The Trusted Exchange Framework and Common Agreement (TEFCA)

January 2022

Background

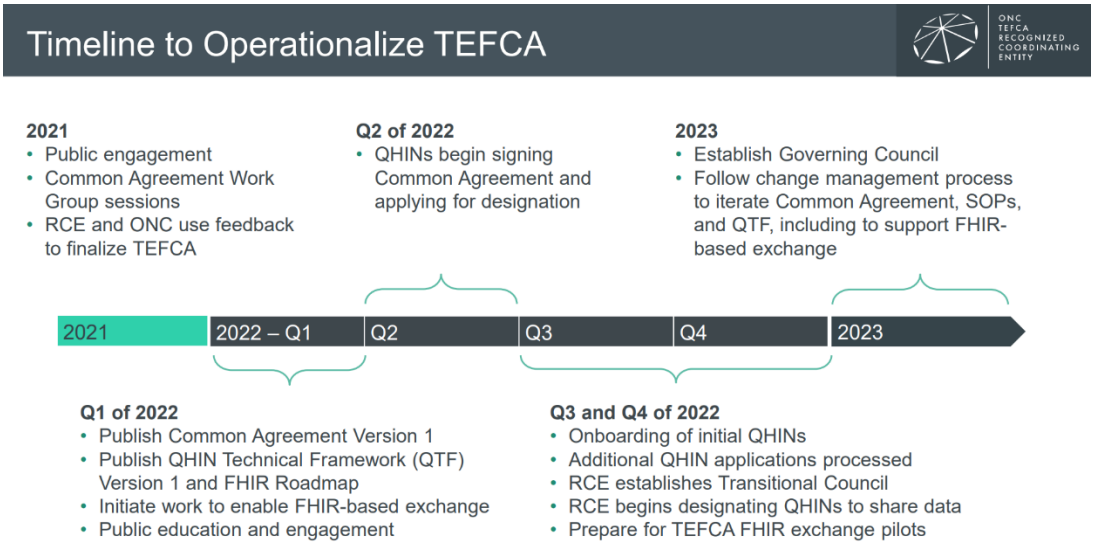
The Trusted Exchange Framework and Common Agreement (TEFCA) was finalized and released as a version 1 document by the Office of the National Coordinator for Health Information Technology (ONC) and the TEFCA's Recognized Coordinating Entity (RCE) the Sequoia Project.

Version 1 of the TEFCA consists of the Trusted Exchange Framework (TEF): Principles for Trusted Exchange and Common Agreement. The TEF is a set of non-binding principles to facilitate data-sharing among health information networks, while the Common Agreement is a legal contract that the RCE will sign with each Qualified Health Information Network (QHIN).

QHINs serves as a de-facto nodes, that facilitate connections to the TEFCA itself. Full eligibility and the application process for organizations to apply to be QHINs will be released in Q2, 2022. All QHINs will be required to follow the QHIN Technical Framework (QTF) that was also finalized along with the TEFCA FHIR Roadmap for implementation of FHIR into the TEFCA overtime.

Trusted Exchange Framework (TEF): Principles for Trusted Exchange

The Trusted Exchange Framework (TEF): Principles for Trusted Exchange is a non-binding set of foundational principles for trust policies and practices that can help facilitate exchange among health information networks (HINs). Patients, their healthcare providers, and other authorized health care stakeholders can use the TEF to facilitate electronic access to their digital health information.



Principles within the TEFCA include:

1. Standardization: HINs should prioritize federally recognized and industry recognized technical standards, policies, best practices, and procedures;
2. Openness and Transparency: HINs should conduct activities openly and transparently, wherever possible;
3. 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;
4. 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;
5. 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;
6. Equity: HINs should consider the impacts of interoperability on different populations and throughout the lifecycle of the activity;
7. 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.

Other Key Provisions:

- HINs should ensure that digital health information is exchanged and used in a manner that promotes safe care and wellness, including consistently and accurately matching digital health information to an individual.
    - To support accurate matching HINs should agree upon and consistently share a core set of demographic data each time digital health information is exchanged.
- HINs should employ a health equity by design approach and should consider the health equity consequences of policy and technology choices up front.
    - A health equity by design approach means HINs should identify the health equity considerations at the outset of any policy creation, technology development process, or implementation approach, and should include those as core constructs to identify and address health inequities and disparities.

Common Agreement for Nationwide Health Information Interoperability

The Common Agreement for Nationwide Health Information Interoperability is the conditions that an organization must agree to and sign prior to being designated a Qualified Health Information Network (QHIN). Prior to signing the Common Agreement all organizations will need to have undergone the QHIN application process.

Key Provisions:

Cybersecurity

- The RCE shall designate a person to serve as the Chief Information Security Officer (CISO) for activities conducted under the Framework Agreements.
- The RCE will establish a Cybersecurity Council to enhance cybersecurity amongst the framework with further details laid out in a to come standard operating procedure (SOP) document.
- QHINs must maintain a policy or policies of insurance for cyber risk and technology errors and omissions, internal financial reserves to self-insure against a cyber-incident, or some combination of the to.
    - SOP for QHIN Cybersecurity Coverage: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/SOP-QHIN-CyberSec-Coverage-FINAL.pdf
- QHINs shall achieve and maintain third-party certification to an industry-recognized cybersecurity framework demonstrating compliance with all relevant security controls.
    - SOP for QHIN Security Requirements for the Protection of TI: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/SOP-QHIN-Security-of-TI-FINAL.pdf
- An unauthorized acquisition, access, Disclosure or Use of unencrypted TEFCA Information (TI) in transit using the Connectivity Services or any Framework Agreement between QHINs and their participants are deemed a TEFCA Security Incident. Exceptions include, except where not permitted under law:
    - Unintentional acquisition, access or use of TI by a QHIN entity that was made in good faith and within the scope of authority and does not result in further use or disclosure;
    - Any inadvertent disclosure by a person who is authorized to access TI at a QHIN or QHIN entity to a person also authorized to access TI at the same QHIN or QHIN entity and does not result in further use or disclosure;
    - Disclosure of TI where a QHIN or QHIN entity 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; and
    - A disclosure of TI that has been de-identified in accordance with government standards.
- Other security events – such as ransomware attacks – as set forth in an SOP, that prevent the affected QHIN, or QHIN entity, from responding to requests for information as required under the Common Agreement or otherwise adversely affect the participation in QHIN-to-QHIN exchange will be deemed a security incident.

    - SOP for QHIN Security Requirements for the Protection of TI: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/SOP-QHIN-Security-of-TI-FINAL.pdf
    - SOP for QHIN Cybersecurity Coverage: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/SOP-QHIN-CyberSec-Coverage-FINAL.pdf
- QHINs must provide information to aid the efforts of other QHINs or their respective participants to understand, contain and mitigate a TEFCA Security Incident at the request of other QHINs.
- QHINs much notify each individual whose TI has been or is reasonably believed to have been affected by a TEFCA Security Incident involving an IAS provider.
    - Notification much be made no later than 60 days after the discovery of the TEFCA Security Incident.
- QHINs must notify the RCE and all likely impacted QHINs of a TEFCA Security Incident no more than five days after it has been determined an incident occurred.
    - QHINs must also implement a reporting protocol by which other QHINs can provide notification of a security incident.

Fees

- QHINs shall pay the fees attached to the Common Agreement and invoices are due and payable by the QHIN within 60 days after receipt of the invoice.
- QHINs are prohibited from charging fees to other QHINs for any exchange of information using Connectivity Services within the TEFCA.

Individual Access Services (IAS)

- Each QHIN will have the ability to provide individual access services (IAS) to an individual with whom the QHIN, Participating and Subparticipant has a Direct Relationship to satisfy that individuals ability to access, inspect, or obtain a copy of that Individual's Required Information that is maintained by or for any QHIN, Participant, or Subparticipant.

TEFCA Exchange Activities

- A QHIN, Participant or Subparticipant may only Request information under the applicable Framework Agreement for a specific Exchange Purpose if the QHIN, Participant, or Subparticipant is the type of person or entity that has the defined right to request such information.
    - A QHIN must support all Exchange Purposes and must Respond to all Exchange Purposes identified as "required" in the forthcoming Exchange Purposes SOP.
- QHINs are prohibited from engaging in QHIN-to-QHIN exchange for any purpose other than an Exchange Purpose under the Common Agreement.

    - Exceptions include other activities or reasons for which Participants and Subparticipants may request and exchange information within their networks and/or subject to other agreements.
- The Common Agreement does not supersede any state or applicable law related to privacy, access or exchange.
- QHINs must develop, implement, make publicly available and act in accordance with a written privacy policy describing its privacy practices with respect to Individually Identifiable Information that is Used or Disclosed under the Common Agreement.

TEFCA Governance

- QHINs, Participants, and Subparticipants shall have the opportunity to engaged in governance under the Common Agreement through a Transitional Council and then a Governing Council.
    - The Transitional Council will serve for a 12-month term beginning 30 days after the RCE announces the first group of QHINs designated by the RCE.
    - At the end of the 12-months following the formation of the Transitional Council, the Governing Council shall assume responsibility for participating in the governance of the exchange and related activities under the common agreement.
    - Further information on the Transitional Council is contained in the SOP for Transitional Council: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/SOP-Transitional-Council-FINAL.pdf
- The QHIN Governing Council will be established through election of individual members by each of the QHIN causes.
    - The election process and constitution is further defined in the SOP for TEFCA Governing Council: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/SOP-Governing-Council-FINAL.pdf

Additional Resources:

- Trusted Exchange Framework: Principles of Trusted Exchange: https://www.healthit.gov/sites/default/files/page/2022-01/Trusted_Exchange_Framework_0122.pdf
- Common Agreement for Nationwide Health Information Interoperability: https://www.healthit.gov/sites/default/files/page/2022-01/Common_Agreement_for_Nationwide_Health_Information_Interoperability_Version_1.pdf
- Qualified Health Information Network (QHIN) Technical Framework (QTF): https://rce.sequoiaproject.org/wp-content/uploads/2022/01/QTF_0122.pdf
- FHIR Roadmap for TEFCA Exchange: https://rce.sequoiaproject.org/wp-content/uploads/2022/01/FHIR-Roadmap-v1.0_updated.pdf
- RCE Developed TEFCA Resources: https://rce.sequoiaproject.org/tefca-and-rce-resources/