BACKROUND ON TEFCA AND CYBER-FOCUSED COMPONENTS
February 2024

Background

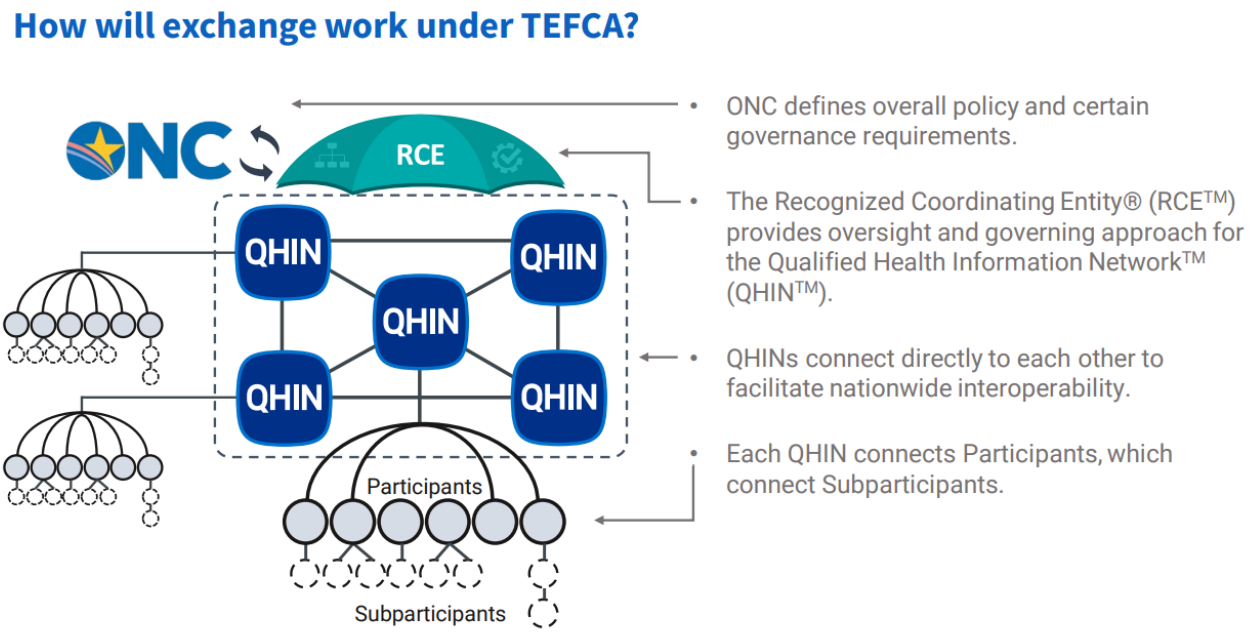
The 21st Century Cures Act signed into law in 2016, established the Trusted Exchange Framework under Section 4003(b) [Adobe page 133] (**See Appendix A**) intended to facilitate. There are two central documents associated with this effort:

1. The Trusted Exchange Framework (TEF), which describes high-level principles that networks should adhere to for trusted exchange; and
2. The Common Agreement (CA), which is a legal agreement that will enable network-to-network data sharing.

Together these documents comprise the Trusted Exchange Framework and Common Agreement (TEFCA) intended to establish a universal floor for interoperability across the country. In addition to the two aforementioned documents, there are several accompanying technical and governing documents including some specific to security.

The Trusted Exchange Framework

The TEF is a common set of principles designed to facilitate trust between HINs. The HINs voluntarily choose to participate and abide by these principles to enable widespread information exchange. These principles are standardization; openness and transparency; cooperation and non-discrimination; **privacy and security;** safety; access; equity; and public health.



Recognized Coordinating Entity (RCE)

The Sequoia Project has been selected by the Office of the National Coordinator for Health Information Technology (ONC) to serve as the **Recognized Coordinating Entity (RCE)**. The RCE's role is to develop, implement, maintain, and update the CA, In addition to the CA, the RCE collaborates with ONC to designate and monitor Qualified Health Information Networks (QHINs), modify and update an accompanying QHIN Technical Framework, engage with stakeholders through virtual public listening sessions, adjudicate noncompliance with the CA, and propose sustainability strategies to support TEFCA beyond the cooperative agreement's period of performance.

Qualified Health Information Networks (QHINs)

A QHIN is a HIN that has been designated by the RCE and is a party to the CA countersigned by the RCE. Thus far, ONC has designated seven QHINs. They include: eHealth Exchange; Epic Nexus; Health Gorilla; KONZA; MedAllies; CommonWell Health Alliance; and Kno2.

The Common Agreement

The CA is the legal contract that the RCE (Sequoia) will sign with each QHIN. It defines legal and technical requirements for secure information sharing on a nationwide scale. It also establishes the infrastructure model and governing approach to enable users in different HINs to securely share information with each other. The current version of the CA is the Common Agreement for Nationwide Health Information Interoperability Version 1.1 (59 pages).

Main sections of the CA that address privacy and security include:

- **Section 1.** Among the terms defined are "TEFCA Security Incident and "Threat Condition." See Appendix B for definitions.
- **Section 10.** Individual Access Services (Required Flow-Downs, if Offering Individual Access Services (starting page 31)
- **Section 11.** Privacy (starting page 36)
- **Section 12.** Security (starting page 39) which includes a section requiring signatories to obtain third-party cybersecurity certification (12.1.2) and annual risk assessments (12.2.3) among other things.

There are plans to update the CA to Version 2 by March. The draft version can be found here. Draft changes related to security matters as proposed include:

- An addition of a definition of "Breach of Unencrypted Individually Identifiable Information";
- Changes to the definition of TEFCA Security Incident(s) to remove language "in transit" related to an unauthorized acquisition, access, Disclosure, or Use of unencrypted TI;
- Removal of language in Section 3.2 related to Participation in Governance specific to roles which includes removal of language indicating the Governing Council supporting the RCE in evaluation of security incidents; and
- Changes to the definition of Threat Condition to add into subsection (iii) language that includes the RCE as among the entities listed and a new subsection (iv) that adds "any event that could pose a risk to the interests of national security as directed by an agency of the United States government."

QHIN Technical Framework (QTF)

The Qualified Health Information Network(QHIN) Technical Framework (QTF) is 36-page document and it focuses on the technical components for exchange among QHINs, including patient identity resolution, authentication, and performance measurement. The QTF requirements are incorporated by reference into the CA.

According to the QTF, "Protecting the privacy and security of health information 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." According to the QTF, the "Initiating QHIN connects to each Responding QHIN using the Internet Engineering Task Force (IETF) Transport Layer Security (TLS) protocol to establish a secure channel for the QHIN Query transaction; each QHIN authenticates the other QHIN (i.e., mutual authentication)."

As with the CA, there are plans to update the QTF to Version 2 in March. The draft version can be found here. The draft document is longer than the original and security-related changes include:

- Adding requirements for Facilitated FHIR exchange between QHINs, Participants, and Subparticipants including the use of the FHIR Provenance resource to track data transformation to and from FHIR resources and the HL7® FAST UDAP Security Implementation Guide;
- Changes to "Error Handing" to include changes that allow QHINs, Participants and Subparticipants to elect to obscure some of Operation Outcome details for security reasons; and
- Addition of security-focused constraints related to OATH 2.0 to further enable interoperability without reducing the security of transactions.

QHIN Cybersecurity Certification

Last updated in 2022, this seven-page document, the Standard Operating Procedure (SOP): QHIN Security Requirements for the Protection of TI, identifies specific requirements that QHINs must follow to protect the security of TEFCA Information (TI) including provisions related to annual security risk assessments and a requirement that the RCE shall designate a person to serve as the Chief Information Security Officer (CISO) for activities conducted under the Framework Agreements. It also requires QHINs to protect the security of TI. And, it provides specific information about the Cybersecurity Council, as discussed further below.

Cybersecurity Coverage

Section 12.1.1 of the CA, "Cybersecurity Coverage," dictates that, "In accordance with the Cybersecurity Coverage SOP, Signatory shall maintain, throughout the term of this Common Agreement: (i) a policy or policies of insurance for cyber risk and technology errors and omissions; (ii) internal financial reserves to self-insure against a cyber-incident; or (iii) some combination of (i) and (ii)."

Cybersecurity Council

The Cybersecurity Council is required to be established by the RCE (Sequoia) to enhance cybersecurity commensurate with the risks to QHIN-to-QHIN exchange, as more fully set forth in an SOP (part of the CA).

According to Section 3.2 of the CA, QHINs, Participants, and Subparticipants shall have the opportunity to engage in governance under the CA. This will include helping the Governing Council (a governing body for activities conducted under the Framework Agreements) evaluate possible and actual TEFCA Security Incidents, other Threat Conditions, and information and/or recommendations from the Cybersecurity Council.

Where to Go for More Information

- TEFCA Overview here
- ONC Website here
- Sequoia Project (RCE) Resources can be found here
    - Includes privacy and security SOPs

APPENDIX A

Section 4003(b) Cures Act

‘‘(B) ESTABLISHING A TRUSTED EXCHANGE FRAMEWORK.—

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

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

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

‘‘(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and ‘‘(IV) a process for filing and adjudicating non-compliance with the terms of the common agreement.

‘‘(ii) TECHNICAL ASSISTANCE.—The National Coordinator, in collaboration with the National Institute of Standards and Technology, shall provide technical assistance on how to implement the trusted exchange framework and common agreement under this paragraph.

‘‘(iii) PILOT TESTING.—The National Coordinator, in consultation with the National Institute of Standards and Technology, shall provide for the pilot testing of the trusted exchange framework and common agreement established or supported under this subsection (as authorized under section 13201 of the Health Information Technology for Economic and Clinical Health Act). The National Coordinator, in consultation with the National Institute of Standards and Technology, may delegate pilot testing activities under this clause to independent entities with appropriate expertise.

‘‘(C) PUBLICATION OF A TRUSTED EXCHANGE FRAMEWORK AND COMMON AGREEMENT.—Not later than 1 year after convening stakeholders under subparagraph (A), the National Coordinator shall publish on its public Internet website, and in the Federal register, the trusted exchange framework and common agreement developed or supported under subparagraph (B). **Such trusted exchange framework and common agreement shall be published in a manner that protects proprietary and security information, including trade secrets and any other protected intellectual property.**

‘‘(D) DIRECTORY OF PARTICIPATING HEALTH INFORMATION NETWORKS.— ‘‘(i) IN GENERAL.— Not later than 2 years after convening stakeholders under subparagraph (A), and annually thereafter, the National Coordinator shall publish on its public Internet website a list of the health information networks that have adopted the common agreement and are capable of trusted exchange pursuant to the common agreement developed or supported under paragraph (B). ‘‘(ii) PROCESS.—The Secretary shall, through notice and comment rulemaking, establish a process for health information networks that voluntarily elect to adopt the trusted exchange framework and common agreement to attest to such adoption of the framework and agreement.

‘‘(E) APPLICATION OF THE TRUSTED EXCHANGE FRAME- WORK AND COMMON AGREEMENT.— As appropriate, Federal agencies contracting or entering into agreements with health information exchange networks may require that as each such network upgrades health information technology or trust and operational practices, such network may adopt, where available, the trusted exchange framework and common agreement published under subparagraph (C).

‘‘(F) RULE OF CONSTRUCTION.—

> ‘‘(i) GENERAL ADOPTION.—Nothing in this paragraph shall be construed to require a health information network to adopt the trusted exchange framework or common agreement.
>
> ‘‘(ii) ADOPTION WHEN EXCHANGE OF INFORMATION IS WITHIN NETWORK.—Nothing in this paragraph shall be construed to require a health information network to adopt the trusted exchange framework or common agreement for the exchange of electronic health information between participants of the same network.
>
> ‘‘(iii) EXISTING FRAMEWORKS AND AGREEMENTS.— The trusted exchange framework and common agreement published under subparagraph (C) shall take into account existing trusted exchange frameworks and agreements used by health information networks to avoid the disruption of existing exchanges between participants of health information networks.
>
> ‘‘(iv) APPLICATION BY FEDERAL AGENCIES.—Notwithstanding clauses (i), (ii), and (iii), Federal agencies may require the adoption of the trusted exchange framework and common agreement published under subparagraph (C) for health information exchanges contracting with or entering into agreements pursuant to subparagraph (E).
>
> **‘‘(v) CONSIDERATION OF ONGOING WORK.—In carrying out this paragraph, the Secretary shall ensure the consideration of activities carried out by public and private organizations related to exchange between health information exchanges to avoid duplication of efforts.’’**

APPENDIX B

TEFCA Security Incident

TEFCA Security Incident(s):

(i) An unauthorized acquisition, access, Disclosure, or Use of unencrypted 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.

Threat Condition

Threat Condition:

(i) a breach of a material provision of this Common Agreement that has not been cured within fifteen (15) days of receiving notice of the material breach (or such other period of time to which the Parties have agreed), which notice shall include such specific information about the breach that the RCE has available at the time of the notice; or

(ii) a TEFCA Security Incident; or

(iii) an event that Signatory, its Participant, or their Subparticipant has reason to believe will disrupt normal exchange under the Framework Agreements, either due to actual compromise of or the need to mitigate demonstrated vulnerabilities in systems or data of the QHIN, Participant, or Subparticipant, as applicable, or could be replicated in the systems, networks, applications, or data of another QHIN, Participant, or Subparticipant.