Coppersmith Briefs

What You Need to Know about TEFCA: The Common Agreement

Melissa Soliz, Coppersmith Brockelman PLC
Edited by Merrill Hodnefield | *Affiliated with Coppersmith Brockelman PLC on designated matters, admitted in Michigan*

February 2, 2022
Technical correction made on March 3, 2022
Substantive revisions made on April 4, 2022

Introduction

On January 18, 2022, the U.S. Department of Health and Human Services (HHS), Office of National Coordinator for Health Information Technology (ONC), in cooperation with the Sequoia Project—the Regional Coordinating Entity (RCE), published the Trusted Exchange Framework, Common Agreement version 1 (v1) and QHIN Technical Framework v1 (collectively, "TEFCA"). The RCE also released a number of Standard Operating Procedures (SOPs), FHIR Roadmap for TEFCA Exchange, and User's Guide to the Trusted Exchange Framework (see RCE Common Agreement Resources). **Participation in TEFCA is voluntary and not currently mandated by other ONC and CMS interoperability regulations.** It does not affect a person's or organization's participation in other exchange activities.

This briefing provides health information exchanges/networks (collectively, "HINs"), health care providers, health plans, and other interested stakeholders with the information they need to know about participating in TEFCA.

The Trusted Exchange Framework and Common Agreement

The 21st Century Cures Act of 2016 (the "Cures Act") required ONC, in collaboration with other relevant departments of HHS, to develop a trusted exchange framework and common agreement to support nationwide data exchange.[1] The goal is to provide a single onramp for individuals and organizations to exchange health data in compliance with a complex patchwork of state and federal health information privacy and access laws. The TEFCA infrastructure is intended to support a wide range of participants and use cases ranging from individuals and individual access requests to providers and payers for treatment, payment and health care operation purposes, as well as public health authorities for public health activities.

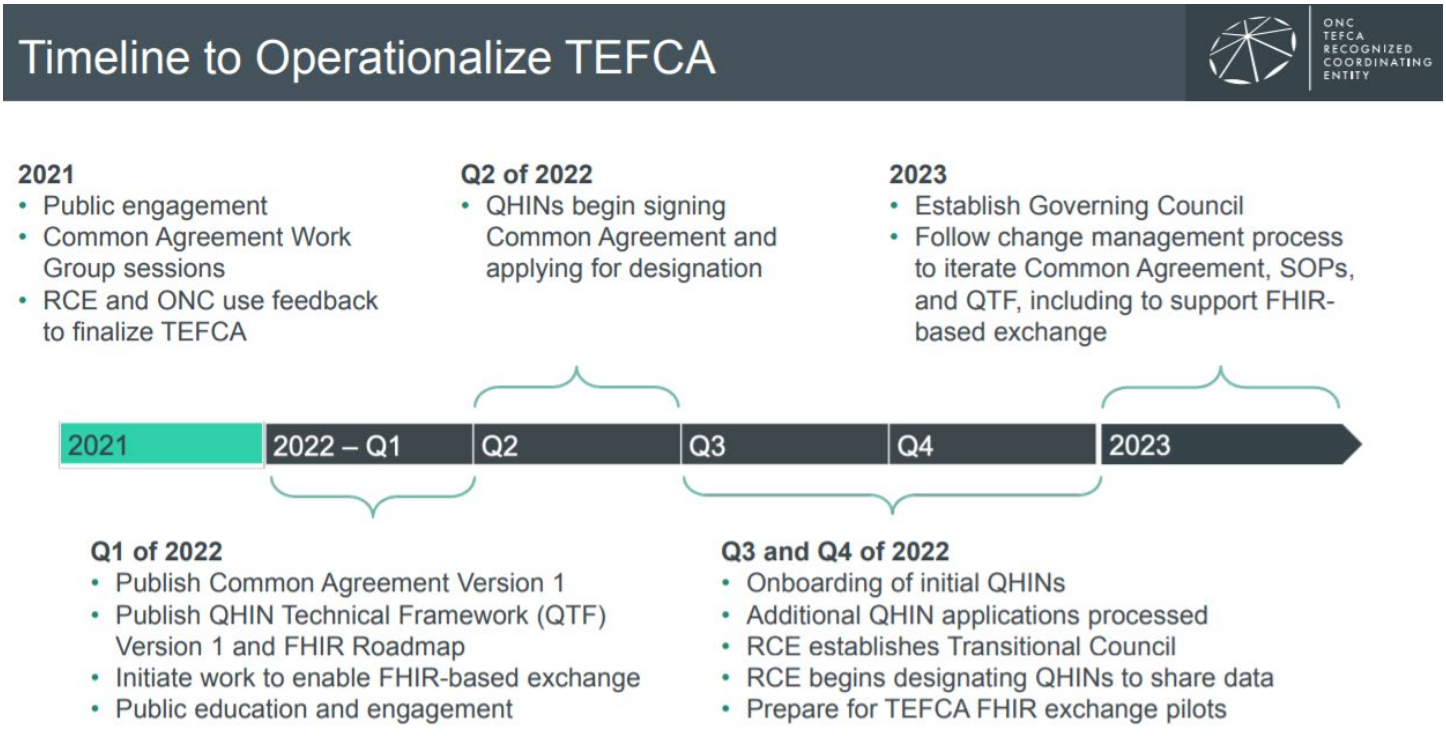
ONC published the first draft of TEFCA in January of 2018, followed by the second draft in April of 2019.[2] On January 18, 2022, ONC released the final TEFCA for implementation by the RCE.

TEFCA consists of the following seven core components:

- Trusted Exchange Framework
- Common Agreement
- Standard Operating Procedures (SOPs)
- QHIN Technical Framework (QTF)
- QHIN Onboarding
- Metrics
- Governing Approach

This briefing focuses primarily on the key features of the Common Agreement. However, it also provides a high level of summary of the other components, as well as a list of resource if you are interested in learning more about TEFCA. Importantly, participation in TEFCA is voluntary and is not currently required (or afforded safe harbor protection) by other interoperability mandates, such as the ONC Information Blocking Rule[3] or CMS Interoperability and Patient Access Final Rule.[4]

Below is a graphic created by the RCE that depicts the RCE's timeline for operationalizing the TEFCA components described in this briefing:[5]



The Trusted Exchange Framework

The Trusted Exchange Framework v1 is a set of seven, non-binding principles. While non-binding, these policy principles help explain the terms and conditions of the Common Agreement. These seven principles are:

- **Standardization.** HINs should prioritize federally recognized and industry recognized technical standards, policies, best practices, and procedures. Specifically, HINs should use standards adopted by HHS for HIPAA Standard Transactions and the ONC Health IT Certification Program, including updated standards approved through the Standards Version Advancement Process (SVAP).

- **Openness and Transparency.** HINs should conduct activities openly and transparently, wherever possible. This means that HINs should make their participation agreements publicly available; publicly specify and have all their participants agree to the uses and disclosure of electronic health information (EHI) over their networks; publish and keep current their privacy practices; and establish and implement an equitable and transparent dispute resolution process.

- **Cooperation and Non-Discrimination.** HINs should collaborate with stakeholders across the continuum of care to electronically exchange digital health information, even when a stakeholder may be a business competitor. For example, HINs should **not**: (1) treat EHI as an asset; (2) withhold EHI when requested for legally permissible treatment, payment and health care operations purposes; (3) establish internal policies and procedures for improper withholding of EHI; (4) implement technology in a manner that improperly withholds EHI; (5) make knowingly misleading statements regarding privacy and security laws as a pretext for withholding EHI; (6) charge unreasonable fees or use fees to interfere with EHI exchange between HINs; (7) use contract provisions or proprietary technology to limit interoperability; or (8) use other methods to discourage or impede interoperability with competitors or potential competitors.

- **Privacy, Security, and Safety.** HINs should exchange digital health information in a manner that supports privacy; ensures data confidentiality, integrity, and availability; and promotes patient safety. This means that HINs should: (1) ensure that EHI is exchanged and used in a manner that promotes safe care and wellness, including consistently and accurately matching EHI to an individual; and (2) enforce policies concerning individuals' ability to consent to the access, exchange, or use of their EHI consistently with applicable law.

- **Access.** HINs should ensure that individuals and their authorized caregivers have easy access to their digital health information and understand how it has been used or disclosed and HINs should comply with civil rights obligations on accessibility. Thus, HINs should not impede or impose any unnecessary or unreasonable barriers to the ability of individuals or their legal representatives to access or direct

their EHI to designated third parties, or to learn how information about them has been accessed or disclosed.

- **Equity.** HINs should consider the impacts of interoperability on different populations and throughout the lifecycle of the activity. Accordingly, HINs should use a health equity by design approach and consider health equity consequences of policy and technology choices before making these decisions. HINs should also evaluate interoperability efforts to ensure health equity is being achieved and adjust when it is not.

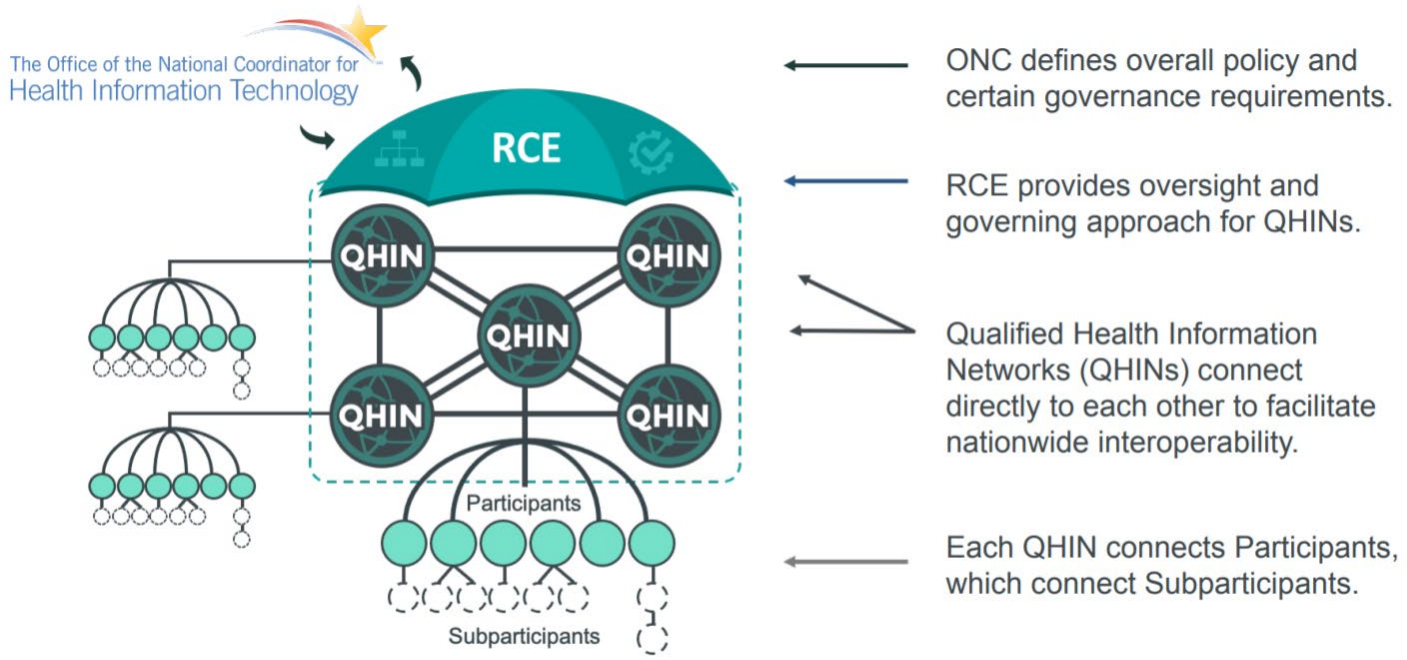
- **Public Health.** HINs should support public health authorities and population-level use cases to enable the development of a learning health system that improves the health of the population and lowers the cost of care. This means that HINs should consider use cases that advance public health, population health, quality improvement and research.

Key Features of the Common Agreement

The Common Agreement establishes the contractual, legal and governance infrastructure to support the entire TEFCA network. Is it is a 64-page legal agreement between the RCE and a "signatory" that desires to be designated as a QHIN. A QHIN is an entity that has the technical and organizational capabilities to connect diverse participants to support nationwide data exchange (see Section 1. QHINs: Eligibility and Ongoing Requirements).

The Common Agreement incorporates by reference the SOPs and QHIN Technical Framework discussed below. And although it is only binding as between the RCE and signatory, it contains a number of contractual provisions that the signatory ***must*** flow down to its "Participants"—U.S. entities that have entered into an agreement with the QHIN for TEFCA data exchange—and that Participants must flow down to any "Subparticipants"—U.S. entities that have entered into an agreement with the Participant or another Subparticipant for TEFCA data exchange (collectively, "Flow-Downs"). In this way, the Common Agreement will require all persons and entities participating in the TEFCA infrastructure to comply with the same "rules of the road" when engaging in data exchange through a TEFCA network. Importantly, neither the RCE nor any QHIN, Participant, or Subparticipant is required under the Common Agreement to be a HIPAA covered entity or business associate.

The following graphic created by the RCE depicts the TEFCA infrastructure:[6]



Due to its length, it is not feasible to summarize each provision of the Common Agreement. Rather, this briefing breaks down the Common Agreement v1 topically by its key features:

1. QHINs: Eligibility and Ongoing Requirements (Sections 4, 14 and 16)
2. Participants and Subparticipants: Flow-Downs (Throughout)
3. Governance and Change Management (Sections 3 and 5)
4. Requirement of Cooperation and Non-Discrimination (Section 6)
5. Exchange Purposes and Downstream Uses (Section 9)
6. Individual Access Services (IAS) and IAS Providers (Sections 9 and 10)
7. TEFCA Privacy and Security Requirements (Sections 11 and 12)
8. TEFCA Fee Schedule and QHIN Fees (Section 17)
9. Other Important Business Terms (Sections 7, 13, 15 and 18)

Please note: This topical summary of the Common Agreement is provided for educational and information purposes only. This is not legal advice. Organizations should consult with their attorney for legal advice regarding how the Common Agreement may apply to them.

1. QHINs: Eligibility and Ongoing Requirements (Sections 4, 14 and 16)

The RCE controls who can be a QHIN. In order for a signatory to obtain QHIN status, the signatory must attest to and demonstrate that it meets the following eligibility requirements:

- Corporate Status. The signatory must be a U.S. entity and not owned or operated by any non-U.S. persons or entities. Foreign corporations are not eligible for QHIN designation at this time.

- Exchange Content. The signatory must be able to exchange "Required Information." Required Information is very broadly defined and goes beyond what would be maintained in a health care provider's or health plan's HIPAA Designated Record Sets (DRS).[7] Required Information is defined as "[e]lectronic information maintained by any QHIN, Participant, or Subparticipant prior to or during the term of the applicable Framework Agreement: (i) that would be ePHI [Electronic Protected Health Information] if maintained by a Covered Entity or a Business Associate; and (ii) regardless of whether the information is or has already been transmitted via QHIN-to-QHIN exchange. Notwithstanding the foregoing, the following types of information are not Required Information: (a) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or (b) [HIPAA P]sychotherapy [N]otes (as defined at 45 CFR 164.501)."[8]

  The RCE will release a future SOP that specifies the means for demonstrating satisfaction of this requirement.

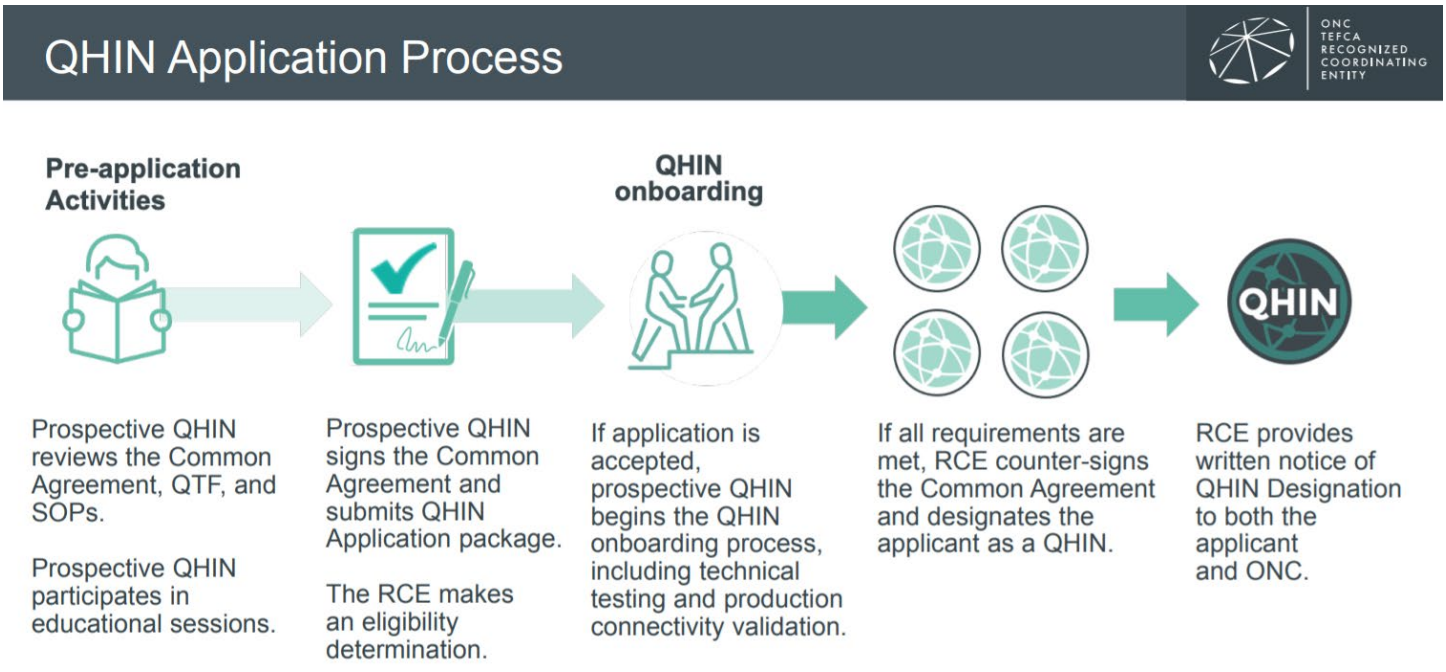
- Exchange Manner. The signatory must demonstrate that it can meet all required functions of a QHIN under the Common Agreement, the SOPs, the QHIN Technical Framework, and all other applicable guidance. RCE expects to evaluate this by requiring an applicant to demonstrate query functionality (or other functional comparable exchange method) for at least 12 calendar months. The RCE also has discretion to grant provisional status for an organization that cannot demonstrate 12 months of query-based activity, such as an applicant that supports "push" transactions but has less developed query (or "pull") functionality. The RCE has thus far declined to specify the amount (or range) of exchange transactions that must be demonstrated over that 12-month period.

- Legal and Governing Infrastructure. ***At the time of application,*** the signatory must have the organizational infrastructure, legal authority and functioning governing structure for its health information network. QHINs must contractually flow down a number of TEFCA requirements to its Participants, which are described in great detail below in Section 2. Participants and Subparticipants: Flow-Down Requirements (Throughout).

- Resources. ***At the time of application***, the signatory must demonstrate the technical and financial resources to support a reliable and trusted network. The means of demonstrating satisfaction of this requirement will be set forth in a future Onboarding & Designation SOP.

Signatories that the RCE designates as QHINs will be required to provide ongoing and extensive metrics to the RCE for the RCE to monitor performance. These metrics are expected to be set out in greater detail in a future SOP. Section 16 of the Common Agreement further specifies the circumstances under which the Common Agreement may terminate, as well as RCE and QHIN suspension rights, and RCE selection and transition services. Section 14 also sets forth specific QHIN obligations, including requirements for: (1) transparency (*e.g.*, providing copies of the Participant-QHIN agreement under certain circumstances); (2) compliance with SOPs; (3) incorporation of required Flow-Downs into Participant-QHIN agreements and Participant-Subparticipant agreements; and (4) compliance with the QTF.

The RCE has stated that it "will conduct extensive education for candidate QHINs on the application and onboarding process,"[9] including a dedicated webinar on this topic, which will be scheduled at a future date. The QHIN application process will be entirely electronic. The RCE has published the following graphic to describe the process:[10]

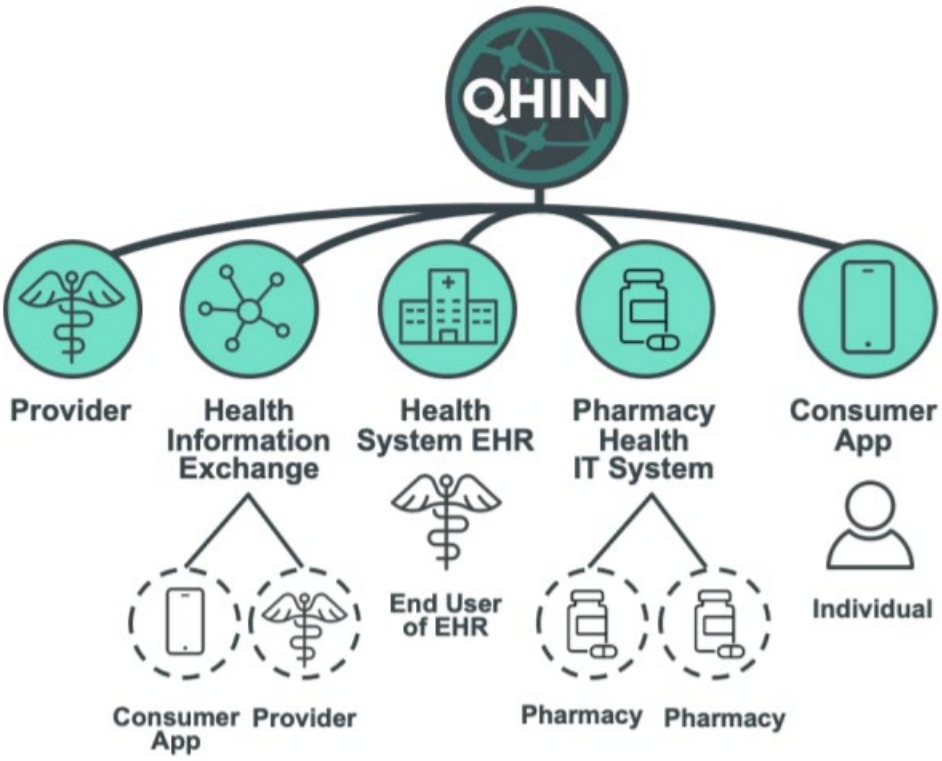


Interested applicants can learn more about the application process on the RCE website.

The RCE has also declined to specify the target number (or range) of QHINs it anticipates will be approved this year. The RCE stated on its January 26, 2022 webinar that it will be "a minimum of two, [but] less than a hundred."[11] Based on the Governance structure set forth in the Common Agreement and relevant SOPs, it seems likely that the RCE is expecting to approve approximately ten (10) QHINs during the first round of approvals.

2. Participants and Subparticipants: Flow-Downs (Throughout)

The RCE expects the following types of organizations to participate in TEFCA as Participants that directly contract with a QHIN: health care providers; HIEs; health system electronic health record (EHR) vendors; pharmacy health IT systems; and consumer applications. The RCE further expects Subparticipants will be those organizations that contract with Participants and other Subparticipants to have access to the full TEFCA network, such as providers, consumer applications and pharmacies. The RCE created the graphic below to display the expected structure of a QHIN network:[12]



In order to participate in a TEFCA network as a Participant or Subparticipant, the Common Agreement requires QHINs (and in turn Participants) to flow down over thirty contractual requirements and obligations to Participants and Subparticipants, including the following Sections that the RCE has designated as "Required Flow-Downs:"

- 6.1 Cooperation
- 6.2.1 Prohibition Against Exclusivity
- 6.2.2 No Discriminatory Limits on Exchange of TEFCA Information
- 7.1 Confidential Information
- 8.2 Utilization of the RCE Directory Service
- 9.2 Uses
- 9.3 Disclosures
- 9.4 Responses
- 9.5 Special Legal Requirements
- 10 Individual Access Services: 7 sub-Flow-Downs
- 11.1 Compliance with the HIPAA Privacy Rule: 11 sub-Flow-Downs
- 12.1.4 Participants and Subparticipants: security requirements
- 12.2 TEFCA Information Outside the United States
- 13.1 Compliance with Applicable Law and the Framework Agreements
- 13.2.2 Responsibility of Signatory
- 13.3 Flow-Down Rights to Suspend
- 13.4 Survival for Participants and Subparticipants

There also other provisions in the Common Agreement that are not designated as Required Flow-Downs, but still require flow-down to Participants and Subparticipants. For example, Section 14.2 requires QHINs to flow down compliance with applicable SOPs to Participants.

Accordingly, organizations interested in participating in a TEFCA network at the QHIN, Participant or even Subparticipant level will likely need to amend their data sharing agreements with their Participants and Subparticipants to satisfy these Flow-Down requirements.

Interestingly, the RCE did not include a separate HIPAA Business Associate Agreement (BAA) to cover the services the RCE and/or QHINs will perform on behalf of one another in connection with locating records, patient matching, and similar activities which are necessary to facilitate nationwide data exchange, even if a QHIN's participants might not have a relationship with the individual whose information is being queried or pushed.

3. Governance and Change Management (Sections 3 and 5)

In September of 2019, ONC entered a Cooperative Agreement with the RCE to develop, implement, maintain, and update the Common Agreement. Under the Cooperative Agreement, the RCE is responsible for the

development and operation of TEFCA. The ONC provides oversight and has the right to review the RCE's conduct, including complaints made against the RCE.

Under the Common Agreement, the RCE has created a framework that will enable QHINs, Participants and Subparticipants to participate in varying levels of TEFCA governance. Specifically, the Common Agreement establishes a Transition Council and Governance Council, as well as a QHIN Caucus and Participant/Subparticipant Caucus.

The Transition Council will be comprised of QHIN representatives and Participant representatives as set forth in the Transition Council SOP, and they will serve in an interim governance capacity for one year after the RCE approves the first group of QHINs. The Governance Council will be comprised of 21 members drawn from the QHIN Caucus and Participant/Subparticipant Caucus, as set forth in the Governance Council SOP. The Transition Council and Governance Council have the following responsibilities:

- Reviewing proposed amendments to the Common Agreement, SOPs and QTF;
- Participating in the development of new SOPs and strategic roadmaps for exchange activities;
- Serving as a resource to the RCE and discussion forum;
- Providing oversight for the TEFCA dispute resolution process; and
- Advocating for the value and success of TEFCA.

The Councils may also draw upon the expertise of the QHIN Caucus, Participant/Subparticipant Caucus and Advisory Groups—all of which are mechanisms by which stakeholders can participate in the governance and development of the TEFCA infrastructure.

All changes to the Common Agreement, QTF and SOPs must also be done in coordination with the RCE and ONC. **The ONC must approve all changes, additions and deletions.** The approval process for amendments to the Common Agreement and QTF is set forth in Section 5.2 of the Common Agreement. The process for changes to the SOPs is set forth in Section 5.3.

4. Requirement of Cooperation and Non-Discrimination (Section 6)

The Common Agreement imposes robust cooperation and non-discriminatory requirements on QHINs, Participants and Subparticipants. In its January 26, 2022 webinar, the RCE emphasized the critical importance of this requirement in the TEFCA ecosystem. QHINs, Participants and Subparticipants are expected to:

- Timely respond to inquiries;
- Support the RCE in resolving issues before pursuing the dispute resolution process;
- Make reasonable efforts to notify the RCE and other QHINs of persistent and widespread connectivity failures;
- Share information regarding cyber security requests; and

- ***Not*** limit interoperability with others (*e.g.*, QHINs, Participants and Subparticipants) in a discriminatory manner. The Common Agreement defines "discriminatory manner" in Section 6.2.2 as an "action that is inconsistently taken or not taken with respect to any similarly situated QHIN, Participant, Subparticipant, Individual, or group of them, whether it is a competitor, or whether it is affiliated with or has a contractual relationship with any other entity, or in response to an event." The RCE offered this illustration: "QHIN A treats QHIN B favorably, but treats QHIN C unfavorably"—this is prohibited because QHINs "are pretty much [similarly situated]." The RCE emphasized that this is an "important concept" that has "far reaching implications" for organizations that choose to participate in TEFCA.[13]

5. Exchange Purposes and Downstream Uses (Section 9)

A critical component of the Common Agreement are the reasons for which information may be requested or shared through the TEFCA network—called an "Exchange Purpose." An "Exchange Purpose" is the reason for which information may be requested or shared on the TEFCA network. There are permitted and mandatory Exchange Purposes. The permitted Exchange Purposes are for:

- Treatment (as defined by HIPAA)
- Payment (as defined by HIPAA)
- Health Care Operations (as defined by HIPAA)
- Public Health (as described by HIPAA)
- Government Benefits Determinations (for governmental agencies to make non-health benefits determinations)
- Individual Access Services (for consumer-facing applications to assist individuals in obtaining access)

These Exchange Purposes are limited by the requirements of applicable law, as well as the privacy and security requirements set forth in the Common Agreement and any other applicable privacy and security notices.

The RCE is expected to release a SOP that will designate Treatment and Individual Access Services as mandatory Exchange Purposes. This means that when there is a request for a Treatment purpose or Individual Access Services the receiving organization at the QHIN, Participant or Subparticipant level ***must*** respond to the request with ***all*** the Required Information that they have (*e.g.*, all ePHI excluding HIPAA Psychotherapy Notes and ePHI maintained for litigation or administrative proceedings). There are two primary exceptions to the mandatory response requirement: (1) a response is not required if it is prohibited by applicable law; or (2) a response is not required if the receiving person or entity is a Public Health Authority (as defined by HIPAA), users of a Government Benefits Determination Exchange Purpose, or federal agencies to the extent that the requested disclosure is not permitted under applicable law. Importantly, failure of the requesting entity to pay for services is not grounds for denying the request under the Common Agreement.

The RCE expects to make other Exchange Purposes mandatory once technical implementation guides are developed. The RCE has not yet released a timeline for when that will occur.

These Exchange Purposes will also grow over time as the legal, technical and administrative structures mature to support additional use cases, such as research.

Additionally, the underlying administrative and technical infrastructure that will support these Exchange Purposes must be capable of capturing and transmitting information about the person or entity requesting the exchange to ensure that the person or entity is permitted under HIPAA to make that request, see the QHIN Technical Framework (QTF) section below. The example the RCE gives is that only a user designated in the system as a "Health Care Provider" (or a "Business Associate, agent, or contractor acting on that Health Care Provider's behalf") may request information for a Treatment purpose.[14]

Finally, the Common Agreement does ***not*** restrict the downstream uses of any data exchanged over a TEFCA network once it is received, with the exception of certain use restrictions imposed on non-HIPAA entities who reasonably believe the data is TEFCA Information (see Section 7 below). "TEFCA Information" or "TI" is information exchanged between QHINs for one or more of the Exchange Purposes pursuant to any of the TEFCA framework agreements. Subject to this one exception, there are generally ***no*** prohibitions on QHINs, Participants and Subparticipants retaining or subsequently using and disclosing TEFCA Information received under the laws that apply to that recipient. Thus, restrictions that might exist on the use of a data at the data supplier level—such as federal or state-based restrictions on certain uses cases (such as research) or individual privacy restrictions (such as prohibiting the disclosure of self-pay data to health plans)—might not be enforceable once that data is released through a TEFCA connection. Data suppliers to a TEFCA network should consider whether they have sufficient data segmentation and technical mechanisms in place to prevent unauthorized downstream disclosures.

6. Individual Access Services (IAS) and IAS Providers (Sections 9 and 10)

"Individual Access Services" or "IAS" is a type of Exchange Purpose that is permitted and expected to be mandatory under the Common Agreement. IAS refers to giving an individual—who has a direct relationship with a QHIN, Participant, or Subparticipant—the ability to access, inspect or obtain a copy of the individual's Required Information that is maintained by or for any QHIN, Participant or Subparticipant. **Under the anticipated SOP that will make IAS a mandatory use case, all QHINs, Participants and Subparticipants must respond to an IAS request, even if they are not an IAS Provider,** unless they are prohibited by applicable law from responding.

An IAS Provider is a QHIN, Participant or Subparticipant that offers IAS to individuals. The Common Agreement does ***not*** require that a person or entity offer IAS. However, participation in TEFCA means that a receiving person or entity must respond to an IAS request.

An IAS Provider must meet the following requirements in order to participate in a TEFCA network:

- Notice. The IAS Provider must have a written privacy and security notice. Additionally, individuals must be informed of their right to data deletion and data portability.
- Security. The IAS Provider must protect all of the individual's identifiable information (not just TEFCA Information) in accordance with TEFCA security requirements, including encryption (in transit and at rest). An IAS Provider must also notify individuals of security incidents that affect TEFCA Information.
- Consent. The IAS Provider must obtain an individual's written consent to access, exchange, use and disclose that individual's information.
- Data Deletion. The IAS Provider must provide individuals with the right to delete their information that is maintained by the IAS Provider, subject to certain exceptions.
- Data Portability. The IAS Provider must provide individuals with the right to export their data in a computable (*e.g.*, machine readable) format.
- Subcontractors. The IAS Provider must require compliance with all of the foregoing by any subcontractors or agents they engage to assist with the provision of IAS.

7. TEFCA Privacy and Security Requirements (Sections 11 and 12)

All persons and entities that exchange data in the TEFCA ecosystem must comply with HIPAA privacy and security requirements, regardless of whether they are legally subject to HIPAA. However, non-HIPAA entities (NHEs) must only comply with the HIPAA Security Rule[15] and certain provisions of the HIPAA Privacy Rule[16] with respect to individually identifiable information that they reasonably believe is TEFCA Information. However, this requirement does not extend to non-HIPAA entities acting as an entity entitled to make a Government Benefits Determination, a Public Health Authority, or a Government Health Care Entity.

Additionally, TEFCA's security requirements for QHINs go beyond the minimum standards required by the HIPAA Security Rule. Specifically, TEFCA requires that all QHINs must:

- Obtain third-party certification that they meet industry-recognized cyber security standards;
- Perform annual security assessments;
- Have a Chief Information Security Officer; and
- Have cyber risk insurance coverage. The Common Agreement does not specify insurance coverage limits.

All QHINs, Participants and Subparticipants must also agree to:

- Give notice of "TEFCA Security Incidents"[17] involving or affecting exchange, including other security events set forth in a SOP. The Common Agreement requires reporting within five business days of determining that a TEFCA Security Incident has occurred; and
- Evaluate the risks of any uses and disclosures of TEFCA Information outside of the United States to determine whether they satisfy the HIPAA Security Rule.

The RCE will establish a Cybersecurity Council to support compliance with these security requirements.

8. TEFCA Fee Schedule and QHIN Fees (Section 17)

The RCE is not currently imposing any fees on organizations interested in applying for QHIN status or TEFCA participation. However, the RCE will charge fees in the future. The Common Agreement specifically provides that the signatory will pay the fees set forth on a future Schedule 1 (QHIN Fees). The RCE reports that it is unaware of any federal funding that will be made available to support the QHIN infrastructure at this time, and thus anticipates eventually imposing an application fee, annual fee and ongoing testing fees. The RCE is also considering charging fees for application preparation services and educational sessions. Importantly, the Common Agreement exempts changes to Schedule 1 from the Change Management process (*e.g.*, voting and approval) and entitles the RCE to unilaterally impose fees with 90 days' advance written notice.

The Common Agreement is largely silent on how QHINs, Participants and Subparticipants finance their own internal networks that connect to the TEFCA infrastructure and whether they charge fees for additional services. However, the Common Agreement ***prohibits*** a QHIN from charging fees to another QHIN. This means that QHINs cannot charge other QHINs fees on a transaction basis. Additionally, QHINs, Participants and Subparticipants must all comply with applicable laws that might impact whether fees are charged and the amount, such as the ONC Information Blocking Rule and HIPAA prohibited fees.

9. Other Important Business Terms (Sections 7, 13, 15 and 18)

The Common Agreement also contains important provisions regarding the protection of confidential information (other than ePHI), liability, disputes and other miscellaneous terms. For example:

- Responsibility. The Common Agreement does not contain any indemnification protection for QHINs. Rather, the RCE employs a responsibility (aka accountability) clause that requires signatories (*e.g.*, QHINs) to be responsible for their acts and omissions as well as the acts and omissions of their Participants and Subparticipants, but without any duty to hold harmless or defend. Specifically, signatories are responsible for harms suffered by the RCE or other QHINs to the extent the harm was caused by the signatory's breach of the Common Agreement or any SOP. Government agencies protected by sovereign immunity are not subject to this responsibility clause. Additionally, signatories must agree to ***not*** hold the RCE (or anyone acting on the RCE's behalf) liable for any harms, except to the extent the harm is a direct result of the RCE's breach of the Common Agreement.

- Monetary Cap. The RCE's and signatory's liability under the Common Agreement is capped at $2 million per incident and $5 million aggregate or as otherwise specified in a SOP. This monetary cap is not applicable to governmental agencies that are prohibited from limiting liability.

- Dispute Resolution. Signatories agree to submit disputes to the RCE for non-binding resolution. The RCE has no power to impose monetary damages. Disputes involving the RCE may be submitted to the ONC. The dispute resolution process is set forth in greater detail in a SOP.

- Governing Law and Venue. In the event of legal proceedings, signatories must agree to exclusive jurisdiction of a state or federal court in Virginia that is within 25 miles of Alexandria, Virginia. That court's conflict of laws provision will determine what governing law will apply.

Standard Operating Procedures (SOPs)

The SOPs are written procedures that provide detailed information or requirements regarding TEFCA data exchange. The SOPs are incorporated by reference into the Common Agreement. SOPs are effective when adopted pursuant to Section 5.3 of the Common Agreement and listed on a public website.
Thus far the RCE has released SOPs on the following topics:

- Advisory Groups
- Conflicts of Interest
- Dispute Resolution
- TEFCA Governing Council
- QHIN Cybersecurity Coverage
- QHIN Security Requirements for the Protection of TEFCA Information
- Transition Council

The RCE also plans to release at a future date SOPs on:

- Onboarding & Designation
- Required Information
- Treatment (Required Exchange Purpose)
- IAS (Required Exchange Purpose)

SOPs can be accessed on the RCE's Common Agreement Resource page.

QHIN Technical Framework (QTF)

The QTF v1 sets out the technical requirements a HIN must fulfill to serve as a QHIN. For example, QHINs must be capable of supporting the following two exchange modalities: (1) QHIN Query (*i.e.*, a data pull / request from one or more QHINs); and (2) QHIN Message Delivery (*i.e.*, a data push to one or more QHINs).

Additionally, under the final QTF v1, QHINs must be technically capable of the following:

- When initiating a QHIN Query or QHIN Message Delivery, a QHIN ***must*** transmit the Exchange Purpose as identified by the staff or users at the QHIN, Participant, or Subparticipant requesting the use of the TEFCA network. Thus, in order to participate in the TEFCA ecosystem, the technical systems used must—at the QHIN, Participant and Subparticipant levels—have the ability to capture the reason for the data exchange.

- When initiating a QHIN Query or QHIN Message Delivery, a QHIN ***must*** also verify the query source's asserted Exchange Purpose against those listed for the query source in the RCE directory service. Indeed, QHINs are required to create directory entries for each individual facility within a Participant's or Subparticipant's organization that includes all intended Exchange Purpose codes a Participant or Subparticipant will use for all initiated transactions (*i.e.*, Treatment, Payment, Health Care Operations, Public Health, IAS or Government Benefits Determinations). This means that participants in the TEFCA ecosystem must have at least administrative (if not technical) processes in place to capture and document at a facility level Participants' and Subparticipants' role-based access status/authority (*e.g.*, heath care provider, payer, public health authority, IAS Provider, *etc.*).

A detailed summary of the QTF is beyond the scope of this briefing and the expertise of the author.

FHIR® Roadmap for TEFCA Exchange

Lastly, ONC and the RCE have published a three-year roadmap for FHIR® readiness. FHIR® (Fast Healthcare Interoperability Resources) is a technical standard describing data formats and elements (known as "resources") and an application programming interface (API) for exchanging health information between different computer systems. FHIR exchange is currently required by the CMS interoperability mandate for certain CMS-regulated payers to satisfy Patient Access API requirements. However, many healthcare organizations that are not subject to the CMS interoperability mandate have only begun the process of implementing FHIR. FHIR is not being widely used in multi-networked environments, such as HIEs. Thus, **TEFCA does not currently require FHIR for TEFCA exchanges**.

However, by 2025, the RCE expects QHINs to be able to facilitate and broker FHIR API exchange. Organizations interested in becoming or maintaining QHIN status should thus include developing FHIR capabilities in their technical roadmaps.

Want to Learn More?

If you are interested in learning more about TEFCA, please see the following resources:

- ONC, Trusted Exchange Framework (TEF): Principals for Trusted Exchange (January 2022)
- ONC, Common Agreement for Nationwide Health Information Interoperability (v1) (January 2022)
- ONC, Qualified Health Information Network (QHIN) Technical Framework (QTF) (v1) (January 2022)
- FHIR® Roadmap for TEFCA Exchange (January 2022)
- ONC, 3…2…1…TEFCA is Go For Launch
- Sequoia Project, TEFCA and RCE Resources, Common Agreement Resources
- Sequoia Project, Frequently Asked Questions

About Coppersmith Brockelman and the Author

Coppersmith Brockelman works with health information exchanges, health care providers, health plans and vendors on a wide range of interoperability and health information privacy mandates and efforts, including TEFCA developments and compliance with the ONC Information Blocking Rule, CMS interoperability mandates, HIPAA, 42 C.F.R. Part 2 and other state and federal privacy and security laws. Please do not hesitate to contact us for assistance with this new and developing area.

Melissa Soliz is a leader in compliance with data privacy and access laws (such as HIPAA, 42 C.F.R. Part 2, the ONC Information Blocking Rule, the CMS Interoperability and Patient Access Final Rule, and state laws), health information exchange (HIE), behavioral health/substance use disorder law issues, data breaches and OCR investigations, as well as clinical research compliance and contracting. Melissa regularly speaks in local and national forums on these topics and has been active in state and federal policy making on data privacy and health information exchange issues.

By the way, you know the Coppersmith Briefs are not legal advice, right? Right!
Check with your attorney for legal advice applicable to your situation.

ENDNOTES

[1] 21st Century Cures Act, Pub. L. No. 114-255, § 4003 (2016) (codified at 42 U.S.C. § 300jj-11(c)).
[2] ONC, TEFCA (last reviewed on January 18, 2022) (see historical documents).
[3] 42 U.S.C. § 300jj-52 and 45 C.F.R. Part 171 (collectively, the "ONC Information Blocking Rule").
[4] 85 Fed. Reg. 25510 (May 1, 2020).
[5] Sequoia Project, User's Guide to the Trusted Exchange Framework and Common Agreement – TEFCA (Jan. 2022), at slide 62.
[6] Sequoia Project, User's Guide to the Trusted Exchange Framework and Common Agreement – TEFCA (Jan. 2022), at slide 12.
[7] "Designated record set means: (1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity." 45 C.F.R. § 164.501.
[8] Common Agreement v1, § 1.1.
[9] Sequoia Project, Webinar: Common Agreement Overview (Jan. 26, 2022).
[10] Sequoia Project, User's Guide to the Trusted Exchange Framework and Common Agreement – TEFCA (Jan. 2022), at slide 60.
[11] Sequoia Project, Webinar: Common Agreement Overview (Jan. 26, 2022), at 2:01:26.
[12] Sequoia Project, User's Guide to the Trusted Exchange Framework and Common Agreement – TEFCA (Jan. 2022), at slide 16.
[13] Sequoia Project, Webinar: Common Agreement Overview (Jan. 26, 2022), at 52:00.
[14] Sequoia Project, Webinar: Common Agreement Overview (Jan. 26, 2022), at 1:03:25.
[15] 45 C.F.R. Part 164, Subpart C.
[16] 45 C.F.R. Part 164, Subpart E.

[17] A "TEFCA Security Incident" is defined as: "(i) An unauthorized acquisition, access, Disclosure, or Use of unencrypted [TEFCA Information ("TI")] in transit using the Connectivity Services or pursuant to any Framework Agreement between Signatory and its Participants, between Signatory's Participants and their Subparticipants, or between Subparticipants, but NOT including the following:
(a) Any unintentional acquisition, access, or Use of TI by a workforce member or person acting under the authority of a QHIN, Participant, or Subparticipant, if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under Applicable Law and this Common Agreement.
(b) Any inadvertent Disclosure by a person who is authorized to access TI at a QHIN, Participant, or Subparticipant to another person authorized to access TI at the same QHIN, Participant, or Subparticipant, or Organized Health Care Arrangement in which a QHIN, Participant, or Subparticipant participates or serves as a Business Associate, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under Applicable Law and this Common Agreement.
(c) A Disclosure of TI where a QHIN, Participant, or Subparticipant has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.
(d) A Disclosure of TI that has been de-identified in accordance with the standard at 45 CFR § 164.514(a).
(ii) Other security events (*e.g.*, ransomware attacks), as set forth in an SOP, that prevent the affected QHIN, Participant, or Subparticipant from responding to requests for information as required under this Common Agreement or otherwise adversely affect their participation in QHIN-to-QHIN exchange." Common Agreement v1, § 1.1.