with the HIN. At a minimum, such prerequisites shall include the following:

(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 requirements of Section 6 below; and

(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 that (a) are required for Designation and (b) are required for ongoing operations as a QHIN. The written plan shall include, without limitation, the necessary personnel, technological infrastructure, privacy and security protections, and other appropriate resources, all as described in the ARTCs.

2.1.4 Provisional QHIN Status. Upon the RCE's written approval of a HIN's QHIN Application, the RCE shall use commercially reasonable efforts to promptly provide the HIN with a copy of the Common Agreement for signature by the HIN. The RCE also shall provide the HIN with a copy of the QHIN Technical Framework. The HIN must sign and return the Common Agreement within a stated period after receipt. Upon return to the RCE of the Common Agreement signed by the HIN, the RCE shall promptly sign it, return a fully executed copy to the HIN, and assign the HIN in writing to a Cohort, specifying the applicable Cohort Deadline. Upon the RCE's execution of the Common Agreement, the HIN shall automatically become a Provisional QHIN and continue in such status until it either fails to be Designated by the RCE as a QHIN by the applicable Cohort Deadline; or is terminated by the RCE for material breach of the Common Agreement or failure to be Designated by the RCE.

2.1.5 Obligation to Achieve QHIN Designation. Each Provisional QHIN shall use commercially reasonable efforts to take all action necessary to achieve QHIN Designation by its applicable Cohort Deadline. However, the RCE may in its reasonable discretion, assign the Provisional QHIN to another Cohort with a later Cohort Deadline but the RCE is not obligated to do so.

2.1.6 Requirements for QHIN Designation. A QHIN Designation shall not be issued by the RCE unless and until the Provisional QHIN certifies, and the RCE has confirmed and documented, that the Provisional QHIN in question has satisfied the applicable requirements of the Common Agreement and the QHIN Technical Framework, including satisfaction of any testing requirements set forth therein. A Provisional QHIN shall automatically become a QHIN upon receipt of written QHIN Designation from the RCE. The RCE shall provide written notice of such QHIN Designation simultaneously to ONC. Under no circumstances shall a Provisional QHIN or the RCE refer to the Provisional QHIN as a QHIN prior to its QHIN Designation.

2.2 QHIN Operations

2.2.1 QHIN Exchange Purposes and EHI Reciprocity. The following applies in the context of the Common Agreement to which the QHIN is a party. All actions permitted or required hereunder shall be taken only in accordance with the requirements of the Common Agreement and Applicable Law. For the avoidance of doubt, a new version of the USCDI shall be the "then applicable" USCDI eighteen (18) months after it is approved by the National Coordinator.

(i) Initiating a QHIN Query. A QHIN shall initiate a QHIN Query by using its Connectivity Services if all of the following conditions are satisfied:

(a) The QHIN Query is only for one or more of the Exchange Purposes and is initiated in one of the following ways:

1. by the QHIN on its own behalf in accordance with the Common Agreement; or

2. by the QHIN on behalf of a Participant in accordance with the Participant-QHIN Agreement; or

3. by the QHIN for Individual Access Services on behalf of an Individual User with whom it has a Direct Relationship.

(b) The QHIN Query satisfies all elements and related conditions (if any) required for Use or Disclosure of EHI consistent with Applicable Law of the relevant Exchange Purpose(s).

If a QHIN initiates a QHIN Query on its own behalf, the QHIN Query must be in accordance with any applicable Minimum Necessary Requirements as noted in Section 3.3.

(ii) <u>Responding to a QHIN Query</u>. A QHIN shall respond to a QHIN Query in the following ways:

(a) When a QHIN receives a QHIN Query from another QHIN, the QHIN shall request EHI from appropriate Participants and transmit the response(s) to the QHIN that initiated the QHIN Query.

(b) If the QHIN stores or maintains EHI, the QHIN shall also respond by providing all of the EHI in the then applicable USCDI to the extent that all of the following conditions are satisfied:

1. the EHI is appropriate for and relevant to the applicable Exchange Purpose;

2. the EHI is available;

3. the Disclosure of EHI is permitted under and meets all required conditions of Applicable Law; and

4. the Disclosure is in accordance with any applicable Minimum Necessary Requirements as noted in Section 3.3.

(iii) <u>Delivering Results of a QHIN Query</u>. A QHIN that receives the results of a QHIN Query from another QHIN shall transmit the results to the Participant or Individual User that initially requested the EHI, as applicable.

(iv) Initiating a QHIN Message Delivery. A QHIN shall initiate a QHIN Message Delivery by using its Connectivity Services only if all of the following conditions are satisfied:

(a) The QHIN Message Delivery is only for one or more of the Exchange Purposes and is initiated in one of the following ways:

1. by the QHIN on its own behalf in accordance with the Common Agreement; or

2. by the QHIN on behalf of a Participant in accordance with the Participant-QHIN Agreement; or

3. by the QHIN for Individual Access Services on behalf of an Individual User with whom it has a Direct Relationship.

(b) The QHIN Message Delivery satisfies all elements and conditions (if any) of the relevant Exchange Purpose(s).

If a QHIN initiates a QHIN Message Delivery on its own behalf, the QHIN Message Delivery must be in accordance with any applicable Minimum Necessary Requirements as noted in Section 3.3.

(v) Performing a QHIN Message Delivery. A QHIN that receives a QHIN Message Delivery and is not the final destination for the contents of the message shall send the message to the appropriate Participant(s) or Individual User(s). Upon receipt of automated message responses (e.g., confirmation of receipt) from a Participant or Individual User pursuant to QHIN Message Delivery, a QHIN shall transmit the response to the initiating QHIN only to the extent consistent with the request and permitted by Applicable Law and the Common Agreement. If a QHIN is the final destination for EHI pursuant to a QHIN Message Delivery, then the QHIN shall transmit a message response (e.g., confirmation of receipt) to the initiating QHIN only to the extent consistent with the request and permitted by Applicable Law and the Common Agreement

(vi) Delivering a Response to a QHIN Message Delivery. When a QHIN receives automated message responses (e.g., confirmation of receipt) from another QHIN pursuant to QHIN Message Delivery, it shall transmit the response to the applicable Participant or Individual User who requested the QHIN to send the EHI but only to the extent consistent with the request and permitted by Applicable Law and the Common Agreement.

2.2.2 Permitted and Future Uses of EHI. Once EHI is received by a QHIN, the recipient QHIN may exchange, retain, aggregate, Use, and Disclose such EHI only in accordance with Applicable Law and only for: (i) one or more of the Exchange Purposes in accordance with the Common Agreement (subject to the restriction below with respect to Individual Access as Services); (ii) the proper management and administration of its business and to carry out its legal responsibilities pursuant to the Common Agreement and the BAA, if applicable; (iii) investigation of a Breach or to comply with the HIPAA Rules or other applicable legal privacy and security obligations; (iv) judicial and administrative proceedings and for law enforcement purposes as well any other applicable governmental authorities (e.g. Federal Trade Commission); (v) as otherwise permitted by Applicable Law; and (vi) any purpose explicitly approved by an Individual only after the Individual has received at least a written privacy summary and the Minimum Information for such purpose. Notwithstanding the foregoing, if the Exchange Purpose is Individual Access Services, then the QHIN shall be allowed to exchange, retain, aggregate, Use, and Disclose EHI only for purposes of Individual Access Services. All exchanges, retentions, aggregations, Uses and Disclosures of EHI by QHINs shall be subject to audit procedures as described in the ARTCs.

2.2.3 Individual Exercise of Meaningful Choice. Each QHIN shall respect the Individual's exercise of Meaningful Choice by requesting that his or her EHI not be Used or Disclosed by a QHIN unless EHI is required by Applicable Law to be Used or Disclosed by the QHIN. However, any Individual's EHI that has been Used or Disclosed prior to the Individual's exercise of Meaningful Choice may continue to be Used or Disclosed for an Exchange Purpose. Each QHIN shall process each exercise of Meaningful Choice from any Individual, or from Participants or Participant Members on behalf of any Individual, and communicate the choice to all other QHINs within five (5) business days after receipt in accordance with the requirements of the QHIN Technical Framework. The QHIN shall post instructions on its public website explaining how an Individual can exercise Meaningful Choice. The QHIN shall not charge Individuals any amount for their exercise of Meaningful Choice or for communicating it to the other QHINs.

2.2.4 Processing of Individual Access Services Request.

(i) An Individual User may assert his or her right of Individual Access Services with respect to a QHIN if it has a Direct Relationship with the QHIN. The QHIN may require such Individual User to assert his or her right to Individual Access Services to EHI in writing and may require such Individual User to use the QHIN's own supplied form, provided that the use of such a form does not create a barrier to or unreasonably delay the Individual User from obtaining access to the EHI. Each QHIN shall provide Individual Users with the option of using electronic means (e.g., e-mail or secure web portal) to assert their rights for Individual Access Services to EHI.

(ii) Each QHIN that receives a request for Individual Access Services from an Individual with whom it has a Direct Relationship shall provide such Individual with Individual Access Services with respect to his or her EHI regardless of whether the QHIN is a Covered Entity or Business Associate; provided, however, that if the Individual wants the EHI to go to a third party, the Individual has satisfied the conditions at 45 CFR § 164.524(c)(3)(ii) as if it applies to EHI.

(iii) When the QHIN is acting as a Business Associate and the request for Individual Access Services is received by a Covered Entity that directs the QHIN to satisfy the request, then the QHIN may respond to a request for Individual Access Services if permitted or required by the terms of the applicable Business Associate Agreement.

(iv) A QHIN is prohibited from requiring the submission of a HIPAA authorization (see 45 CFR 164.508), or a Business Associate Agreement (see 45 CFR 164.504(e)), in order to process a request for Individual Access Services from a Participant who provides Individual Access Services that has been selected by the Individual User who is requesting EHI for Individual Access Services.

(v) With respect to a QHIN Query for Individual Access Services, the response shall be provided as required by these terms and conditions regardless of whether it was prompted by (a) the Individual User; or (b) a QHIN, Participant, or Participant Member who provides Individual Access Services and has been selected by the Individual User who is requesting EHI for Individual Access Services.

2.2.5 Mandatory Updating of Technical Capacity. If the National Coordinator approves a new version of the USCDI; and it is identified in ONC's Interoperability Standards Advisory, after a QHIN has signed the Common Agreement, the QHIN shall technically support the exchange of such new data not more than eighteen (18) months after the date that the new version of the USCDI was approved by the National Coordinator.

2.2.6 Mandatory Updating of Participant-QHIN Agreements. Each QHIN shall update its Participant-QHIN Agreements to incorporate the applicable mandatory minimum obligations stated in Section 7 herein to the extent that a change in the Common Agreement requires such update within eighteen (18) months of the date that an updated version of the Common Agreement is published by ONC.

2.2.7 Failure to Incorporate Mandatory Minimum Obligations in Participant-QHIN Agreement. A QHIN's failure to incorporate the mandatory minimum obligations described in Section 7 below into a Participant-QHIN Agreement shall be considered evidence of a material breach of the Common Agreement.

2.2.8 Completion of Onboarding Requirements. Each QHIN shall ensure that each Participant has completed the necessary Onboarding requirements before the Participant may exchange EHI with the QHIN. In addition, prior to the Cohort Deadline for a Provisional QHIN, the Provisional QHIN (a) shall have signed a Participant-QHIN Agreement with at least one Participant that has more than one Participant Member with signed Participant Member Agreements; and (b) both said Participant and at least two of such Participant Members shall be exchanging EHI in a live clinical environment. Each QHIN further shall be responsible for continuing to monitor each Participant after the necessary Onboarding requirements have been completed on a periodic basis to confirm that each Participant is meeting its mandatory minimum obligations set forth in Section 7 below and any subsequent updates thereto.

2.2.9 Compliance with the QHIN Technical Framework. Each QHIN shall meet the requirements of the then applicable QHIN Technical Framework which is incorporated herein by reference into these MRTCs and made a part hereof. Except as otherwise expressly provided herein, the QHIN shall be required to comply with any updates to the QHIN Technical Framework no later than eighteen (18) months after such updates have been approved by ONC. If there is any conflict between the terms of the QHIN Technical Framework and these MRTCs, then the MRTCs shall control.

2.2.10 Notice to Individuals. When a QHIN has a Direct Relationship with an Individual, then the QHIN shall be responsible for notifying the Individual of the mandatory provisions stated in Section 9 by posting such mandatory provisions on its public website.

2.2.11 No EHI Outside the United States. With respect to activities that are subject to these terms and conditions and the Common Agreement, no QHIN shall Use or Disclose any EHI outside the United States except as required by Applicable Law or as provided below.

(i) QHINs shall not Use or Disclose any EHI to any person or entity outside the United States (or allow any third party acting on its behalf to take such action) except to the extent that an Individual User requires his or her EHI to be Used or Disclosed outside of the United States.

(ii) QHINs may only utilize cloud-based services that are physically located within the United States. All EHI provided to a cloud services provider shall be stored physically within the United States and shall not be transferred to or located in any other countries or jurisdictions.

2.2.12 Termination of Participation in the Common Agreement. In the event that a QHIN's Common Agreement is terminated due to a material breach of its terms by the QHIN without cure, then the QHIN shall, to the extent required by the Common Agreement, return or destroy all EHI received from, created by, or received by the QHIN that the QHIN still maintains in any form and retain no copies of such EHI except as provided below. If the return or destruction of such EHI is not feasible or the QHIN needs to retain some or all of the EHI in order to demonstrate compliance with the Common Agreement, satisfy Applicable Law or defend against or assert a bona fide claim, then the QHIN shall comply with the privacy and security standards relating to EHI and described in Section 6 as long as it retains the EHI.

2.2.13 Selection of RCE and Successor RCEs and QHIN Continuing Obligations. Each QHIN agrees that ONC shall have the right to select the initial RCE or any successor RCE, and act as an interim RCE until the RCE has been selected. Each QHIN further agrees to work cooperatively with the RCE or any successor RCE selected by ONC in accordance with the Common Agreement. Additionally, each QHIN shall continue to abide by the provisions of the Common Agreement during the transition to any interim or successor RCE.

3. Data Quality and Minimum Necessary

3.1 Patient Demographic Data for Matching. Each QHIN shall send and receive all of the "patient matching data" so labelled and specified in the QHIN Technical Framework when and to the extent that all of the requirements of Section 3.3 are satisfied.

3.2 Data Quality Characteristics. To help confirm that QHINs exchange accurate patient demographic data that is used for matching, QHINs shall annually evaluate their patient demographic data management practices using the then applicable PDDQ Framework. The first such evaluation shall be conducted within eighteen (18) months after the QHIN has executed the Common Agreement.

3.3 Minimum Necessary Requirements. A QHIN shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI and when the QHIN requests EHI in the context of the Common Agreement. The Minimum Necessary Requirements shall apply to a QHIN when it requests, Uses, or Discloses EHI. Any provisions in the HIPAA Rules (e.g., 45 CFR § 164.514(d)) that include conditions shall also apply to the QHIN when Using, Disclosing or requesting EHI if such provisions are applicable.

In addition, the Minimum Necessary Requirements do not apply under certain circumstances set forth in the HIPAA Rules including the following: (i) a Disclosure of PHI to or request by a health care provider for Treatment; (ii) a Disclosure to an Individual who is the subject of the information; (iii) a Disclosure pursuant to an Individual's authorization under 45 CFR § 164.508; or (iv) Disclosures that are required by law as described in 45 CFR § 164.512(a). These exclusions apply to a QHIN with regard to EHI.

4. Transparency

4.1 Agreements and Fee Schedules.

4.1.1 Access to Participant-QHIN Agreements including Fees. Each QHIN shall make its Participant-QHIN Agreements available to ONC and the RCE upon request including information about the Fees to be charged. When making such agreements available, each QHIN may clearly label all information with respect to Fees that may contain trade secrets or commercial or financial information that is privileged or confidential.

4.1.2 Fee Schedule. Within thirty (30) calendar days after signing the Common Agreement, each QHIN shall file with the RCE a schedule of Fees used by the QHIN relating to the use of the QHIN's services provided pursuant to the Common Agreement that are charged to other QHINs and Participants. If any of the Fees change while the Common Agreement is in effect, the QHIN changing such Fees shall file an updated disclosure of the Fees with the RCE within thirty (30) days after the effective date of such change. For purposes of this filing requirement, a change in Fees shall include any change in Fees, waiver of Fees or additional Fees that the QHIN applies to all QHINs or Participants or to any one or more of the QHINs or Participants. When filing such Fee schedule with the RCE, the QHIN shall clearly label all information with respect to Fees that may contain trade secrets or commercial or financial information that is privileged or confidential.

4.2 Disclosures for Specific Purposes. Upon request, each QHIN shall disclose information to the Participants, Participant Members, and other entities described below for the following purposes to the extent permitted by or required by Applicable Law: (i) reporting of EHR-related adverse events, hazards, and other unsafe conditions to government agencies, accrediting bodies, patient safety organizations, or other public or private entities that are specifically engaged in patient quality or safety initiatives; (ii) participating in cyber threat sharing activities; and (iii) identifying security flaws in the operation of the

QHIN that would not otherwise fall into subsection (ii). Participants and Participant Members that are Covered Entities or Business Associates should consider their obligations under the HIPAA Rules before further Disclosing EHI for these purposes.

5. Cooperation and Non-Discrimination

5.1 Non-Discrimination.

5.1.1 Prohibition Against Exclusivity. A QHIN may not require exclusivity or otherwise prohibit (or attempt to prohibit) any of its Participants from joining, exchanging EHI with, conducting other transactions with, using the services of, or supporting any other QHIN.

5.1.2 No Discriminatory Limits on Exchange of EHI. A QHIN shall not unfairly or unreasonably limit exchange or interoperability with any other QHIN, Participant, Participant Member, or Individual User such as by means of burdensome testing requirements that are applied in a discriminatory manner or other means that limit the ability of a QHIN to send or receive EHI with another QHIN, Participant, Participant Member, or Individual User or slows down the rate at which such EHI is sent or received if such limitation or slower rate would have an anti-competitive effect. As used in this Section 5, a discriminatory manner means action that is taken or not taken with respect to any QHIN, Participant, Participant Member, Individual User, or group of them due to the role it plays in the health care system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that limitations, load balancing of network traffic or other activities, protocols or rules shall not be deemed discriminatory to the extent that they either: (i) benefit patients by prioritizing Treatment over other activities; or (ii) are based on a reasonable and good faith belief that the other entity or group has not satisfied or will not be able to satisfy the applicable terms hereof (including compliance with Applicable Law) in any material respect including, if applicable, Section 7 or Section 8 below. For example, imposing different testing requirements on a QHIN because it primarily serves providers that are not users of a certain electronic health record system or because it primarily serves payers would be considered discriminatory for purposes of this Section.

5.1.3 Updates to Connectivity Services. In revising and updating its Connectivity Services from time to time, a QHIN will use commercially reasonable efforts to do so in accordance with generally accepted industry practices implemented in a manner that will not cause other QHINs unreasonable cost, expense or delay in executing Queries from the revised or updated Connectivity Services; provided, however, this provision shall not apply to the extent that such revisions or updates are required by Applicable Law or in order to respond promptly to newly discovered privacy or security threats.

5.1.4 Notice of Updates to Connectivity Services. Each QHIN shall use commercially reasonable efforts to provide reasonable prior written notice of all revisions or updates of its Connectivity Services to all other QHINs if such revisions or updates could adversely affect the exchange of EHI between QHINs or require changes in the Connectivity Services of any other QHIN regardless of whether they are necessary due to Applicable Law or newly discovered privacy or security threats.

5.2 Fees.

5.2.1 Reasonable and Non-Discriminatory Fees. A QHIN must use reasonable and non-discriminatory criteria and methods in creating and applying pricing models if it charges any Fees or imposes any other costs or expenses on another QHIN. Nothing in these terms and conditions requires any QHIN to charge or pay any amounts to another QHIN.

5.2.2 No Fees for Individual Access Services. Notwithstanding anything to the contrary set forth in the Common Agreement, a QHIN may not charge another QHIN any amount for a QHIN Query or QHIN Message Delivery for the Exchange Purpose of Individual Access Services.

5.2.3 No Fees for Use or further Disclosure of EHI. A QHIN may not impose any Fee on the Use or further Disclosure of the EHI (including secondary uses) once it is accessed by another QHIN.

6. Privacy, Security, and Patient Safety

6.1 Privacy Requirements.

6.1.1 Breach Notification Requirements and Security Incidents. Each QHIN shall comply with the HIPAA Rules as if they apply to EHI, including but not limited to the Breach notification requirements applicable to Business Associates pursuant to 45 CFR Part 164 Subpart D regardless of whether it is a Business Associate; provided, however, that if the QHIN is a Covered Entity, it shall comply with the Breach reporting requirements that apply to Covered Entities in addition to providing the notices required below. Each QHIN further shall notify, in writing, the RCE and the following to the extent that they are affected by the Breach: other QHINs, Participants, Participant Members, and Individuals with whom the QHIN has a Direct Relationship. Such notice shall be provided without unreasonable delay in accordance with this Section and Applicable Law. Whenever possible, early notification of Discovery of the Breach is advisable in order to allow other affected parties to satisfy their reporting obligations. Each QHIN shall implement commercially reasonable policies and procedures to address security incidents as defined at 45 CFR §164.304 and shall identify, if possible, and respond to suspected or known security incidents, and shall mitigate, to the extent reasonably practicable, any harmful effects of any security incidents that are suspected by or known to the QHIN. Each QHIN shall document any suspected or known security incidents and its outcomes and maintain a copy of such documentation. The foregoing does not modify or replace any obligation that a QHIN may have under the FTC Rule with respect to a breach of security as defined in the FTC Rule if applicable.

6.1.2 Law Enforcement Exception to Breach Notification. Notwithstanding Section 6.1.1 above, if a QHIN is notified, in writing or by oral statement by any law enforcement official or by any other governmental agency (e.g. Federal Trade Commission), that a Breach notification would impede a criminal investigation or cause damage to national security, and the statement has been documented consistent with 45 CFR 164.412(b), then the QHIN shall delay the Breach notification for the time period specified by the law enforcement official.

6.1.3 Demand for Compulsory Disclosures. If the QHIN is requested or required (by oral questions, interrogatories, requests for information or documents, subpoena, civil investigation, demand, or similar process) to Disclose any EHI, then the QHIN shall provide (unless prohibited by Applicable Law) prompt written notice of the request to the Participant, Participant Member, or Individual with whom the QHIN has a Direct Relationship that contributed the EHI so that the Participant, Participant Member or Individual may seek an appropriate protective order. In the event that such protective order or other appropriate remedy to prevent such Disclosure is not obtained, the QHIN may disclose only that portion of the EHI (and only to those persons or entities) which is legally required, and the QHIN agrees to reasonably cooperate with the party making the request to the extent permitted by Applicable Law in securing assurances that the disclosed EHI will be accorded confidential treatment. QHINs should consider their obligations under the HIPAA Rules before Disclosing EHI for these purposes.

6.1.4 Other Legal Requirements. If and to the extent that Applicable Law requires that an Individual either consent to or approve the Use or Disclosure of his or her EHI to the QHIN, then each QHIN that has a Direct Relationship with the Individual shall not Use or Disclose such EHI in connection with the Common Agreement unless the QHIN has obtained the Individual's consent, approval or other documentation with respect to such Uses or Disclosures consistent with the requirements of Applicable Law. The QHIN shall maintain copies of such consent, approval or other documentation and may make it available electronically to any other QHIN upon request to the extent permitted by Applicable Law. The QHIN shall maintain written policies and procedures to allow an Individual to revoke such consent or approval on a prospective basis. Each QHIN shall specify responsibilities comparable to those described above in its Participant-QHIN Agreements and each Participant shall specify responsibilities comparable to those described above in its Participant Member Agreements.

6.1.5 Written Privacy Summary. Each QHIN agrees to publish and make publicly available a written notice in plain language that describes each QHIN's privacy practices regarding the access, exchange, Use and Disclosure of EHI with substantially the same content as described in ONC's Model Privacy Notice. The written privacy summary shall include the following additional information: (i) a description, including at least one (1) example, of each type of Exchange Purpose; (ii) a description that provides an Individual with a reasonable understanding of how to exercise Meaningful Choice; and (iii) who Individuals can contact for further information about the QHIN's privacy policies. This written privacy summary requirement does not supplant the HIPAA Privacy Rule obligations of a QHIN that is a Covered Entity to post and distribute a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520.

6.1.6 Summary of Disclosures of EHI. Each QHIN shall satisfy its obligations as described under Section 9.5.

6.2 Minimum EHI Security Requirements. To promote the confidentiality, integrity, and availability of EHI and minimize the potential for Breaches of EHI, each QHIN shall be required to comply with the HIPAA Rules as if they applied to EHI including but not limited to: (i) maintaining reasonable and appropriate administrative, technical, and physical safeguards for protecting EHI; (ii) protect against reasonably anticipated impermissible Uses and Disclosures of EHI; (iii) identifying and protecting against reasonably anticipated threats to the security or integrity of EHI; and (iv) monitoring compliance with such safeguards by its workforce. In determining which administrative, technical and physical safeguards to implement, the QHIN shall consider the following: (i) its size, complexity, and capabilities; (ii) its technical, hardware, and software infrastructure; (iii) the costs of security measures; and (iv) the likelihood and possible impact of potential risks to EHI. Each QHIN further shall review and modify such safeguards to continue protecting EHI in a changing environment of security threats within a reasonable period of time. Additionally, each QHIN shall be required to implement the following minimum security requirements described below.

6.2.1 Application of NIST Standards and ONC/OCR Security Risk Assessment Tool.

(i) HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework and ONC/OCR Security Risk Assessment Tool. Each QHIN shall evaluate its security program on at least an annual basis. As part of its ongoing security risk analysis and risk management program, such evaluation shall include a review of the then most recently published version of the HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework and the then most recently published version of the ONC/OCR HIPAA Security Risk Assessment Tool to help the QHIN ensure its compliance with the HIPAA Rules. To the extent that such evaluation identifies any risks, vulnerabilities or gaps in the QHIN's compliance with the HIPAA Rules or other Applicable Law, then the QHIN shall assess and implement security measures consistent with current industry standards and best practices to ensure the confidentiality, integrity and availability of the EHI that it creates, receives, maintains or transmits, and provide documentation of such evaluation, and shall document these assessments and a description of the implementation of any security measures.

(ii) Protecting the Confidentiality of Controlled Unclassified Information (CUI) in Non Federal Systems and Organizations. Each QHIN shall evaluate its security program for the protection of CUI on at least an annual basis, provide documentation of such evaluation, and develop and implement an action plan to comply with the security requirements of the then most recently published version of the NIST Special Publication 800-171.

6.2.2 Data Integrity. Each QHIN's security policy shall include the following elements to promote data integrity of all EHI that it receives, maintains or transmits:

(i) Procedures to safeguard that EHI is not improperly altered or destroyed;

(ii) Procedures to protect against reasonably anticipated, impermissible Uses or Disclosures of EHI;

(iii) Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption, if the QHIN is serving as a certificate authority;

(iv) Procedures to test and restore backup copies of systems, databases, and private keys, if the QHIN is serving as a certificate authority, so that the QHIN can retrieve data from backup copies in the event of a disaster, emergency, or other circumstance requiring the restoration of EHI to preserve data integrity; and

(v) Procedures to document the methodologies and results of tests to restore backup copies of systems, databases, and private keys, if the QHIN is serving as a certificate authority. Such documentation shall be maintained in a manner consistent with 45 CFR § 164.316(b).

Each QHIN shall report known instances of inaccurate or incomplete EHI to the Participant who is the originator of the EHI, and request that the Participant remediate such data integrity issues in a timely manner to the extent reasonably possible.

6.2.3 Authorization. Each QHIN's security policy shall include written authorization procedures to confirm that any entities requesting access to system functions or EHI possess the appropriate credentials (e.g., privileges granted and provisioned in security and privacy management).

6.2.4 Identity Proofing. Each QHIN's security policy shall include the following identity proofing requirements:

(i) QHINs. Prior to the issuance of access credentials, each QHIN shall identity proof any staff or users at the QHIN who may initiate a QHIN Query or QHIN Message Delivery at a minimum of IAL2.

(ii) Participants/Participant Members. Prior to the issuance of access credentials, each QHIN shall require that Participants be identity proofed at a minimum of IAL2. Each QHIN also shall require each of its Participants to identity proof its Participant Members at a minimum of IAL2 prior to the issuance of access credentials.

(iii) Individual Users. Each QHIN shall require that Individual Users with whom it has a Direct Relationship be identity proofed at a minimum of IAL2 prior to issuance of access credentials by the QHIN. The identity information may be supplemented by the Participant or Participant Member acting as authoritative sources by using knowledge of the identity of the Individuals in accordance with written policies and procedures. Such policies and procedures must be commensurate with the risk of incorrect identity proofing (e.g., procedures for applicants receiving credentials to access their medical information may be less rigorous than procedures used for applicants receiving credentials that can be used to access medical information on multiple patients). For example, IAL2 identity proofing for an applicant receiving credentials to access to his or her own medical information can be accomplished by any two of the following:

(a) physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges;

(b) 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

(c) comparison to information from an electronic health record (EHR) containing information entered from prior encounters.

All personally identifiable information collected shall be limited to the minimum necessary to resolve a unique identity and the QHIN shall not copy or retain such personally identifiable information.

6.2.5 User Authentication. Each QHIN shall adhere to the user authentication functional requirements as described in the QHIN Technical Framework where applicable. Additionally, each QHIN shall require that any staff or users at the QHIN, Participants, or Individual Users who request EHI or request to send EHI shall be authenticated at a minimum of AAL2 and, if not an Individual User, also provide support for at least FAL2. Each QHIN shall also require each of its Participants to authenticate any Participant Members or Individuals Users that request EHI or request to send EHI at a minimum of AAL2 and, if not an Individual User, also provide support for at least FAL2.

6.2.6 Transport Security. Each QHIN's security policy shall include written policies and procedures consistent with the technical requirements specified in the QHIN Technical Framework to ensure a secure channel for communications between QHINs and between QHINs and Participants.

6.2.7 Certificate Policies. Each QHIN's security policy shall require that all Participant cryptographic certificates meet or exceed the applicable criteria in the QHIN Technical Framework.

6.2.8 Auditable Events. Each QHIN shall abide by the auditable events requirements described in the QHIN Technical Framework. Additionally, each QHIN's security policy shall include the following auditing requirements for each Exchange Purpose that it performs:

(i) Auditable events as required by the QHIN Technical Framework;

(ii) An audit log including records for all auditable events required by the QHIN Technical Framework. A QHIN shall retain all audit logs (both electronic and non-electronic) in accordance with Applicable Law and make such audit logs available during any audit; and

(iii) A record of an auditable event which at a minimum should include the following information:

- The description of the event;
- The date and time the event occurred;
- A success or failure indicator; and (where appropriate)
- The identity of the entity and/or operator that was responsible for the event.

6.2.9 Certificate Authority Backup and Recovery. Each QHIN who is an issuer of certificates shall maintain backup copies of system, databases, and private keys in order to rebuild the certificate authorities' capability in the event of software and/or data corruption.

7. Participant Minimum Obligations

Each QHIN shall be responsible for incorporating the mandatory minimum obligations described in this Section 7 into all Participant-QHIN Agreements.

7.1 Exchange Purposes and EHI Reciprocity. The following applies in the context of the Participant-QHIN Agreement to which the Participant is a party. All action permitted or required hereunder shall be taken only in accordance with the requirements of the Participant-QHIN Agreement to which the Participant is a party and Applicable Law. For the avoidance of doubt, a new version of the USCDI shall be the "then applicable" USCDI eighteen (18) months after it is approved by the National Coordinator.

(i) Requests for EHI. A Participant may request EHI from a QHIN only if all of the following conditions are satisfied:

(a) The request for EHI is only for one or more of the Exchange Purposes and is initiated in one of the following ways:

1. By the Participant on its own behalf in accordance with the Participant-QHIN Agreement; or

2. By the Participant on behalf of a Participant Member in accordance with the Participant Member Agreement; or

3. By the Participant for Individual Access Services on behalf of an Individual User with whom it has a Direct Relationship.

(b) The request for EHI satisfies all elements and related conditions (if any) required for Use or Disclosure consistent with Applicable Law of the relevant Exchange Purpose(s).

If a Participant initiates a request for EHI on its own behalf, the request must be in accordance with any applicable Minimum Necessary Requirements as noted in Section 7.19.

(ii) Response to QHIN Queries. A Participant shall respond to a request for EHI from a QHIN, pursuant to a QHIN Query, in the following ways:

(a) When a Participant receives a request for EHI from a QHIN, pursuant to a QHIN Query, the Participant shall request EHI from appropriate Participant Members and transmit the response(s) it receives from such Participant Members to the QHIN that requested EHI.

(b) If the Participant stores or maintains EHI, the Participant shall also respond by providing all of the EHI it receives in the then applicable USCDI to the extent that all of the following conditions are satisfied:

1. The EHI is appropriate for and relevant to the applicable Exchange Purpose;

2. The EHI is available;

3. The Disclosure of EHI is permitted under and meets all required conditions of Applicable Law; and

4. The Disclosure is in accordance with any applicable Minimum Necessary Requirements as noted in Section 7.19 below.

Notwithstanding the foregoing, a Participant who only provides Individual Access Services shall not be required to respond to requests for EHI except as necessary to respond to an Individual User's request for Individual Access Services, including where such requests utilize a third party.

(iii) Requests to Send EHI. A Participant may request a QHIN to send EHI only if all of the following conditions are satisfied:

(a) The request is initiated by the Participant on its own behalf in accordance with the Participant-QHIN Agreement, or the request is initiated by the Participant on behalf of a Participant Member in accordance with the Participant Member Agreement, or the request is initiated by the Participant for Individual Access Services on behalf of an Individual User with whom it has a Direct Relationship; and

(b) The request is for one or more of the Exchange Purpose(s), and all elements and conditions (if any) required for Use or Disclosure consistent with Applicable Law of the relevant Exchange Purpose(s) are satisfied.

If the request to send EHI is initiated by the Participant on its own behalf, the request must be in accordance with any applicable Minimum Necessary Requirements as noted in Section 7.19.

(iv) Response to QHIN Message Delivery. When a Participant receives a request to send EHI from a QHIN pursuant to QHIN Message Delivery, and the Participant is not the final destination for the EHI, the Participant shall send the EHI to the appropriate Participant Member(s) or Individual User(s). When a Participant receives automated message responses (e.g., confirmation of receipt) from a Participant Member or Individual User pursuant to QHIN Message Delivery, a Participant shall transmit the response to the QHIN that requested the Participant to send EHI only to the extent consistent with the request and permitted by Applicable Law and the Participant-QHIN Agreement. If a Participant is the final destination for EHI, then the Participant shall transmit a message response (e.g., confirmation of receipt) to the QHIN that sent EHI only to the extent consistent with the request and permitted by Applicable Law and the Participant-QHIN Agreement.

7.2 Permitted and Future Uses of EHI. Once EHI is received by a Participant, the recipient Participant may exchange, retain, aggregate, Use, and Disclose such EHI only in accordance with Applicable Law and only for: (i) one or more of the Exchange Purposes in accordance with the Framework Agreement to which the Participant is a party (subject to the restriction below with respect to Individual Access Services); (ii) the proper management and administration of its business and to carry out its legal responsibilities pursuant to the Framework Agreement to which it is a party and the BAA, if applicable; (iii) investigation of a Breach or to comply with the HIPAA Rules or other applicable legal privacy and security obligations; (iv) judicial and administrative proceedings and for law enforcement purposes as well as any other applicable governmental authorities (e.g. Federal Trade Commission); (v) if the Participant is a Covered Entity or a Business Associate, as otherwise permitted by Applicable Law; and (vi) any purpose explicitly approved by an Individual only after the Individual has received at least a written privacy summary and the Minimum Information for such purpose. Notwithstanding the foregoing, if the Exchange Purpose is Individual Access Services, then the Participant shall be allowed to exchange, retain, aggregate, Use, and Disclose EHI only for purposes of Individual Access Services. All exchanges, retentions, aggregations, Uses and Disclosures of EHI by Participants shall be subject to audit procedures as described in the ARTCs.

7.3 Individual Exercise of Meaningful Choice. Each Participant shall respect the Individual's exercise of Meaningful Choice by requesting that his or her EHI not be Used or Disclosed by a Participant unless Applicable Law requires the Participant to Use or Disclose the EHI. However, any Individual's EHI that has been Used or Disclosed prior to the Individual's exercise of Meaningful Choice may continue to be Used or Disclosed for an Exchange Purpose. Each Participant shall process each exercise of Meaningful Choice from any Individual, or from Participant Members on behalf of any Individual, and communicate the choice to the QHIN with which it has a signed Participant-QHIN Agreement within five (5) business days after receipt. The Participant shall post instructions on its public website explaining how an Individual can exercise Meaningful Choice. The Participant shall not charge Individuals any amount for their exercise of Meaningful Choice or for communicating it to the applicable QHIN.

7.4 Other Legal Requirements. If and to the extent that Applicable Law requires that an Individual either consent to or approve the Use or Disclosure of his or her EHI to the Participant, then each Participant that has a Direct Relationship with the Individual shall not Use or Disclose such EHI in connection with the Participant-QHIN Agreement unless the Participant has obtained the Individual's consent, approval or other documentation with respect to such Uses or Disclosures consistent with the requirements of Applicable Law. The Participant shall maintain copies of such consent, approval or other documentation and may make it available electronically to any other Participant, QHIN, or Participant Member upon request to the extent permitted by Applicable Law. The Participant shall maintain written policies and procedures to allow an Individual to revoke such consent or approval on a prospective basis. In its Participant Member Agreements, each Participant shall require Participant Members to satisfy responsibilities comparable to those set forth above.

7.5 Non-Discrimination.

(i) A Participant may not require exclusivity or otherwise prohibit (or attempt to prohibit) any of its Participant Members from joining, exchanging EHI with, conducting other transactions with, or using the services of or supporting any other Participant pursuant to the Participant Member Agreement.

(ii) A Participant shall not unfairly or unreasonably limit exchange or interoperability with any QHIN, other Participant, Participant Member, or Individual User such as by means of burdensome testing requirements that are applied in a discriminatory manner, other means that limit the ability of a Participant to send or receive EHI with another Participant, Participant Member, or Individual User or slows down the rate at which such EHI is sent or received if such limitation or slower rate would have an anti-competitive effect. As used in this Section 7.5(ii), a discriminatory manner means action that is taken or not taken with respect to any QHIN, other Participant, Participant Member, Individual User or group of them due to the role it plays in the health care system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that limitations, load balancing of network traffic or other activities, protocols or rules shall not be deemed discriminatory to the extent that they either: (a) benefit patients by prioritizing Treatment over other activities; or (b) are based on a reasonable and good faith belief that the other entity or group has not satisfied or will not be able to satisfy the mandatory minimum obligations stated in Section 7 (including compliance with Applicable Law) in any material respect. For example, imposing different testing requirements on a Participant Member because the Participant Member primarily serves providers that are not users of a certain electronic health record system or because it primarily serves payers would be considered discriminatory for purposes of this Section 7.5(ii).

7.6 Written Privacy Summary. Each Participant agrees to publish and make publicly available a written notice in plain language that describes each Participant's privacy practices regarding the access, exchange, Use and Disclosure of EHI with substantially the same content as described in ONC's Model Privacy Notice. The written privacy summary shall include the following additional information: (i) a description, including at least one (1) example, of each type of Exchange Purpose; (ii) a description that provides an Individual with a reasonable understanding of how to exercise Meaningful Choice; and (iii) whom Individuals can contact for further information about the Participant's privacy policies. This written privacy summary requirement does not supplant the HIPAA Privacy Rule obligations of a Participant that is a Covered Entity to post and distribute a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520.

7.7 Minimum Security Requirements. To promote the confidentiality, integrity, and availability of EHI and minimize the potential for Breaches of EHI, each Participant shall be required to: (i) maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting EHI; (ii) protect against reasonably anticipated impermissible Uses and Disclosures of EHI; (iii) identify and protect against reasonably anticipated threats to the security or integrity of EHI; and (iv) monitor compliance with such safeguards by its workforce. In determining which administrative, technical and physical safeguards to implement, the Participant shall consider the following: (i) its size, complexity, and capabilities; (ii) its technical, hardware, and software infrastructure; (iii) the costs of security measures; and (iv) the likelihood and possible impact of potential risks to EHI. Each Participant further shall review and modify such safeguards to continue protecting EHI in a changing environment of security threats within a reasonable period of time. Additionally, each Participant shall be required to implement the following minimum security requirements described below.

7.8 Authorization. Each Participant's security policy shall include written authorization procedures to confirm that any entities requesting access to system functions or EHI possess the appropriate credentials (e.g., granted and provisioned in security and privacy management).

7.9 Identity Proofing. Each Participant's security policy shall include the following identity proofing requirements:

(i) Participant Members. Each Participant shall require that Participant Members be identity proofed at IAL2 prior to issuance of access credentials; and

(ii) Individual Users. Each Participant shall require that Individual Users with whom it has a Direct Relationship be identity proofed at a minimum of IAL2 prior to issuance of access credentials by the Participant. The identity information may be supplemented by Participant Members acting as authoritative source by using knowledge of the identity of the individuals in accordance with written policies and procedures. Such policies and procedures must be commensurate with the risk of incorrect identity proofing (e.g., procedures for applicants receiving credentials to access their medical information may be less rigorous than procedures used for applicants receiving credentials that can be used to access medical information on multiple patients). For example, IAL2 identity proofing for an applicant receiving credentials to access to his or her own medical information can be accomplished by any two of the following:

(a) physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges;

(b) 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

(c) comparison to information from an electronic health record (EHR) containing information entered from prior encounters.

All personally identifiable information collected shall be limited to the minimum necessary to resolve a unique identity and the Participant shall not copy or retain such personally identifiable information.

7.10 User Authentication. Each Participant shall require that any Participant Member or Individual User that requests EHI or requests to send EHI be authenticated at a minimum of AAL2, and any Participant Member shall also provide support for at least FAL2. Each Participant shall also require each of its Participant Members to authenticate any Individual Users that request EHI or request to send EHI at a minimum of AAL2.

7.11 Auditable Events. Each Participant shall utilize the security policy established by the QHIN with whom the Participant has a signed a Participant-QHIN Agreement to identify a set of auditable events. Said security policy shall be consistent with the QHIN's security policy but with appropriate modifications based on the transactions being performed. Each Participant's security policy shall include the following auditing requirements for each Exchange Purpose that it performs:

(i) A list of auditable events described in said security policy;

(ii) An audit log including records for all auditable events identified by said security policy. A Participant shall retain all audit logs (both electronic and non-electronic) in accordance with Applicable Law and make such audit logs available during any audit; and

(iii) A record of an auditable event which at a minimum should include the following information:

- The description of the event;
- The date and time the event occurred;
- A success or failure indicator; and
- Where appropriate, the identity of the entity and/or operator that was responsible for the event.

7.12 Breach Notification Requirements and Security Incident. Each Participant shall comply with the Breach notification requirements applicable to Business Associates pursuant to 45 CFR Part 164 Subpart D regardless of whether it is a Business Associate; provided, however, that if the Participant is a Covered Entity, it shall comply with the Breach reporting requirements that apply to Covered Entities in addition to providing the notices required below. Each Participant further shall notify, in writing, the QHIN and the following to the extent that they are affected by the Breach: other Participants, Participant Members, and Individuals with whom the Participant has a Direct Relationship. Such notice shall be provided without unreasonable delay in accordance with this Section and Applicable Law. Whenever possible, early notification of Discovery of the Breach is advisable in order to allow other affected parties to satisfy their reporting obligations. Each Participant shall implement commercially reasonable policies and procedures to address security incidents as defined at 45 CFR §164.304. Each Participant further shall identify, if possible, and respond to suspected or known security incidents, and shall mitigate, to the extent reasonably practicable, any harmful effects of any security incidents that are suspected by or known to the Participant and shall document any suspected or known security incidents and its outcomes and maintain a copy of such documentation. The foregoing does not modify or replace any obligation that a Participant may have under the FTC Rule with respect to a breach of security as defined in the FTC Rule if applicable.

7.13 Law Enforcement Exception to Breach Notification. Notwithstanding Section 7.12 above, if a Participant is notified in writing or by oral statement by any law enforcement official or other applicable governmental agency (e.g. Federal Trade Commission), that a Breach notification would impede a criminal investigation or cause damage to national security, and the statement has been documented consistent with 45 CFR 164.412(b), then the Participant shall delay the Breach notification for the time period specified by the law enforcement official.

7.14 Processing of Individual Access Services Request.

(i) An Individual User may assert his or her right of Individual Access Services with respect to a Participant if it has a Direct Relationship with the Participant. The Participant may require such Individual User to assert his or her right to Individual Access Services to EHI in writing and may require such Individual User to use the Participant's own supplied form, provided that the use of such a form does not create a barrier to or unreasonably delay the Individual User from obtaining access to the EHI. Each Participant shall provide Individual Users with the option of using electronic means (e.g., e-mail or secure web portal) to assert their rights for Individual Access Services to EHI.

(ii) Each Participant that receives a request for Individual Access Services from an Individual with whom it has a Direct Relationship shall provide such Individual with Individual Access Services with respect to his or her EHI regardless of whether the Participant is a Covered Entity or Business Associate; provided, however, that if the Individual wants the EHI to go to a third party, the Individual has satisfied the conditions at 45 CFR § 164.524(c)(3)(ii) as if it applies to EHI.

(iii) When the Participant is acting as a Business Associate and the request for Individual Access Services is received by a Covered Entity that directs the Participant to satisfy the request, then the Participant may respond to a request for Individual Access Services if permitted or required by the terms of the applicable Business Associate Agreement.

(iv) A Participant is prohibited from requiring the submission of a HIPAA authorization (see 45 CFR § 164.508), or a Business Associate Agreement (see 45 CFR § 164.504(e)), in order to process a request for Individual Access Services from a Participant Member who provides the Individual Access Services and has been selected by the Individual User who is requesting EHI for Individual Access Services.

(v) With respect to a QHIN Query for Individual Access Services, the response shall be provided as required by these terms and conditions regardless of whether it was prompted by (a) the Individual User; or (b) a QHIN, Participant, or Participant Member who provides Individual Access Services and has been selected by the Individual User who is requesting EHI for Individual Access Services.

7.15 Notice to Individuals. If a Participant has a Direct Relationship with an Individual, then the Participant shall be responsible for notifying the Individual of the mandatory provisions stated in Section 9 by posting such mandatory provisions on its public website.

7.16 Data Integrity. Each Participant's security policy shall include the following elements to promote data integrity of all EHI that it receives, maintains, or transmits with respect to the Exchange Purposes that it performs:

(i) Procedures to safeguard that EHI is not improperly altered or destroyed;

(ii) Procedures to protect against reasonably anticipated, impermissible Uses or Disclosures of EHI;

(iii) Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption, if the Participant is serving as a certificate authority;

(iv) Procedures to test and restore backup copies of systems, databases, and private keys, if the Participant is serving as a certificate authority, so that the Participant can retrieve data from backup copies in the event of a disaster, emergency, or other circumstance requiring the restoration of EHI to preserve data integrity; and

(v) Procedures to document the methodologies and results of tests to restore backup copies of systems, databases, and private keys, if the Participant is serving as a certificate authority. Such documentation shall be maintained in a manner consistent with 45 CFR § 164.316(b).

Each Participant shall report known instances of inaccurate or incomplete EHI to the Participant Member who is the originator of the EHI, and request that the Participant Member remediate such data integrity issues in a timely manner to the extent reasonably possible.

7.17 Transport Security. Each Participant's security policy shall include written policies and procedures to ensure a secure channel for communications between Participants and QHINs and between Participants and Participant Members.

7.18 Compliance with Applicable Law. Each Participant shall comply with all Applicable Law.

7.19 Minimum Necessary Requirements. Each Participant shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI for applicable Exchange Purposes or when the Participant requests EHI in the context of the applicable Framework Agreement. The Minimum Necessary Requirements shall apply to a Participant regardless of whether it is a Covered Entity or a Business Associate when it requests, Uses, or Discloses EHI. Any provisions set forth in the HIPAA Rules (e.g., 45 CFR §164.514(d)) that include conditions shall also apply to the Participant when Using, Disclosing or requesting EHI if such provisions are applicable.

In addition, the Minimum Necessary Requirements do not apply under certain circumstances set forth in the HIPAA Rules including the following: (i) a Disclosure of PHI to or request by a health care provider for Treatment; (ii) a Disclosure to an Individual who is the subject of the information; (iii) a Disclosure pursuant to an Individual's authorization under 45 CFR § 164.508; or (iv) Disclosures that are required by law as described in 45 CFR § 164.512(a). These exclusions apply to a Participant with regard to EHI.

7.20 Summary of Disclosures of EHI. Each Participant shall satisfy its obligations as described under Section 9.5.

7.21 Federal Agencies Serving as a Participant. Notwithstanding anything to the contrary in these MRTCs, a federal agency that is serving as a Participant and is not otherwise subject to the HIPAA Rules is not required to comply with the HIPAA Privacy and Security Rules referenced in these MRTCs. The federal agency will comply with all privacy and security requirements imposed by applicable federal law.

7.22 Mandatory Updating of Participant Member Agreements. Each Participant shall update its Participant Member Agreements to incorporate the mandatory applicable minimum obligations set forth in Section 8 herein (to the extent that a change in the Common Agreement requires such update) within eighteen (18) months of the date that an updated version of the Common Agreement is published by ONC.

7.23 Completion of Onboarding Requirements. Each Participant shall ensure that each Participant Member has completed the necessary Onboarding requirements before the Participant Member may exchange EHI with the Participant. Each Participant further shall be responsible for continuing to monitor each Participant Member after the necessary Onboarding requirements have been completed on a periodic basis to confirm that each Participant Member is meeting its minimum obligations set forth in Section 8 below and any subsequent updates thereto.

7.24 Compliance with Minimum Obligations. Each Participant shall be responsible for taking reasonable steps to confirm that all Participant Members are abiding by the mandatory minimum obligations stated in Section 8. Each Participant further shall require that each Participant Member provides written confirmation of compliance with these obligations on at least an annual basis. In the event that a Participant becomes aware of a Participant Member's material non-compliance with any of the obligations stated in Section 8, then the Participant shall promptly notify the Participant Member in writing. Such notice shall inform the Participant Member that its failure to correct any such deficiencies shall constitute a material breach of the Participant Member Agreement, which may result in early termination of the Participant Member's Agreement with the Participant.

8. Participant Member Minimum Obligations

Each Participant shall be responsible for incorporating mandatory minimum obligations described in this Section 8 into all Participant Member Agreements.

8.1 Exchange Purposes and EHI Reciprocity. The following applies in the context of the Participant Member Agreement to which the Participant Member is a party. All action permitted or required hereunder shall be taken only in accordance with the requirements of the Participant Member Agreement to which the Participant Member is a party and Applicable Law. For the avoidance of doubt, a new version of the USCDI shall be the "then applicable" USCDI eighteen (18) months after it is approved by the National Coordinator.

(i) Requests for EHI. A Participant Member may request EHI from a Participant only if all of the following conditions are satisfied:

(a) The request for EHI is only for one or more of the Exchange Purposes and is initiated in one of the following ways:

1. By the Participant Member on its own behalf in accordance with the Participant Member Agreement; or

2. By the Participant Member for Individual Access Services on behalf of an Individual User with whom it has a Direct Relationship.

3. The request for EHI satisfies all elements and related conditions (if any) required for Use or Disclosure consistent with Applicable Law of the relevant Exchange Purpose(s).

(b) If a Participant Member initiates a request for EHI on its own behalf, the request must be in accordance with the applicable Minimum Necessary Requirements as noted in Section 8.19.

(ii) Response to Requests for EHI. When a Participant Member receives a request for EHI from a Participant, the Participant Member shall respond by providing all of the EHI in the then applicable USCDI to the extent that all of the following conditions are satisfied:

(a) the EHI is appropriate for and relevant to the applicable Exchange Purpose;

(b) the EHI is available;

(c) the Disclosure of EHI is permitted under and meets all required conditions of Applicable Law; and

(d) the Disclosure is in accordance with the applicable Minimum Necessary Requirements as noted in Section 8.19 below.

Notwithstanding the foregoing, a Participant Member who only provides Individual Access Services shall not be required to respond to requests for EHI except as necessary to respond to an Individual User's request for Individual Access Services, including where such requests utilize a third party.

(iii) Requests to Send EHI. A Participant Member may request a Participant to send EHI only if all of the following conditions are satisfied:

(a) The request to send EHI is only for one or more of the Exchange Purposes and is initiated in one of the following ways:

1. by the Participant Member on its own behalf in accordance with the Participant Member Agreement; or

2. by the Participant Member for Individual Access Services on behalf of an Individual User with whom it has a Direct Relationship.

(b) The request to send EHI satisfies all elements and conditions (if any) required for Use or Disclosure consistent with Applicable Law of the relevant Exchange Purpose(s).

If a Participant Member initiates a request to send EHI on its own behalf, the request must be in accordance with any applicable Minimum Necessary Requirements as noted in Section 8.19.

(iv) Responses to Requests to Send EHI. When a Participant Member receives a request to send EHI from a Participant, and the Participant Member is not the final destination for the EHI, the Participant Member shall send the EHI to the appropriate Individual User(s). When a Participant Member receives automated message responses (e.g., confirmation of receipt) from an Individual User, a Participant Member shall transmit the response to the Participant that requested the Participant Member to send EHI only to the extent consistent with the request and permitted by Applicable Law and the Participant Member Agreement. If a

Participant Member is the final destination for EHI, then the Participant Member shall transmit a message response (e.g., confirmation of receipt) to the Participant that sent EHI only to the extent consistent with the request and permitted by Applicable Law and the Participant Member Agreement.

8.2 Permitted and Future Uses of EHI. Once EHI is received by a Participant Member, the recipient Participant Member may exchange, retain, aggregate, Use, and Disclose such EHI only in accordance with Applicable Law and only for: (i) one or more of the Exchange Purposes in accordance with the Framework Agreement to which the Participant Member is a party (subject to the restriction below with respect to Individual Access Services); (ii) the proper management and administration of its business and to carry out its legal responsibilities pursuant to the Framework Agreement to which it is a party and the BAA, if applicable; (iii) investigation of a Breach or to comply with the HIPAA Rules or other applicable legal privacy and security obligations; (iv) judicial and administrative proceedings and for law enforcement purposes as well as any other applicable governmental authorities (e.g., Federal Trade Commission); (v) if the Participant Member is a Covered Entity or a Business Associate, as otherwise permitted by Applicable Law; and (vi) any purpose explicitly approved by an Individual only after the Individual has received at least a written privacy summary and the Minimum Information for such purpose. Notwithstanding the foregoing, if the Exchange Purpose is Individual Access Services, then the Participant Member shall be allowed to exchange, retain, aggregate, Use, and Disclose EHI only for purposes of Individual Access Services. All exchanges, retentions, aggregations, Uses and Disclosures of EHI by Participant Members shall be subject to audit procedures as described in the ARTCs.

8.3 Individual Exercise of Meaningful Choice. Each Participant Member shall respect the Individual’s exercise of Meaningful Choice by requesting that his or her EHI not be Used or Disclosed by a Participant Member unless EHI is required by Applicable Law to be Used or Disclosed by the Participant Member. However, any Individual’s EHI that has been Used or Disclosed prior to the Individual’s exercise of Meaningful Choice may continue to be Used or Disclosed for an Exchange Purpose. Each Participant Member shall process each exercise of Meaningful Choice from any Individual, or from other Participant Members on behalf of any Individual, and communicate the choice to the Participant with which it has a signed Participant Member Agreement within five (5) business days after receipt. The Participant Member shall post instructions on its public website explaining how an Individual can exercise Meaningful Choice. The Participant Member shall not charge Individuals any amount for their exercise of Meaningful Choice or for communicating it to the applicable Participant.

8.4 Other Legal Requirements. If and to the extent that Applicable Law requires that an Individual either consent to or approve the Use or Disclosure of his or her EHI to the Participant Member, then each Participant Member that has a Direct Relationship with the Individual shall not Use or Disclose such EHI in connection with the Participant Member Agreement unless the Participant Member has obtained the Individual’s consent, approval or other documentation with respect to such Uses or Disclosures consistent with the requirements of Applicable Law. The Participant Member shall maintain copies of such consent, approval or other documentation and may make it available electronically to any other Participant Member, Participant or QHIN upon request to the extent permitted by Applicable Law. The Participant Member shall maintain written policies and procedures to allow an Individual to revoke such consent or approval on a prospective basis.

8.5 Non-Discrimination. A Participant Member shall not unfairly or unreasonably limit exchange or interoperability with any QHIN, Participant, other Participant Member, or Individual User such as by means of burdensome testing requirements that are applied in a discriminatory manner, other means that limit the ability of a Participant Member to send or receive EHI with a QHIN, Participant, Participant Member, or Individual User slows down the rate at which such EHI is sent or received if such limitation or slower rate would have an anti-competitive effect. As used in this Section 8.5, a discriminatory manner means action that is taken or not taken with respect to any QHIN, Participant, other Participant Member, Individual User, or group of them due to the role it plays in the health care system, whether it is a competitor, whether it is affiliated with or has a contractual relationship with any other entity, or whether it has or fails to have any other characteristic; provided, however, that limitations, load balancing of network traffic or other activities, protocols or rules shall not be deemed discriminatory to the extent that they either: (i) benefit patients by prioritizing Treatment over other activities; or (ii) are based on a reasonable and good faith belief that the other entity or group has not satisfied or will not be able to satisfy the minimum obligations stated in Section 8 of the Common Agreement (including compliance with Applicable Law) in any material respect. For example, one Participant Member failing to share EHI with a Participant in a timely manner would be considered discriminatory for purposes of this Section 8.5 unless due to a permitted exception set forth above.

8.6 Written Privacy Summary. Each Participant Member agrees to publish and make publicly available a written notice in plain language that describes each Participant Member's privacy practices regarding the access, exchange, Use and Disclosure of EHI with substantially the same content as described in ONC's Model Privacy Notice. The written privacy summary shall include the following additional information: (i) a description, including at least one (1) example, of each type of Exchange Purpose; (ii) a description that provides an Individual with a reasonable understanding of how to exercise Meaningful Choice; and (iii) whom Individuals can contact for further information about the Participant Member's privacy policies. This written privacy summary requirement does not supplant the HIPAA Privacy Rule obligations of a Participant Member that is a Covered Entity to post and distribute a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520.

8.7 Minimum Security Requirements. To promote the confidentiality, integrity, and availability of EHI and minimize the potential for Breaches of EHI, each Participant Member shall be required to: (i) maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting EHI; (ii) protect against reasonably anticipated impermissible Uses and Disclosures of EHI; (iii) identify and protect against reasonably anticipated threats to the security or integrity of EHI; and (iv) monitor compliance with such safeguards by its workforce. In determining which administrative, technical and physical safeguards to implement, the Participant Member shall consider the following: (i) its size, complexity, and capabilities; (ii) its technical, hardware, and software infrastructure; (iii) the costs of security measures; and (iv) the likelihood and possible impact of potential risks to EHI. Each Participant Member further shall review and modify such safeguards to continue protecting EHI in a changing environment of security threats within a reasonable period of time. Additionally, each Participant Member shall be required to implement the following minimum security requirements described below.

8.8 Authorization. Each Participant Member's security policy shall include written authorization procedures to confirm that any entities requesting access to system functions or EHI possess the appropriate credentials (e.g., privileges granted and provisioned in security and privacy management).

8.9 Identity Proofing. Each Participant Member's security policy shall require that Individual Users with whom it has a Direct Relationship be identity proofed at a minimum of IAL2 prior to issuance of access credentials by the Participant Member. The identity information may be supplemented by Participant

Members acting as an authoritative source by using knowledge of the identity of the individuals in accordance with written policies and procedures. Such policies and procedures must be commensurate with the risk of incorrect identity proofing (*e.g.*, procedures for applicants receiving credentials to access their medical information may be less rigorous than procedures used for applicants receiving credentials that can be used to access medical information on multiple patients). For example, IAL2 identity proofing for an applicant receiving credentials to access to his or her own medical information can be accomplished by any two of the following:

a) physical comparison to legal photographic identification cards such as driver's licenses or passports, or employee or school identification badges;

b) 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

c) comparison to information from an electronic health record (EHR) containing information entered from prior encounters.

All personally identifiable information collected shall be limited to the minimum necessary to resolve a unique identity and the Participant Member shall not copy or retain such personally identifiable information.

8.10 User Authentication. Each Participant Member shall require that any Individual User that requests EHI or requests to send EHI be authenticated at a minimum of AAL2.

8.11 Auditable Events. Each Participant Member shall utilize the security policy established by the Participant with whom the Participant Member has a signed a Participant member Agreement to identify a set of auditable events. Said security policy shall be consistent with the Participant's security policy but with appropriate modifications based on the transactions being performed. Each Participant Member's security policy shall include the following auditing requirements for each Exchange Purpose that it performs:

(i) A list of auditable events described in said security policy;

(ii) An audit log including records for all auditable events identified by said security policy. A Participant Member shall retain all audit logs (both electronic and non-electronic) in accordance with Applicable Law and make such audit logs available during any audit; and

(iii) A record of an auditable event which at a minimum should include the following information:

- The description of the event;
- The date and time the event occurred;
- A success or failure indicator; and
- Where appropriate, the identity of the entity and/or operator that was responsible for the event.

8.12 Breach Notification Requirements and Security Incidents. Each Participant Member shall comply with the Breach notification requirements applicable to Business Associates pursuant to 45 CFR Part 164 Subpart D, regardless of whether it is a Business Associate; provided, however, that if the Participant Member is a Covered Entity, it shall comply with the Breach reporting requirements that apply to Covered Entities in addition to providing the notices required below. Each Participant Member further shall notify, in writing, the Participant and the following to the extent that they are affected by the Breach: other Participant Members, and Individuals with whom the Participant Member has a Direct Relationship. Such notice shall be provided without unreasonable delay in accordance with this Section and Applicable Law. Whenever possible, early notification of Discovery of the Breach is advisable in order to allow other affected parties to satisfy their reporting obligations. Each Participant Member shall implement commercially reasonable policies and procedures to address security incidents as defined at 45 CFR §164.304. Each Participant Member shall identify, if possible, and respond to suspected or known security incidents, shall mitigate, to the extent reasonably practicable, any harmful effects of any security incidents that are suspected by or known to the Participant Member, and shall document and maintain a copy of such documentation of any suspected or known security incidents and its outcomes. The foregoing does not modify or replace any obligation that a Participant Member may have under the FTC Rule with respect to a breach of security as defined in the FTC Rule if applicable.

8.13 Law Enforcement Exception to Breach Notification. Notwithstanding Section 8.12 above, if a Participant Member is notified, in writing or by oral statement by any law enforcement official, or other applicable governmental agency (e.g. Federal Trade Commission), that a Breach notification would impede a criminal investigation or cause damage to national security, and the statement has been documented consistent with 45 CFR 164.412(b), then the Participant Member shall delay the Breach notification for the time period specified by the law enforcement official.

8.14 Processing of Individual Access Services Request.

(i) An Individual User may assert his or her right of Individual Access Services with respect to a Participant Member if it has a Direct Relationship with the Participant Member. The Participant Member may require such Individual User to assert his or her right to Individual Access Services to EHI in writing and may require such Individual User to use the Participant Member's own supplied form, provided that the use of such a form does not create a barrier to or unreasonably delay the Individual User from obtaining access to the EHI. Each Participant Member shall provide Individual Users with the option of using electronic means (e.g., e-mail or secure web portal) to assert their rights for Individual Access Services to EHI.

(ii) Each Participant Member that receives a request for Individual Access Services from an Individual with whom it has a Direct Relationship shall provide such Individual with Individual Access Services with respect to his or her EHI regardless of whether the Participant Member is a Covered Entity or Business Associate; provided, however, that if the Individual wants the EHI to go to a third party, the Individual has satisfied the conditions at 45 CFR § 164.524(c)(3)(ii) as if it applies to EHI.

(iii) When the Participant Member is acting as a Business Associate and the request for Individual Access Services is received by a Covered Entity that directs the Participant Member to satisfy the request, then the Participant Member may respond to a request for Individual Access Services if permitted or required by the terms of the applicable Business Associate Agreement.

(iv) A Participant Member is prohibited from requiring the submission of a HIPAA authorization (as defined in 45 CFR §164.508) or a Business Associate Agreement (as defined in the HIPAA Rules) in order to process a request for Individual Access Services from a Participant Member who provides Individual Access Services and has been selected by the Individual User who is requesting EHI for Individual Access Services.

(v) With respect to a QHIN Query for Individual Access Services, the response shall be provided as required by these terms and conditions regardless of whether it was prompted by (a) the Individual User; or (b) a QHIN, Participant, or Participant Member who provides Individual Access Services and has been selected by the Individual User who is requesting EHI for Individual Access Services.

8.15 Notice to Individuals. When a Participant Member has a Direct Relationship with an Individual, then the Participant Member shall be responsible for notifying the Individual of the mandatory minimum provisions stated in Section 9 by posting such mandatory provisions on its public website.

8.16 Data Integrity. Each Participant Member's security policy shall include the following elements to promote data integrity of all EHI that it receives, maintains or transmits with respect to the Exchange Purposes that it performs:

(i) Procedures to safeguard that EHI is not improperly altered or destroyed;

(ii) Procedures to protect against reasonably anticipated, impermissible Uses or Disclosures of EHI;

(iii) Procedures to maintain backup copies of systems, databases, and private keys in the event of software and/or data corruption, if the Participant Member is serving as a certificate authority;

(iv) Procedures to test and restore backup copies of systems, databases, and private keys, if the Participant Member is serving as a certificate authority, so that the Participant Member can retrieve data from backup copies in the event of a disaster, emergency, or other circumstance requiring the restoration of EHI to preserve data integrity; and

(v) Procedures to document the methodologies and results of tests to restore backup copies of systems, databases, and private keys, if the Participant Member is serving as a certificate authority. Such documentation shall be maintained in a manner consistent with 45 CFR § 164.316(b).

Each Participant Member shall report known instances of inaccurate or incomplete EHI to the originator of the EHI, and request that such data integrity issues be remediated in a timely manner to the extent reasonably possible.

8.17 Transport Security. Each Participant Member's security policy shall include written policies and procedures to ensure a secure channel for communications between Participant Members and Participants.

8.18 Compliance with Applicable Law. Each Participant Member shall comply with all Applicable Law.

8.19 Minimum Necessary Requirements. Each Participant Member shall satisfy the Minimum Necessary Requirements as if they applied to EHI when it Uses or Discloses EHI and when the Participant Member requests EHI in the context of the applicable Framework Agreement. The Minimum Necessary Requirements shall apply to a Participant Member regardless of whether it is a Covered Entity or a Business Associate when it requests, Uses, or Discloses EHI. Any Minimum Necessary provisions set forth in the HIPAA Rules (e.g., 45 CFR §164.514(d)) that include conditions shall also apply to the Participant Member when Using, Disclosing or requesting EHI if such provisions are applicable.

In addition, the Minimum Necessary Requirements do not apply under certain circumstances set forth in the HIPAA Rules including the following: (i) a Disclosure of PHI to or request by a health care provider for Treatment; (ii) a Disclosure to an Individual who is the subject of the information; (iii) a Disclosure pursuant to an Individual's authorization under 45 CFR § 164.508; or (iv) Disclosures that are required by law as described in 45 CFR § 164.512(a). These exclusions apply to a Participant Member with regard to EHI.

8.20 Summary of Disclosures of EHI. Each Participant Member shall satisfy its obligations as described under Section 9.5.

8.21 Federal Agencies Serving as a Participant Member. Notwithstanding anything to the contrary in these MRTCs, a federal agency that is serving as a Participant Member and is not otherwise subject to the HIPAA Rules is not required to comply with the HIPAA Privacy and Security Rules referenced in these MRTCs. The federal agency will comply with all privacy and security requirements imposed by applicable federal law.

9. Individual Rights and Obligations

9.1 Individual User Access to EHI. An Individual User who has a Direct Relationship with a QHIN, Participant, or Participant Member, may exercise his or her right to Individual Access Services by sending a written notice to said QHIN, Participant, or Participant Member. If required by said QHIN, Participant, or Participant Member, the Individual User shall be responsible for completing the QHIN's, Participant's or Participant Member's own supplied access form provided that the use of such a form does not create a barrier to or unreasonably delay the Individual User from obtaining access to the EHI. Such Individual Users shall have the option of using electronic means (e.g., e-mail, secure web portal) to assert their rights for Individual Access Services to EHI.

9.2 Individual Use or Disclosure of EHI. Individuals shall have the right to Use or Disclose their own EHI without any limitations.

9.3 Identity Proofing. Prior to the issuance of access credentials, an Individual User shall be required to verify his or her identity at a minimum of IAL2 with the QHIN, Participant, or Participant Member to whom the Individual has a Direct Relationship.

9.4 Authentication. Prior to initiating Individual Access Services, an Individual User shall be required to authenticate at AAL2 with the QHIN, Participant, or Participant Member with whom the Individual has a Direct Relationship.

9.5 Right to Receive Summary of Disclosures of EHI.

9.5.1 Right to Request Summary and Applicable Period. As described below, Individuals shall have the right to receive a summary of Disclosures of EHI for applicable Exchange Purposes in the context of the Framework Agreements for up to a period of six (6) years immediately prior to the date on which the summary of Disclosures is requested. Individuals may submit requests for a summary of Disclosures to any QHIN, Participant, or Participant Member with which the Individual has a Direct Relationship. QHINs, Participants, and Participant Members shall provide the summary within sixty (60) days after receiving the request and shall provide an electronic means for an Individual to submit such requests. For Covered Entities, this obligation may be met by complying with the requirements of 45 CFR § 164.528.

9.5.2 Content of Summary. The content of the summary of Disclosure(s) shall contain the following information: (i) date of the Disclosure(s); (ii) name of the entity or person who received the EHI and, if known, the address of such entity or person; (iii) brief description of the EHI disclosed; and (iv) brief statement of the purpose of the Disclosure(s) that reasonably informs the Individual of the basis for the Disclosure(s) or, in lieu of such statement, a copy of the written request for the Disclosure(s).

9.5.3 Exceptions. A summary of Disclosures shall not be required for the following Disclosures: (i) for treatment, payment and health care operations (each as defined in the HIPAA Rules); (ii) to an Individual of his or her own EHI; (iii) pursuant to an Authorization under 45 CFR 164.508 executed by the Individual; (iv) to correctional institutions or law enforcement officials; (v) for national security or intelligence purposes; and (vi) if providing the summary of Disclosures of EHI would be in violation of Applicable Law.

Appendix 3:
Qualified Health Information Network (QHIN) Technical Framework

DRAFT 1

April 19, 2019

TABLE OF CONTENTS

Overview

The Qualified Health Information Network (QHIN) Technical Framework (QTF) describes the functional and technical requirements that a Health Information Network needs to fulfill to serve as a QHIN under the Common Agreement. The QTF specifies the technical underpinnings for QHIN-to-QHIN exchange and other responsibilities described in the Common Agreement.

While the Recognized Coordinating Entity (RCE) (to be selected by ONC) will establish the final operational and technical means by which QHINs exchange Electronic Health Information (EHI), the QTF Draft 1 provides an initial set of QHIN technical responsibilities for public comment. ONC expects the QTF to be updated, expanded, and specified completely for implementation based on public comment and through iterative revisions with the RCE and industry as the Common Agreement is developed and finalized.

The QTF focuses primarily on the technical and functional requirements for interoperability among QHINs, including specification of the standards QHINs must implement to enable QHIN-to-QHIN exchange of information. The technical and functional requirements described in the QTF enable the three information exchange modalities for QHINs expressed in the Common Agreement: QHIN Broadcast Query, QHIN Targeted Query, and QHIN Message Delivery.

The QTF also describes high-level functional requirements QHINs must support within their health information networks. However, the QTF Draft 1 intentionally does not specify standards QHINs must use for these internal-QHIN implementation decisions. For example, the QTF Draft 1 does *not* address the methods used by QHINs to query and deliver messages *within* their own networks and considers such requirements out of scope for the QTF. As long as the QHIN can adequately perform its duties as described in the Common Agreement and the QTF, each QHIN has the operational flexibility to select appropriate standards and approaches consistent with the needs of its business environment.

The technical and functional requirements described in the QTF Draft 1 reflect many of the technologies and standards used for network-based health information exchange today. For example, organizations supporting health information exchange nationally (e.g., Commonwell Health Alliance, eHealth Exchange, Carequality) generally use Integrating the Healthcare Enterprise (IHE) profiles such as Cross-Community Patient Discovery (XCPD)[31] and Cross-Community Access (XCA)[32] to enable clinical document exchange between disparate communities.

Although the healthcare industry has started to explore new exchange modalities, such as Representational State Transfer (RESTful) application program interfaces (APIs) and standards like Health Level Seven (HL7®) Fast Healthcare Interoperability Resources (FHIR®),[33] the QTF Draft 1 seeks to facilitate

---

[31] IHE Cross-Community Access (XCA) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[32] IHE Cross-Community Patient Discovery (XCPD) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[33] HL7 FHIR – latest version is available at: http://build.fhir.org/, including the RESTful API available at: http://build.fhir.org/http.html

the immediate availability of QHIN services. As such, the QTF Draft 1 enables organizations seeking to become QHINs to leverage their existing, deployed technical infrastructure (i.e., services based on IHE profiles) to support network-to-network exchange. The QTF Draft 1 includes requests for comment to highlight where the industry can leverage the QTF development process to recommend appropriate standards or suggest alternatives to today's commonly used technology.

1. Definitions

Definitions for many of the terms contained in this document are included in the MRTCs. Additional terms specific to the QTF are defined here:

- **QHIN Exchange Network:** The network of interconnected QHINs enabled by the Common Agreement
- **First Degree Entity**: Any entity, other than a QHIN, which directly accesses QHIN services, including Participants and Individual Users
- **Initiating QHIN**: A QHIN that initiates a QHIN Query or QHIN Message Delivery
- **Responding QHIN**: A QHIN that receives (and responds as appropriate) to a QHIN Query or QHIN Message Delivery from an Initiating QHIN
- **Message Delivery Solicitation**: A request for a QHIN to initiate a QHIN Message Delivery
- **Query Solicitation**: A request for a QHIN to initiate a QHIN Query

The term "MUST" in the QTF indicates a requirement of the specification.[34]

2. Example QHIN Exchange Scenarios

The following QHIN exchange scenarios present basic workflows for the exchange modalities expressed in the Common Agreement. Each scenario depicts a real-world use case that stakeholders might encounter. The scenarios do not represent all possible workflows or use cases. Rather, they generally describe the various functions performed by QHINs to enable information exchange through the QHIN Exchange Network.

Query Scenario

In this scenario, a healthcare provider (i.e., Participant Member) sees a new patient, and seeks to find the patient's health information through the QHIN Exchange Network to inform diagnosis and treatment. This scenario assumes basic patient demographic information is available to the provider.

The healthcare provider is a member of a local health information exchange organization (HIE), which is connected to the QHIN Exchange Network as a Participant of a QHIN. To find health information about the patient, the provider first submits a Query Solicitation to the HIE, which is routed to the QHIN over a secure channel. The Query Solicitation may include patient demographic information for patient identity resolution, query parameters indicating which information the provider is looking for, and/or a list of entities to query (if the Query Solicitation is for a QHIN Targeted Query). All systems involved in the

[34] *Key words for use in RFCs to Indicate Requirement Levels* (IETF RFC 2119) - available at: https://tools.ietf.org/html/rfc2119

request also transmit information about the provider's identity, as well as an Exchange Purpose specified by the provider ("Treatment" in this scenario).

The QHIN processes the Query Solicitation and uses the appropriate information to initiate a QHIN Query to any appropriate Responding QHINs (for a QHIN Broadcast Query, all other QHINs in the QHIN Exchange Network act as Responding QHINs). The Initiating QHIN connects to each Responding QHIN using the Internet Engineering Task Force (IETF) Transport Layer Security (TLS) protocol[35] to establish a secure channel for the QHIN Query transaction; each QHIN authenticates the other's server (i.e., mutual server authentication). After establishing a secure channel, the Initiating QHIN sends each Responding QHIN a Security Assertion Markup Language (SAML)[36] assertion conforming to the IHE Cross-Enterprise User Assertion (XUA) profile along with the query transaction.[37] The SAML assertion includes information about the provider's identity and the Exchange Purpose.

A QHIN Query typically involves two major workflows, patient discovery via IHE XCPD and document location/retrieval via IHE XCA. In the XCPD workflow, the Initiating QHIN shares patient demographic information via an XCPD request with the appropriate Responding QHIN(s). Each Responding QHIN uses the demographic information to resolve the patient's identity (i.e., "patient matching"), and returns an XCPD response with the resolved identity (including a local patient identifier, demographic information about the patient, information about providers that have seen the patient, etc.).

In the XCA workflow, the Initiating QHIN sends an XCA request including a patient identifier (obtained via the XCPD workflow in this scenario) and query parameters to the appropriate Responding QHIN(s) to discover the location of appropriate clinical documents (i.e., "record location"). Each Responding QHIN uses the query parameters and patient identity to discover clinical documents that meet the query criteria, and sends an XCA response with a list of document identifiers to the Initiating QHIN. The Initiating QHIN then requests any relevant documents, which are retrieved and shared with the Initiating QHIN by the Responding QHIN(s).

After retrieving the relevant documents, the Initiating QHIN transmits them back to the HIE that submitted the Query Solicitation, which then transmits them to the provider. Each QHIN involved in the query maintains audit logs of all activities and transactions the QHIN performed in the process of resolving the query, according to the IHE Audit Trail and Node Authentication (ATNA) profile.[38]

---

[35] *The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246

[36] Security Assertion Markup Language (SAML) – available at: https://www.oasis-open.org/standards#samlv2.0

[37] IHE Cross-Enterprise User Assertion (XUA) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

[38] IHE Audit Trail and Node Authentication (ATNA) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

Note: Queries on behalf of a patient (i.e., Individual User) for the Individual Access Services Exchange Purpose follow a similar workflow. For example, a patient's mobile application might fill the role of the Participant Member in the scenario. Likewise, First Degree Entities may also initiate a Query Solicitation.

Specified standards for a QHIN Exchange Network query are included in *Table 1*.

Table 1. Specified & Alternative Standards for QHIN Exchange Network Query

Query Functions	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Secure Channel	• IETF TLS	-
Mutual QHIN Server Authentication	• IETF TLS	-
User Authentication	• IHE XUA	-
Authorization & Exchange Purpose	• IHE XUA	• IHE Internet User Authorization (IUA)[39] • Nationwide Health Information Network (NHIN) Authorization Framework[40]
QHIN Query	• IHE XCA	• HL7 FHIR RESTful API • IHE Mobile Access to Health Documents (MHD)[41]
	• IHE XCPD	• HL7 FHIR RESTful API
Auditing	• IHE ATNA	• HL7 FHIR RESTful API

Message Delivery Scenario

In this scenario, a healthcare provider (i.e., Participant Member) treats a patient in an emergency department and then seeks to send a summary of the patient's care to the patient's primary care provider through the QHIN Exchange Network.

The healthcare provider is a member of a local health information exchange organization (HIE), which is connected to the QHIN Exchange Network as a Participant of a QHIN. To send the patient's care summary, the provider first sends a Message Delivery Solicitation to the HIE, which is routed to the QHIN over a secure channel. The Message Delivery Solicitation includes the content of the message (i.e., the care summary), patient demographic information or a patient identifier, and an identifier for the recipient(s)

[39] IHE Internet User Authorization (IUA) profile - available as a supplement to the IHE IT Infrastructure (ITI) Technical Framework at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf
[40] *Nationwide Health Information Network (NHIN) Authorization Framework* (version 3.0) – available at: https://sequoiaproject.org/wp-content/uploads/2014/11/nhin-authorization-framework-production-specification-v3.0.pdf
[41] IHE Mobile Access to Health Documents (MHD) profile – available as a supplement to the IHE IT Infrastructure (ITI) Technical Framework at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_MHD.pdf

of the message (may be known by the sender or obtained via a query transaction). Any systems involved in the request also transmit information about the provider's identity, as well as an Exchange Purpose specified by the provider ("Treatment" in this scenario).

The QHIN processes the Message Delivery Solicitation, identifies the appropriate Responding QHIN(s), and initiates a QHIN Message Delivery. The Initiating QHIN connects to each Responding QHIN using the TLS protocol to establish a secure channel for the QHIN Message Delivery transaction; each QHIN authenticates the other's server. After establishing a secure channel, the Initiating QHIN sends each Responding QHIN a SAML assertion conforming to the IHE XUA profile along with the message delivery transaction. The SAML assertion includes information about the provider's identity and the Exchange Purpose.

The QHIN Message Delivery transaction uses the IHE Cross-Community Document Reliable Interchange (XCDR) profile[42] to send the provider's message and other metadata from the Initiating QHIN to the Responding QHIN(s). Each Responding QHIN then converts the XCDR transaction into the appropriate format, if necessary, and transmits the message to the appropriate recipient(s) in their network. The recipient(s) return an acknowledgement message with appropriate disposition information to the Responding QHIN, which forwards the acknowledgment to the Initiating QHIN. The Initiating QHIN sends the acknowledgement through its network, from the HIE to the originating provider.

Each QHIN involved in the message delivery maintains audit logs of all activities and transactions the QHIN performed in the process of delivering the message, according to the IHE ATNA profile.

Note: Message Delivery on behalf of a patient (i.e., Individual User) for the Individual Access Services Exchange Purpose follows a similar workflow. For example, a patient may direct their provider to send EHI to a mobile application or another provider. Likewise, First Degree Entities may also initiate a Message Delivery Solicitation.

---

[42] IHE Cross-Community Document Reliable Interchange (XCDR) profile - available as a supplement to the IHE IT Infrastructure (ITI) Technical Framework at:
http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf

Specified standards for QHIN Exchange Network message delivery are included in *Table 2*.

Table 2. Specified & Alternative Standards for QHIN Exchange Network Message Delivery

Message Delivery Functions	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Secure Channel	• IETF TLS	-
Mutual QHIN Server Authentication	• IETF TLS	-
User Authentication	• IHE XUA	-
Authorization & Exchange Purpose	• IHE XUA	• IHE IUA • NHIN Authorization Framework
Message Delivery	• IHE XCDR	• Direct[43] • HL7 FHIR RESTful API
Auditing	• IHE ATNA	• HL7 FHIR RESTful API

3. Functions and Technology to Support Exchange

Under the Common Agreement, QHINs serve as exchange hubs between disparate health information networks. Participants, Participant Members, and Individual Users can request to send or receive EHI through the QHIN Exchange Network.

Broadly, QHINs are responsible for providing a set of Connectivity Services that support QHIN Broadcast Query, QHIN Targeted Query, and QHIN Message Delivery. To effectively deliver Connectivity Services, QHINs must perform a consistent set of technical functions.

This section outlines these functions, specifying standards and implementation approaches where applicable. In some cases, the healthcare industry has not coalesced around a single standard or preferred approach. For these, the QTF outlines the high-level technical function(s) that QHINs must support and seeks comment on which standards the QTF should specify for implementation.

Future versions of the QTF will include more detailed requirements for QHINs, as determined by the RCE. For example, the QTF may further constrain IHE profiles, require QHINs to support specific data elements/fields, further specify message semantics, etc.

Certificate Policy

Public key infrastructure (PKI) often serves as the basis for securing electronic communications over the internet. PKI involves the use of digital certificates to assert and authenticate identities, encrypt data, and sign communications.

---

[43] *Applicability Statement for Secure Health Transport* (version 1.2) – available at: http://wiki.directproject.org/Applicability_Statement_for_Secure_Health_Transport

The QTF Draft 1 specifies that QHINs must possess appropriate digital certificates for authentication, encryption, and signing. QHIN certificates will be chained to root certificates issued by approved Certificate Authorities, as determined by the RCE. The RCE may also establish a broader certificate policy (e.g., including certificate life-cycle operational requirements, certificate usage policies, naming conventions, etc.). However, such a policy is out of scope for the QTF Draft 1.

The QTF Draft 1 specifies the following Certificate Policy functions:

- QHINs MUST obtain digital certificates that adhere to and/or follow the IETF RFC 5280 specification,[44] Applicable Law, and any policies and procedures determined by the RCE
- QHINs MUST deploy cryptographic modules certified to meet Federal Information Processing Standards (FIPS) Publication 140-2[45]

Secure Channel

Protecting the privacy and security of EHI transmitted across the QHIN Exchange Network is essential for building trust among participating entities. As such, QHINs must provide a secure channel to ensure transport-level security for all transactions under their domain. Modern networked systems typically rely on the TLS protocol to communicate over the internet. TLS provides privacy and data integrity between systems, using cryptographic techniques to encrypt communications between the systems. Specified standards for Secure Channel are included in *Table 3.*

Table 3. Specified & Alternative Standards for Secure Channel

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Secure Channel	• IETF TLS	-

[44] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (IETF RFC 5280) - available at: https://tools.ietf.org/html/rfc5280

[45] *Security Requirements for Cryptographic Modules* (FIPS Publication 140-2) - available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

The QTF Draft 1 specifies the following Secure Channel functions:

- When interacting with another QHIN, a QHIN MUST establish a secure channel using TLS protocol version 1.2 or above
    a. Use of the TLS protocol MUST be consistent with IETF BCP 195[46]
- When interacting with a First Degree Entity, a QHIN MUST establish a secure channel

** ONC Request for Comment #1: Should the QTF specify additional standards or approaches for securing QHIN Exchange Network transactions (e.g. OASIS Web Services Security[47])?*

Mutual QHIN Server Authentication

TLS also provides a "handshake" authentication protocol to verify the identities of systems establishing a secure channel. Whereas TLS can be implemented such that only "one side" (e.g., the server in a server-client relationship) is authenticated, the QTF Draft 1 specifies mutual authentication for QHIN-to-QHIN communication (i.e., both QHINs must authenticate). Specified standards for Mutual QHIN Server Authentication are included in *Table 4*.

Table 4. Specified & Alternative Standards for Mutual QHIN Server Authentication

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Mutual QHIN Server Authentication	• IETF TLS	-

The QTF Draft 1 specifies the following Mutual QHIN Server Authentication function:

- QHINs MUST mutually authenticate when interacting with another QHIN, using TLS protocol version 1.2 or above

User Authentication

Authentication involves establishing confidence in the identity of an entity. All entities requesting use of the QHIN Exchange Network must be authenticated and authentication information must be shared "upstream" for access control and auditing purposes. A QHIN, for example, needs to know and record the identity of any Participant Member or Individual User attempting to query for or send EHI using the QHIN Exchange Network. Because Participant Members only have a relationship with Participants, the QHIN has to rely on a Participant to obtain and share authentication information about a Participant Member.

The QTF Draft 1 does not specify how entities must perform authentication, how QHINs should obtain authentication information about entities within their networks, or how QHINs and other entities should

[46] *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* (IETF BCP 195) - available at: https://tools.ietf.org/html/bcp195
[47] Web Services Security – available at: https://www.oasis-open.org/standards#wssv1.1.1

represent authentication information internally. QHINs, however, must share authentication information with other QHINs using a consistent format.

SAML is an XML-based specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. The IHE XUA Profile leverages SAML to communicate claims about an authenticated entity in transactions that cross enterprise boundaries. The QTF Draft 1 specifies that QHINs implement IHE XUA to support exchange of authentication information among QHINs. Specified standards for User Authentication are included in *Table 5*.

Table 5. Specified & Alternative Standards for User Authentication

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
User Authentication	• IHE XUA	-

The QTF Draft 1 specifies the following User Authentication functions:

- When initiating a QHIN Query or QHIN Message Delivery, a QHIN MUST transmit a SAML assertion using IHE XUA, identifying any staff or users at the QHIN, Participants, and/or Participant Members involved in requesting use of QHIN Connectivity Services
- QHINs MUST be capable of receiving authentication information from First Degree Entities, including the authenticated identity of any Participant Members and/or Individual Users requesting to use the QHIN Exchange Network
    - QHINs MUST specify the mechanism (i.e., format and content) by which First Degree Entities transmit authentication information to the QHIN

** ONC Request for Comment #2: What specific elements should a SAML assertion for User Authentication include?*

Authorization & Exchange Purpose

Authorization involves verifying whether an entity is eligible to access a requested network or service.

All entities participating in the QHIN Exchange Network must sign an appropriate Framework Agreement (i.e., Common Agreement, Participant-QHIN Agreement, or Participant Member Agreement) and are thereby authorized to request use of core functions of the QHIN Exchange Network, such as QHIN Connectivity Services. However, the MRTCs require that all requests to send and receive EHI fall under a defined set of Exchange Purposes:

- Treatment
- Utilization Review
- Quality Assessment and Improvement
- Business Planning and Development
- Public Health

- Individual Access Services
- Benefits Determination

In order to comply with the MRTCs, QHINs must be capable of receiving and transmitting authorization information, including a representation of the Exchange Purpose, along with any request for use of Connectivity Services. The QTF Draft 1 specifies that QHINs use SAML assertions based on the IHE XUA profile to identify one or more Exchange Purposes when initiating a QHIN Query or QHIN Message Delivery. Specified standards for Authorization & Exchange Purpose are included in *Table 6*.

Table 6. Specified & Alternative Standards for Authorization & Exchange Purpose

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Authorization & Exchange Purpose	• IHE XUA	• IHE IUA • NHIN Authorization Framework

The QTF Draft 1 specifies the following Authorization & Exchange Purpose functions:

- When initiating a QHIN Query or QHIN Message Delivery, a QHIN MUST transmit a SAML assertion using IHE XUA, including the Exchange Purpose as identified by the staff or users at the QHIN or First Degree Entity requesting to use the QHIN Exchange Network
- QHINs MUST be capable of receiving authorization information including an Exchange Purpose from a First Degree Entity
    - QHINs MUST specify the mechanism (i.e., format and content) by which First Degree Entities transmit authorization information including an Exchange Purpose to the QHIN

** ONC Request for Comment #3: Should QHINs be required to transmit other authorization information (e.g., user roles, security labels) in addition to Exchange Purpose and any information required by IHE XUA? What specific elements should a SAML assertion include?*

Query

Today, many health information networks support queries for patient information maintained as clinical documents, such as care summaries formatted using the HL7 Clinical Document Architecture specification.[48] IHE provides two widely implemented profiles supporting query-based, network-to-network document exchange: XCPD and XCA.

XCPD enables entities to locate communities that hold relevant patient health data and correlate patient identifiers across communities holding the same patient's data. XCA supports the means to query and retrieve relevant patient health data held by other communities in the form of documents. Using XCA

[48] HL7 CDA® Release 2 – available at: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

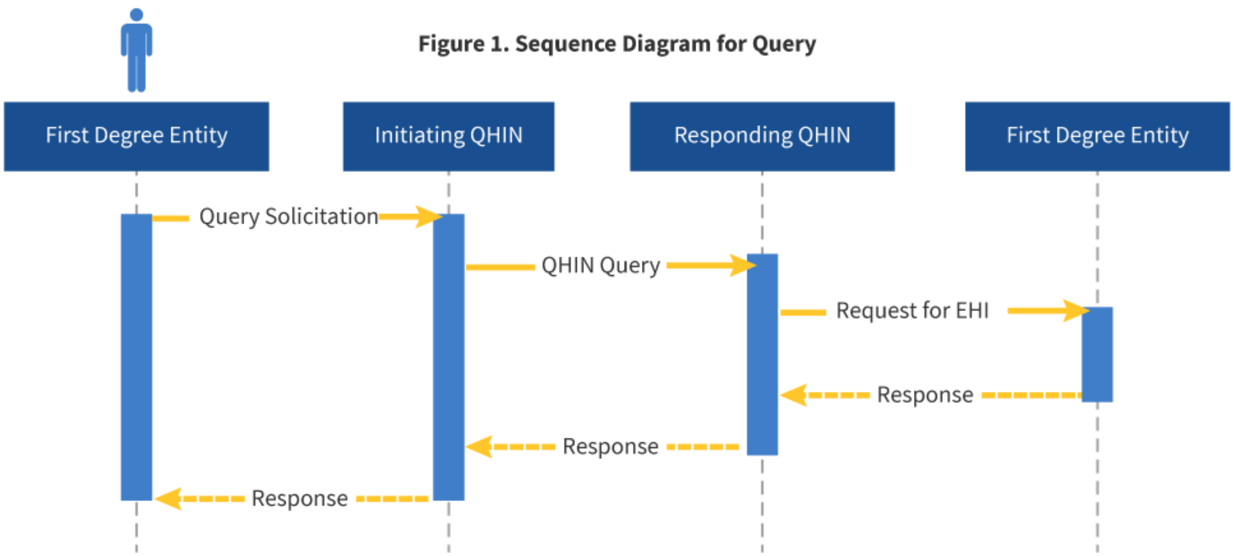
requires knowledge of patient identity when querying for and retrieving clinical documents. Thus, XCA implementations often use XCPD to resolve identities across communities before making XCA requests.

The QTF Draft 1 specifies that QHINs implement the IHE XCA and XCPD profiles to enable query-based network-to-network document exchange. These profiles satisfy a QHIN's obligations under the Common Agreement to initiate and respond to a QHIN Query. Specified standards for Query are included in *Table 7*. A sequence diagram for Query is included in *Figure 1*, and represents both XCPD and XCA transactions.

Table 7. Specified & Alternative Standards for Query

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Query	• IHE XCA	• HL7 FHIR RESTful API • IHE MHD
	• IHE XCPD	• HL7 FHIR RESTful API

Figure 1. Sequence Diagram for Query



The QTF Draft 1 specifies the following functions for Query:

- QHINs MUST specify the format and content of acceptable Query Solicitations
- QHINs MUST implement the IHE XCA and XCPD profiles for QHIN Query
- Initiating QHINs MUST be capable of receiving Query Solicitations from a First Degree Entity
    - Initiating QHINs MUST be capable of processing Query Solicitations to determine the appropriate Responding QHIN(s)
    - Initiating QHINs MUST be capable of processing Query Solicitations to identify patient demographic information to include in XCPD requests to the appropriate Responding QHIN(s)

  - Initiating QHINs MUST be capable of processing Query Solicitations to identify query parameters to include in XCA requests to the appropriate Responding QHIN(s)
- Responding QHINs MUST be capable of processing XCPD requests to resolve patient identity (see Patient Identity Resolution function)
- If necessary, Initiating QHINs MUST be capable of processing XCPD responses and sending the results to the First Degree Entity that sent the Query Solicitation
- Responding QHINs MUST be capable of processing XCA requests to identify and retrieve appropriate documents
- Initiating QHINs MUST be capable of processing XCA responses and sending the results to the First Degree Entity that sent the Query Solicitation

** ONC Request for Comment #4: The Query function above describes a general workflow and set of capabilities for QHINs conducting query-based, inter-network document exchange. However, implementations may vary and result in divergence from the basic workflow. For example, a QHIN might fail to definitively resolve patient identity and consequently rely on a participant or Participant Member to determine the correct match. Likewise, Carequality's Query-Based Document Exchange Implementation Guide[49] describes a number of alternate flows based on a "nominal flow." To inform subsequent work with the RCE to develop more specific technical guidance to address variation, comments are requested on the basic function presented and potential variations to consider.*

** ONC Request for Comment #5: The IHE XCA profile supports a number of defined queries (e.g., FindDocuments, GetAll, GetDocuments, GetRelatedDocuments, etc.). Each query includes a number of optional parameters. Should the QTF specify which queries/parameters a QHIN must support? Which queries/parameters are most widely implemented and/or useful today?*

** ONC Request for Comment #6: The IHE XCA profile is content-agnostic; it enables queries for documents based on metadata about the document but not the contents of the document itself. Therefore, the XCA profile does not necessarily support more granular queries for discrete data (e.g., a request for all clinical documents about a patient that contain a specific medication or laboratory result). Comments are requested on other appropriate standards to consider for implementation to enable more discrete data queries, such as emerging IHE profiles leveraging RESTful APIs and/or use of HL7 FHIR.*

Message Delivery

In addition to query-based document exchange, many health information networks today also provide capabilities for users to send (i.e., push) patient data to other entities. Such networks typically support Direct messaging, which leverages email protocols to securely send health information to a known Direct address.

The QHIN Exchange Network complements existing point-to-point exchange modalities like Direct. In cases where a sender knows the Direct address of a recipient, the sender can effectively send a message without relying on the QHIN Exchange Network. However, a sender may not know a recipient's Direct

[49] Carequality *Query-Based Document Exchange Implementation Guide* - available at: https://sequoiaproject.org/carequality/resources/

address or may not use Direct. In such cases, the QHIN Exchange Network provides a complementary set of Message Delivery capabilities.

The IHE XCDR profile enables entities to send documents across communities. Sending and receiving communities can implement the XCDR profile in a manner that supports local workflows, such as IHE Cross-Enterprise Document Sharing (XDS)[50] or IHE Cross-Enterprise Document Reliable Interchange (XDR).[51]

The QTF Draft 1 specifies that QHINs implement the IHE XCDR profile to support push-based, network-to-network document exchange. Implementation of the XCDR profile satisfies a QHIN's obligations under the Common Agreement to initiate and perform a QHIN Message Delivery. Specified standards for Message Delivery are included in *Table 8*. A sequence diagram for Message Delivery is included in *Figure 2*.

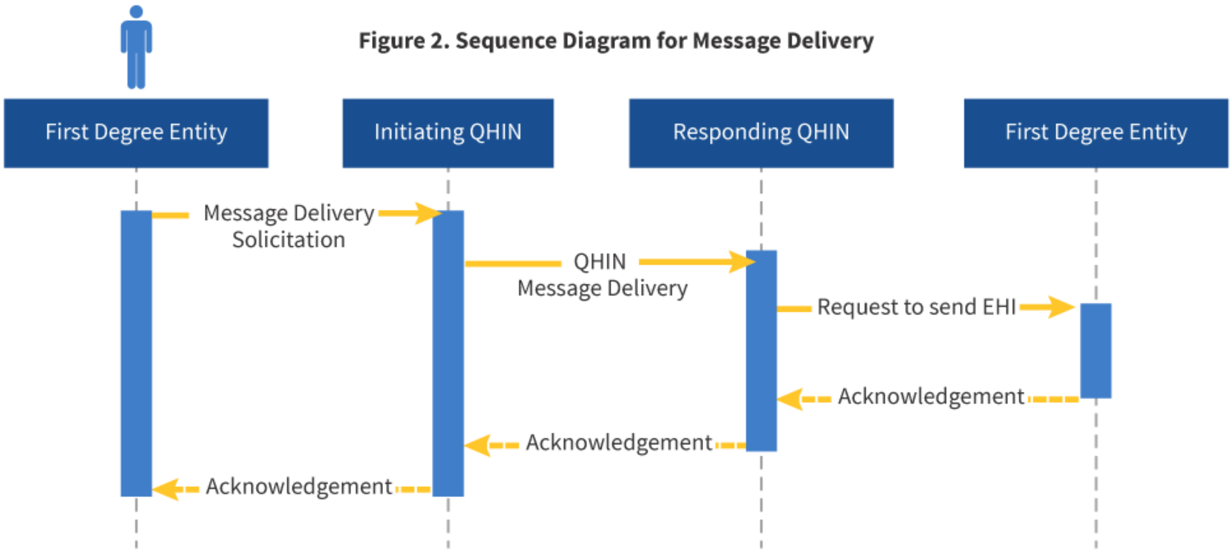
Table 8. Specified & Alternative Standards for Message Delivery

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Message Delivery	• IHE XCDR	• Direct • HL7 FHIR RESTful API

[50] IHE Cross-Enterprise Document Sharing (XDS) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

[51] IHE Cross-Enterprise Document Reliable Interchange (XDR) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

Figure 2. Sequence Diagram for Message Delivery



The QTF Draft 1 specifies the following functions for Message Delivery:

- QHINs MUST specify the format and content of acceptable Message Delivery Solicitations
- QHINs MUST implement the IHE XCDR profile for QHIN Message Delivery
    - Initiating QHINs MUST be capable of receiving Message Delivery Solicitations from a First Degree Entity
    - Initiating QHINs MUST be capable of processing Message Delivery Solicitations to determine the appropriate Responding QHIN(s)
    - Initiating QHINs MUST be capable of processing Message Delivery Solicitations to identify documents and associated metadata to include in XCDR transactions to the appropriate Responding QHIN(s)
- Responding QHIN(s) MUST be capable of processing XCDR transactions to send documents and associated metadata to the appropriate First Degree Entity(ies)
- QHINs MUST be capable of sending and receiving message delivery acknowledgements to and from QHINs and First Degree Entities

Patient Identity Resolution

Patients frequently cross network boundaries when receiving care, contributing to fragmentation of records, duplicate records, and inconsistent representations of patient identity among disparate providers. Accurately resolving patient identity is necessary for ensuring appropriate access to EHI, particularly in query-based contexts. Some QHINs might use a centralized master patient indexing service to manage identity information associated with patients interacting with providers under the QHIN's domain. Other QHINs might rely on more federated approaches to resolve patient identity (e.g., by sending patient demographic information to each Participant connected to the QHIN).

The QTF Draft 1 specifies the following Patient Identity Resolution functions:

- A QHIN MUST be capable of accurately resolving requests to match patient demographic information with patient identities under its domain

** ONC Request for Comment #7: The IHE XCPD profile only requires a minimal set of demographic information (i.e., name and birth date/time). Should QHINs use a broader set of specified patient demographic elements to resolve patient identity? What elements should comprise such a set?*

** ONC Request for Comment #8: There are many possible approaches to Patient Identity Resolution, each with its own benefits and risks. For example, a centralized index of patient identity information may be more efficient for resolving patient identities across disparate communities, but also poses a greater risk to privacy if the system is compromised. Federated approaches may be less susceptible to external threats like cyberattacks, but harder to scale across many communities. Recognizing that new technologies and business entities with robust identity matching solutions may disrupt traditional approaches, should the QTF specify a single standardized approach to Patient Identity Resolution across QHINs?*

** ONC Request for Comment #9: Different communities tolerate different degrees of risk with respect to accurately matching patient identities. Should QHINs meet a minimum performance standard (e.g., a minimum acceptable matching accuracy rate) over a specified time period? Likewise, different algorithmic techniques for matching patient identities use different approaches and must be tuned to the applicable patient population and continuously refined over time. Should QHINs measure and report on the performance of the algorithm(s) they rely on (e.g., by calculating precision, recall, etc.)?*

Record Location

The network-to-network exchange functions enabled by the QHIN Exchange Network depend on accurately determining which entities maintain patient EHI. Query functions, in particular, rely on accurate and comprehensive record location. The QTF Draft 1 does not specify a particular technology or standard for QHINs to use to locate patient records. Some QHINs might provide a centralized record locator service to track the location of patient records under the QHIN's domain. Other QHINs may rely on their Participants to locate records and share those locations with the QHIN.

The QTF Draft 1 specifies the following Record Location function:

- A QHIN MUST be capable of accurately identifying the location of all appropriate patient EHI prior to responding to a QHIN Query

** ONC Request for Comment #10: Recognizing there are different ways to implement Record Location services, should the QTF specify a single standardized approach across QHINs?*

Directory Services

Directory services enable entities to manage information associated with healthcare organizations and individuals. A provider directory, for example, may include information about a provider's demographics (e.g., name, date of birth), relationships (e.g., where a provider works), and electronic endpoints (e.g., a Direct address, HL7 FHIR server URL). QHINs may need to rely on directories to facilitate exchange of EHI through the QHIN Exchange Network. For instance, a QHIN might use a directory to identify the appropriate recipient(s) of a QHIN Message Delivery or QHIN Targeted Query.

The IHE Healthcare Provider Directory (HPD) profile[52] supports queries against, and management of, healthcare provider information that may be publicly shared in a directory structure. However, IHE HPD has not been broadly implemented by the industry. Likewise, the Argonaut Project has developed a FHIR-based specification for provider directories,53 which has also had limited adoption.

The QTF Draft 1 does not specify a particular technology or standard for QHINs to implement Directory Services.

** ONC Request for Comment #11: Should the QTF require QHINs to implement Directory Services? Recognizing there are many possible approaches for implementing Directory Services, should the QTF specify a single standardized approach? If QHINs implement Directory Services, which entities should be included in directories? Should directories be made publicly accessible?*

Individual Privacy Preferences

Individuals whose EHI is available through the QHIN Exchange Network can choose to opt-out of further use and disclosure of their EHI through the network altogether by exercising Meaningful Choice. However, the healthcare industry has not established a common approach for electronically managing patient privacy preferences. Standards to address privacy preference include the IHE Basic Patient Privacy Consents (BPPC) Profile,[54] the IHE Advanced Patient Privacy Consents (APPC) Profile,[55] and the HL7 FHIR Consent Resource, but have not been widely adopted. Therefore, the QTF Draft 1 does not specify a particular technology or standard for QHINs to use to manage Individual privacy preferences.

The QTF Draft 1 specifies the following functions for managing Individual Privacy Preferences:

- A QHIN MUST collect and utilize Meaningful Choice notices received from any First Degree Entity or QHIN
  - A QHIN MUST electronically communicate Meaningful Choice notices to all other QHINs
  - A QHIN MUST electronically maintain Meaningful Choice notices
  - A QHIN MUST use electronically maintained Meaningful Choice notices to determine whether to initiate QHIN Queries or QHIN Message Deliveries

** ONC Request for Comment #12: Future drafts of the QTF will specify a format for Meaningful Choice notices communicated between QHINs. Which standard/format should the QTF specify? What information*

[52] IHE Healthcare Provider Directory (HPD) profile - available as a supplement to the IHE IT Infrastructure (ITI) Technical Framework at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf
[53] Argonaut Provider Directory Implementation Guide (Release 1) - available at: http://www.fhir.org/guides/argonaut/pd/

[54] IHE Basic Patient Privacy Consents (BPPC) profile - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[55] IHE Advanced Patient Privacy Consents (APPC) profile is available as a supplement to the IHE IT Infrastructure (ITI) Technical Framework at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf

should be included in a Meaningful Choice notice (e.g., should a notice include patient demographic information to enable QHINs to resolve the identity of the Individual that exercised Meaningful Choice)?

** ONC Request for Comment #13: In addition to enabling Meaningful Choice, the Common Agreement requires QHINs to collect other information about an Individual's privacy preferences such as consent, approval, or other documentation when required by Applicable Law. Should the QTF specify a function to support the exchange of such information through the QHIN Exchange Network? Which standards and/or approaches should the QTF specify for this function?*

Auditing

Maintaining records of activities and transactions over the QHIN Exchange Network can assist with troubleshooting and help facilitate monitoring for improper use of the network. Moreover, audit records support a QHIN's obligation to provide Individuals with a summary of disclosures of their EHI.

The IHE ATNA profile describes a number of foundational elements of secure systems, including node authentication, user authentication, telecommunications encryption, and event audit logging. The QTF Draft 1 specifies that QHINs implement the IHE ATNA profile requirements specific to event audit logging for activities and transactions between QHINs, including the standard schema for encoding reported events, standard reportable events, and standard transport methods. Other elements of secure systems defined by ATNA, such as authentication, are specified elsewhere in the QTF Draft 1. QHINs must also maintain audit records for transactions with First Degree Entities, but the QTF Draft 1 does not specify a particular standard or approach. QHINs should consider implementing the IHE ATNA event audit logging requirements for all audit related functions. Specified standards for Auditing are included in *Table 9*.

Table 9. Specified & Alternative Standards for Auditing

Function	Specified Standard / Profile	Alternative / Emerging Standard / Profile
Auditing	• IHE ATNA	• HL7 FHIR RESTful API

The QTF Draft 1 specifies the following Auditing functions:

- A QHIN MUST create and store audit records in accordance with the IHE ATNA profile for all activity and transaction events involving another QHIN
    - A QHIN MUST follow auditing guidance for any of the IHE transactions implemented by the QHIN in support of the IHE profiles specified by the QTF Draft 1
- A QHIN MUST create and store audit records for activity and transaction events involving a First Degree Entity
- A QHIN MUST create and store audit records for activity events related to the QHIN's operation

** ONC Request for Comment #14: QHINs may participate in a variety of activities and transactions involving First Degree Entities and/or internal operations, including receiving and processing Query and Message Delivery Solicitations, performing Patient Identity Resolution, performing Record Location, sending EHI, receiving EHI, performing queries, granting/revoking access credentials, etc. Future versions of the QTF may specify a list of events a QHIN must record involving First Degree Entities and/or internal operations. Which activities and transactions should the QTF specify as auditable events? What information should the QHIN record about each event?*

Error Handling

Activities and transactions over the QHIN Exchange Network may fail or otherwise generate errors. Error messages should clearly communicate the cause of the error along with any other appropriate details to assist in resolving the issue.

The QTF Draft 1 specifies the following Error Handling functions:

- A QHIN MUST be capable of generating, sending, and receiving error messages for activities and transactions involving other QHINs
- A QHIN MUST be capable of generating, sending, and receiving error messages for activities and transactions involving First Degree Entities

* ONC Request for Comment #15: Should the QTF specify a consistent set of error messages for interactions between QHINs? Which error messages should the QTF specify? Should the QTF specify a consistent format for error messages?