ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

November 19, 2024

RCE™ Monthly Information Call

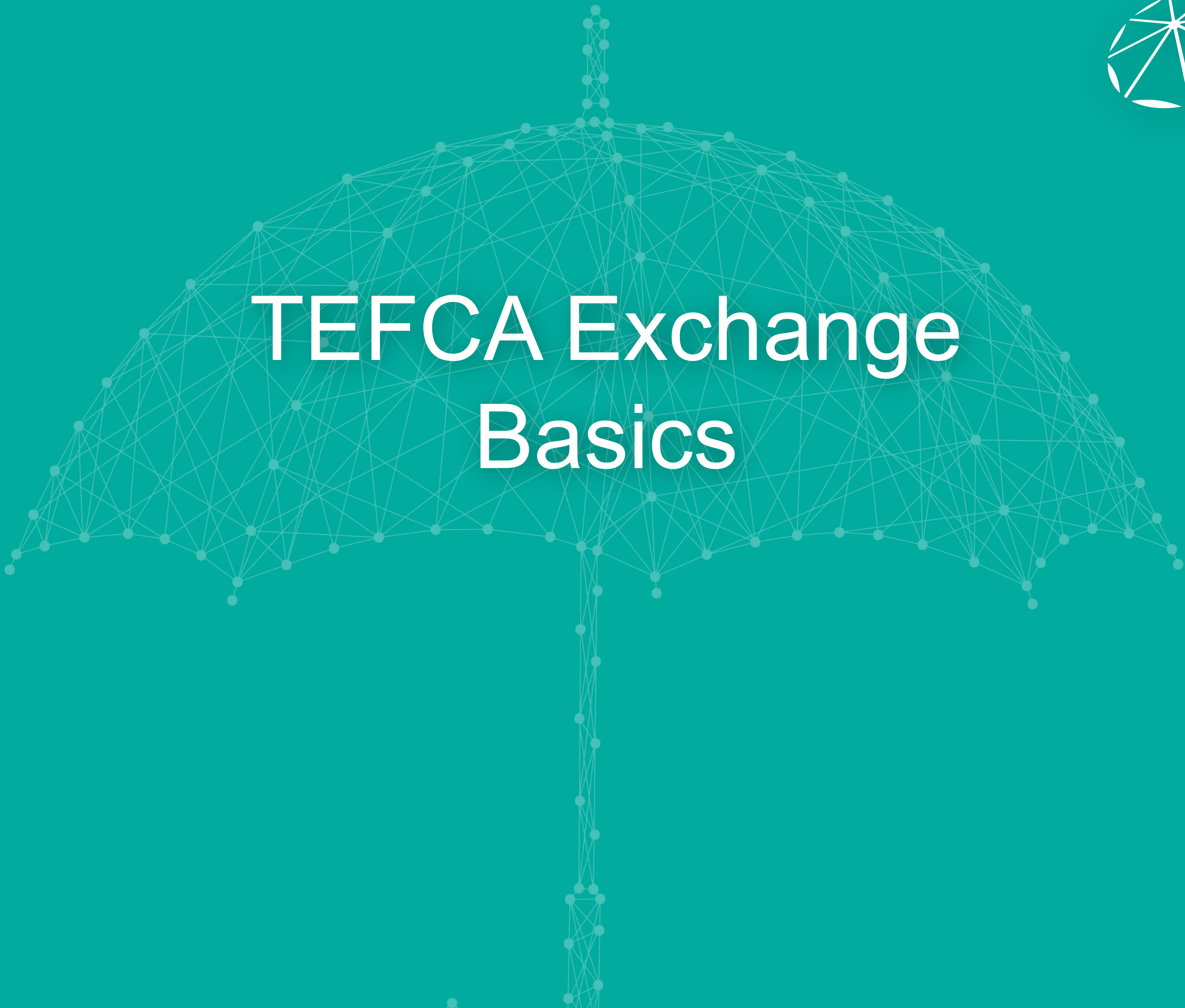
Zoe Barber, RCE Policy Director
Johnathan Coleman, RCE CISO
Didi Davis, RCE Conformance Testing
Dawn Van Dyke, RCE Communications Lead
Lindsey Elkind, RCE Legal SME
Kathryn Lucia, RCE Policy Analyst
Dave Pyke, RCE Technical SME
Steve “Sully” Sullivan, RCE Program Operations
Alan Swenson, RCE Program Operations Lead
Erin Whaley, RCE Legal SME
Chantal Worzala, RCE Stakeholder Engagement
Mariann Yeager, RCE Lead

Agenda

- **Welcome**
  - Remarks from ASTP
- **TEFCA™ Exchange Basics**
- **TEFCA Timeline Review**
- **XP Vetting Process SOP**
- **TEFCA Security**
  - Why it Matters
  - TEFCA Security Requirements
  - Exchange Purposes Implementation SOP: Individual Access Services (IAS)
  - QHIN Technical Framework (QTF)
  - TEFCA Security Incident Reporting
- **Educational Resources and FAQs**
- **Questions & Answers (Q&A)**

HL7® FHIR®

TEFCA is Ramping Up and Looking to the Future with FHIR!



TEFCA Exchange Basics

Participation in TEFCA is Ramping Up!

10,431 entries in the RCE Directory:

- 1,702 total organizations are live
  - 7 QHINs
  - 108 Participants
  - 1,587 Subparticipants
- 8,729 Child entries (parts of the above, not individual organizations with Framework Agreements)

Meet the Qualified Health Information Networks (QHINS)

commonwell® HEALTH ALLIANCE

eHealth Exchange™

Epic Nexus

HEALTH® GORILLA

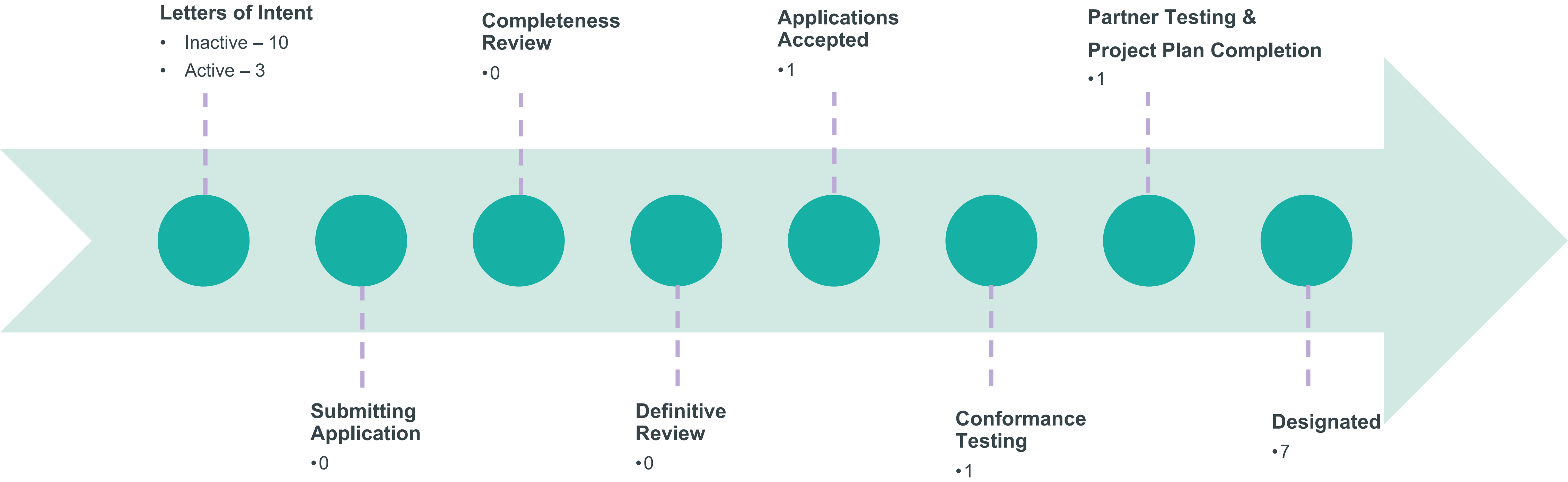
Kno2®

KONZA NATIONAL NETWORK

MedAllies

Learn More: https://rce.sequoiaproject.org/designated-qhins/

QHIN Application and Onboarding & Designation



Letters of Intent
- Inactive – 10
- Active – 3

Submitting Application
- 0

Completeness Review
- 0

Definitive Review
- 0

Applications Accepted
- 1

Conformance Testing
- 1

Partner Testing & Project Plan Completion
- 1

Designated
- 7

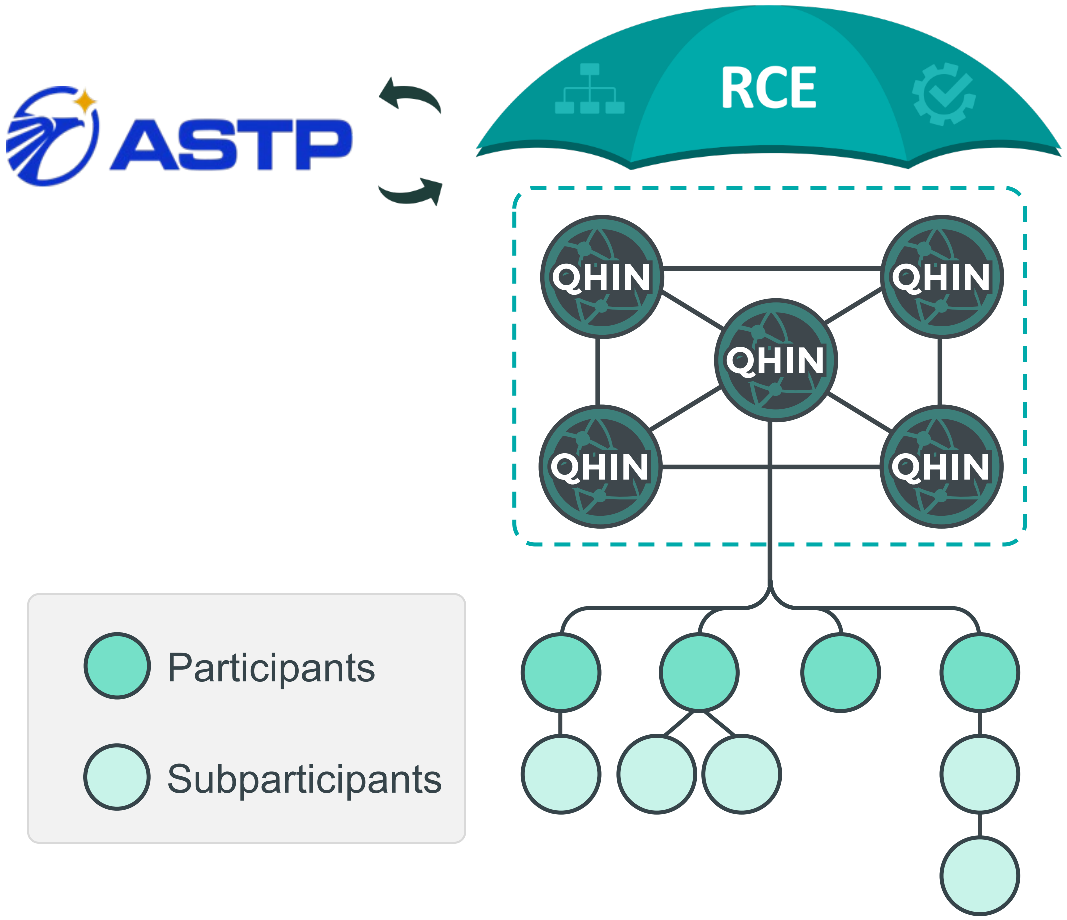
Meet The Candidate QHINs

eClinicalWorks Netsmart surescripts Health Information Network™

TEFCA Components

- Framework Agreements
- Standard Operating Procedures
- Technical Requirements
- RCE Directory
- Oversight & Compliance
- Governance

Exchange Under TEFCA



ASTP defines overall policy and certain governance requirements

RCE provides oversight and governing approach for QHINs

QHINs connect directly to each other to facilitate nationwide interoperability

Each QHIN connects Participants, which connect Subparticipants

Participants and Subparticipants connect to each other through TEFCA Exchange

- Participants contract directly with a QHIN and may choose to also provide connectivity to others (Subparticipants), creating an expanded network of networks
- Participants and Subparticipants sign the same Terms of Participation and can generally participate in TEFCA Exchange in the same manner

Framework Agreements

Framework Agreements and TEFCA connections

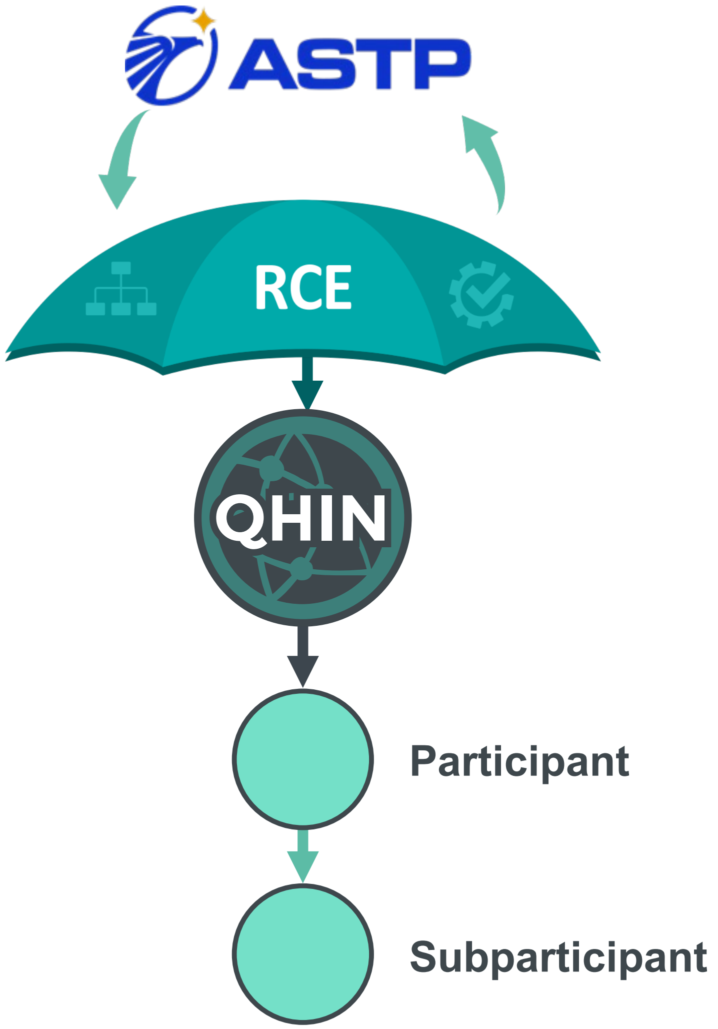
Common Agreement
Each QHIN voluntarily enters into the same contractual agreement with the RCE by signing the Common Agreement

Participant/Subparticipant Terms of Participation
All Participants and Subparticipants voluntarily agree to the Terms of Participation without modification as part of their agreements with their TEFCA connector

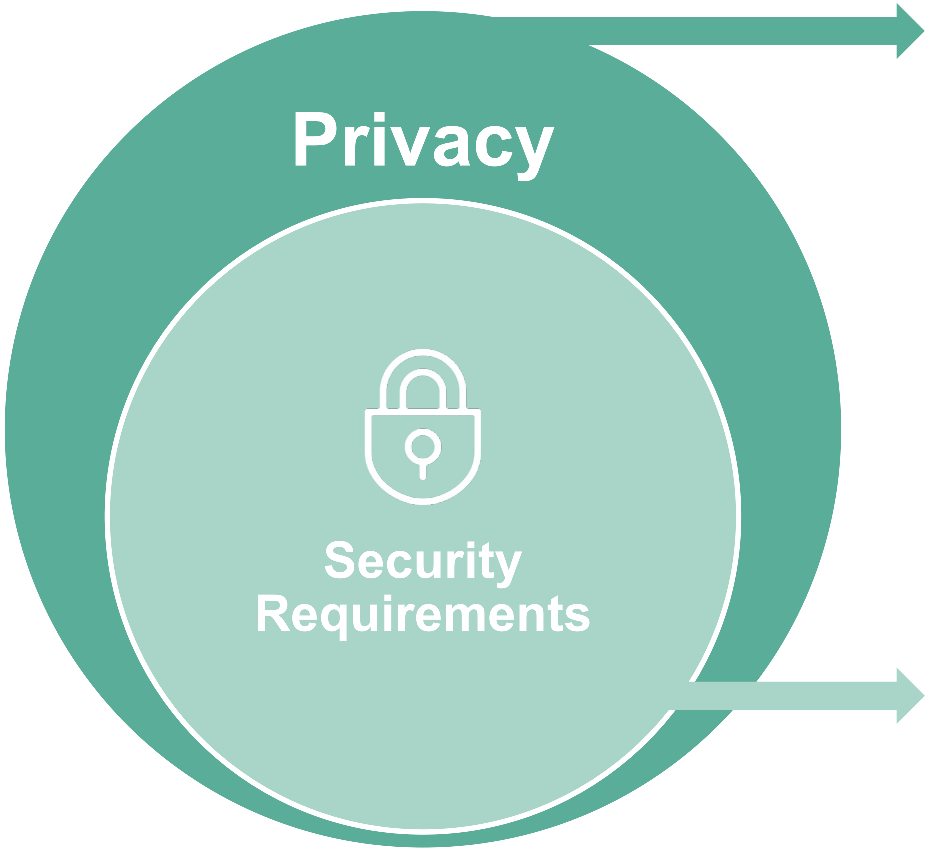
TEFCA connector
A QHIN, Participant, or Subparticipant that offers services to connect into TEFCA exchange

TEFCA connected entity
A QHIN, Participant, or Subparticipant that has signed a Framework Agreement

Entities may connect into exchange at any level



Privacy and Security



Privacy

Security Requirements

Most connected entities will likely be HIPAA Covered Entities or Business Associates of Covered Entities, and thus already be required to comply with HIPAA privacy and security requirements

Non-HIPAA Entities (NHEs) must protect Individually Identifiable Information as if it were protected health information, following HIPAA requirements, under the Common Agreement

- QHINs must meet a high bar for security (e.g., third party certification of industry-recognized cybersecurity standards, annual assessments, a Chief Information Security Officer (CISO), cyber risk coverage)
- Participants and Subparticipants, including Non-HIPAA Entities, must comply with the HIPAA Security Rule for Individually Identifiable Information
- QHINs, Participants, and Subparticipants must report TEFCA Security Incidents
- All TEFCA entities must assess the risks of using or disclosing TEFCA information outside the U.S. to ensure HIPAA Security Rule compliance, with support from the Cybersecurity Council

TEFCA Timeline Review

Expected SOP Batch Release

Published 7/1/2024

- QHIN Technical Framework (QTF) Version 2.0
- Facilitated FHIR Implementation SOP
- Individual Access Services (IAS) Provider Requirements
- Governance Approach SOP
- Delegation of Authority SOP
- Expectations for Cooperation SOP
- Exchange Purposes SOP
- RCE Directory Service Requirements Policy SOP
- Security Incident Reporting SOP
- XP Implementation SOP: Treatment

Published 8/6/24

- Public Health Exchange Purpose (XP) Implementation SOP
- Health Care Operations XP Implementation SOP
- Individual Access Services XP Implementation SOP (updated)
- Exchange Purposes (XP) SOP (updated)
- QHIN Security for the Protection of TEFCA Information (updated)

Published 11/13/24

- **XP Vetting Process SOP**

Upcoming 2024

- Participant/Subparticipant Additional Security Requirements SOP
- QHIN Onboarding & Designation SOP
- QHIN Application SOP
- Updated TEFCA Governance SOP

XP Vetting Process SOP

XP Vetting Process SOP

TEFCA RECOGNIZED COORDINATING ENTITY

NEW SOP RELEASE

Exchange Purpose (XP) Vetting Process SOP Released Today

The Sequoia Project, as the Trusted Exchange Framework and Common Agreement™ (TEFCA™) Recognized Coordinating Entity® (RCE®), today released the new Exchange Purpose (XP) Vetting Process Standard Operating Procedure (SOP).

“We’re very pleased to publish the new XP Vetting Process SOP today,” said Mariann Yeager, CEO of The Sequoia Project and RCE lead. “This important document will enhance trust in TEFCA Exchange. The SOP sets forth a structured process to evaluate entities that plan to ask for data for the TEFCA Required Treatment XP.”

This SOP was developed with significant input from the Policy and Technical Advisory Group, which includes representatives of the Qualified Health Information Networks® (QHINs™), as well as their Participants and Subparticipants, and the Assistant Secretary for Technology Policy (ASTP).

- The XP Vetting Process SOP establishes a clear and transparent framework for evaluating and approving Entrants before their inclusion in the RCE Directory Service to assert a specific Exchange Purpose (XP).
- This process promotes trust and collaboration among Qualified Health Information Networks (QHINs) by providing a structured timeline for submitting Entrants for review and discussing any concerns in an open forum.
- Thorough evaluation and transparency in the XP Vetting Process enhances the integrity and efficacy of TEFCA Exchange.

TEFCA Required Treatment means:

a) The following QHINs, Participants, or Subparticipants may initiate transactions using the TEFCA Required Treatment XP Code:

   i. Covered Entities that electronically transmit any health information in connection with transactions for which the Department of Health and Human Services (HHS) has adopted standards in the normal course of business and are one of the following types of Health Care Providers:

      1. to the extent these terms are defined in 42 USC 1395(x): a Hospital; skilled nursing facility; nursing facility; home health entity; health care clinic; community mental health center; renal dialysis facility; blood center; ambulatory surgical center; emergency medical services provider; Federally Qualified Health Center; group practice; a pharmacist; a pharmacy; a laboratory; a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization (as defined in section 1603 of title 25); or, a rural health clinic; or
      2. a natural person doctor of medicine or osteopathy, doctor of dental surgery or dental medicine, doctor of podiatric medicine, doctor of optometry, chiropractor, or other natural person who is licensed, certified, registered, or otherwise authorized by a State to provide health care, including but not limited to, a physician assistant, nurse, nurse practitioner, social worker, psychologist, registered dietician or nutrition professional, physical therapist, occupational therapist, or speech-language pathologist (collectively, “Licensed Individual Provider”).

   ii. The Veterans Health Administration, the Department of Defense, the Indian Health Service,the National Oceanic and Atmospheric Administration, the Coast Guard, and other Government Health Care Entity(ies).

   iii. Delegates of the QHINs, Participants, and Subparticipants in Section 5.3(a)(i) and 5.3(a)(ii). Notwithstanding the foregoing, a Health Plan cannot be a Delegate of any QHINs, Participants, and Subparticipants in Section 5.3(a)(i) and 5.3(a)(ii) for purposes of initiating a Query using the TEFCA Required Treatment XP Code

TEFCA Required Treatment Continued

b) The TEFCA Required Treatment XP Code can only be asserted by a QHIN, Participant, or Subparticipant set forth in Section 5.3(a) if the Query is in connection with or intended to inform health care services that an entity in Section 5.3(a) is providing or intends to provide to a patient through synchronous or asynchronous interaction (either in-person or virtual) with a Licensed Individual Provider.

   i. This includes, but is not limited to, Querying for records: upon receipt of a notification of admission to or discharge from a hospital, for medication reconciliation and medication management; in support of care management; and for identification of care gaps all for an individual patient. Queries initiated using the TEFCA Required Treatment XP Code are intended to support health care services for individual patients. If a Query is made for a similar purpose at a population level, it is for Health Care Operations.

Key Definitions

- **Entrant:** a potential Principal that may initiate Queries directly through its own Initiating Node, a shared Initiating Node, or through a Delegated Request for a specific Vetted XP and which is submitted for consideration into the Entrant Review List.
- **Objection**: a formal request sent by any QHIN to the RCE regarding an Entrant on the Entrant Review List that is intended to question the factual information about the Entrant submitted by the Sponsoring QHIN and which includes the information required by this SOP.
- **Objecting QHIN**: the QHIN that objects to an Entrant.
- **Sponsoring QHIN**: the QHIN that submits an Entrant into the Entrant Review List.
- **Vetted XP**: the XP(s) for which Entrants must be vetted in accordance with this SOP, which includes TEFCA Required Treatment.

Vetting Paths

Path 1:

- Health Care Provider that participates in any plan or program that provides health benefits, which is funded directly, in whole or in part, by the United States Government (other than the Federal Employees Health Benefits Program) or any State health care program (e.g. Medicare, Medicaid, Tricare) and has in-person, physical interactions with patients; or
- Government Health Care Entity (as defined in the Common Agreement)

Path 2:

- Health Care Provider that does not participate in any plan or program that provides health benefits, which is funded directly, in whole or in part, by the United States Government (other than the Federal Employees Health Benefits Program) or any State health care program (e.g., Medicare, Medicaid, Tricare), but does participate with other payers and has in-person, physical interactions with patients.

Path 3:

- Health Care Provider that participates with any type of payer and does not have in-person, physical interactions with patients (e.g., virtual only provider).
- Health Care Provider that does not participate with any type of payer but does conduct HIPAA standard transactions.

Types of Evidence

The vetting process requires QHINs to work with prospective Participants and Subparticipants to provide appropriate evidence that they fit the definition to request information for a given XP.

For TEFCA Required Treatment, the evidence needed varies by the vetting path, but could include one or more of the following:

- Type I data that demonstrate participation in Medicare or Medicaid
- Type II data that demonstrate the entity meets the definition as both
  - a Health Care Provider; and
  - a Covered Entity under HIPAA
- Information on the Health Care Services the entity provides
- Information on how the entity engages in Patient Interactions with Licensed Professionals

The SOP Appendices list the types of information needed by vetting path

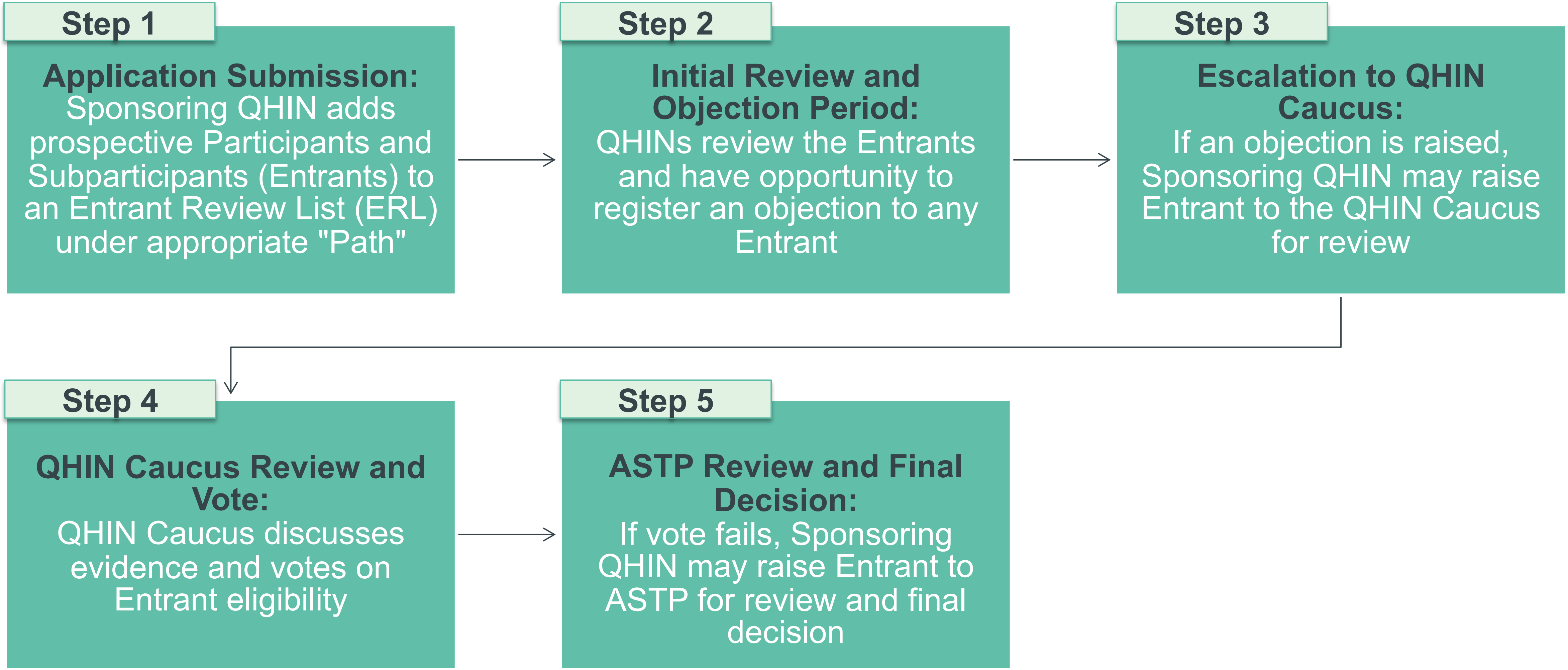
Beyond compliance with the ToP and applicable SOP(s), what additional evidence is required per pathway?

ONC TEFCA RECOGNIZED COORDINATING ENTITY

	Health Care Provider (Appendix 1)	Covered Entity (Appendix 2)	Provides Health Care Services (Appendix 3)	Interaction between LIP and Patient (Appendix 4)
Path 1	**Type I** • Link to Entrant's listing in any directory maintained by CMS • Link to Entrant's listing on any state government list of Medicaid providers • Confirmation that the Entrant is a Government Health Care Entity		No additional evidence required	
Path 2	**Type II** • Documentation reasonably showing the Entrant's receipt of payment from a payer within the six months immediately preceding publication in the Entrant Review List • Link to the Entrant's NPI listing in NPPES showing that the Entrant is the type of Health Care Provider listed in the submission • Link to the Entrant's listing on a state government website confirming it is licensed as the type of Health Care Provider listed in the submission • Copy of a Certificate of Coverage for professional medical malpractice coverage • Copy of or link to Entrant's national accreditation as a health care provider (Joint Commission, AAAHC, NCQA, URAC, etc.) • Link to the Entrant's listing of its CLIA certification on S&C QCOR • Link to the Entrant's inclusion on a list of participating providers published by a payer • Copy of a letter from a payer confirming that Entrant is a participating provider	**Type II** • Documentation reasonably showing the Entrant's submission of claims to a payer or other HIPAA standard transactions within the six months immediately preceding publication in the Entrant Review List. • Link to the Entrant's inclusion on a list of participating providers published by a payer • Copy of a letter from a payer confirming that Entrant is a participating provider	**Health Care Services Information** • Explain the ways in which the Entrant provides health care services to patients • Explain when in relation to health care services provided to patients, the Entrant will make Queries for information through TEFCA Exchange (e.g., right before a visit, at a visit, upon notification of an event, at regularly scheduled intervals, etc.). If the Queries will be automated, explain the triggers for the Queries.	Patient Interaction Attestation
Path 3	Type I or II	Type I or II	Health Care Services Information	**Patient Interaction Information** • Explain the ways in which the Entrant's Licensed Individual Providers interact with patients; and • Explain how the Queries will be connected to or intended to inform the health care services the Entrant is providing or intends to provide to a patient.

This slides provides a high level summary of evidence needs; please refer to the SOP for specific requirements.

Process Steps



Step 1

Application Submission: Sponsoring QHIN adds prospective Participants and Subparticipants (Entrants) to an Entrant Review List (ERL) under appropriate "Path"

Step 2

Initial Review and Objection Period: QHINs review the Entrants and have opportunity to register an objection to any Entrant

Step 3

Escalation to QHIN Caucus: If an objection is raised, Sponsoring QHIN may raise Entrant to the QHIN Caucus for review

Step 4

QHIN Caucus Review and Vote: QHIN Caucus discusses evidence and votes on Entrant eligibility

Step 5

ASTP Review and Final Decision: If vote fails, Sponsoring QHIN may raise Entrant to ASTP for review and final decision

TEFCA Security: Why It Matters

Changing threat landscape

- Per the Office of the Director of National Intelligence (DNI): The number of ransomware attack claims worldwide in 2023 rose 74 percent as compared with 2022. In the US, attacks against the healthcare sector were up 128 percent [1]
- Per HHS: 73% of worldwide ransomware incidents impacting healthcare affected the US Healthcare and Public Health Sector (see HHS Ransomware & Healthcare report, January 18, 2024)[2]
- Per HHS: Over the past five years (through 2023), there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware [3]

[1] https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

[2] https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf

[3] https://www.hhs.gov/about/news/2024/02/21/hhs-office-civil-rights-settles-second-ever-ransomware-cyber-attack.html

CISA's FY23 Risk and Vulnerability Assessments (RVA) Results* (released Sep. 2024)

INITIAL ACCESS

- Gaining initial access to an organization's network is one of the first active steps in a successful attack
- Preventing initial access should be a main goal in protecting network assets and data, both internally and externally
- RVA analyses revealed that Valid Accounts were the most common successful attack technique, responsible for 41% of successful attempts
- The assessments team escalated privileges using Valid Accounts in 45% of instances

LATERAL MOVEMENT

- Pivoting from host to host or from one user account to another spread the foothold
- After obtaining accounts Pass the Hash (PtH) attacks were used in 27% of instances and Pass the Ticket attacks were used in 17% of instances to laterally move through the network

MITIGATIONS AND REMEDIATIONS INCLUDE:

- Implement a secure password policy requiring phishing-resistant multifactor authentication (MFA) for remote access, strong passwords, unique credentials, and the separation of user and privileged accounts, effectively revoking unnecessary or inactive accounts

*https://www.cisa.gov/sites/default/files/2024-09/FY23_RVA_Analysis_508.pdf

Recent Threat Brief – 16 Oct 2024

Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations[1]

Joint advisory from the FBI, CISA, NSA, Canadian CSE, Australia's AFP, and Australia's ACSC

Warns of Iranian cyber actors' use of brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including the healthcare and public health (HPH), government, information technology, engineering, and energy sectors, by:

1) Gathering victim identity information (reconnaissance)

2) Gaining persistent access to victim networks, frequently via brute force techniques such as password spraying, and multifactor authentication (MFA) 'push bombing' to compromise the user accounts. They then frequently modified MFA registrations, enabling persistent access.

3) Further gathering credentials, escalating privileges, and gaining information about the entity's systems and network

4) They also move laterally and download information that could assist other actors with access and exploitation

[1] https://www.cisa.gov/sites/default/files/2024-10/aa24-290a-iranian-cyber-actors-conduct-brute-force-and-credential-access-activity.pdf

Increasing Regulatory Support for Security

- The US government has mandated the use of Multi Factor Authentication (MFA) for federal government websites and applications as part of its Cybersecurity National Action Plan and Executive Order 14028[1] (Improving the Nation's Cybersecurity)
- HTI-2: ASTP/ONC proposes to revise the MFA certification criterion in § 170.315(d)(13) and update the privacy and security certification framework in § 170.550(h) to match industry best practices for information security[3]
- HPH Cybersecurity Performance Goals[5]
- Updates to the HIPAA Security Rule anticipated

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] https://www.healthit.gov/sites/default/files/page/2024-07/HTI-2%20Overview%20PPT_508.pdf

[4] https://hhscyber.hhs.gov/performance-goals.html

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

TEFCA Security Requirements

TEFCA Cybersecurity Council

TEFCA Cybersecurity Council Members

Johnathan Coleman
RCE
Chair

Joe Granneman
Kno2
QHIN Representative

Scott Dresen
Corewell Health
Participant/Subparticipant Representative:
Epic Nexus

Christopher Wolf
Clay County Medical Center
Participant/Subparticipant Representative:
Konza

Debbie Condrey
eHealth Exchange
QHIN Representative

Emerson Bentley
Epic Nexus
QHIN Representative

Jeremy Maxwell
Veradigm
Participant/Subparticipant Representative:
MedAllies

Mark W. Dill
MedAllies
QHIN Representative

Tabrez Naqvi
Health Gorilla
QHIN Representative

Hanna Sicker
Virta Health
Participant/Subparticipant Representative:
Health Gorilla

Chuck Golliday
CommonWell
QHIN Representative

Eric Thompson
KONZA National Network
QHIN Representative

Bezawit (Bez) Sumner
CRISP Shared Services (CSS)
Participant/Subparticipant Representative:
eHealth Exchange

Non-Member Subject Matter Experts

Bob Ganim
eClinicalWorks
Candidate QHIN Representative

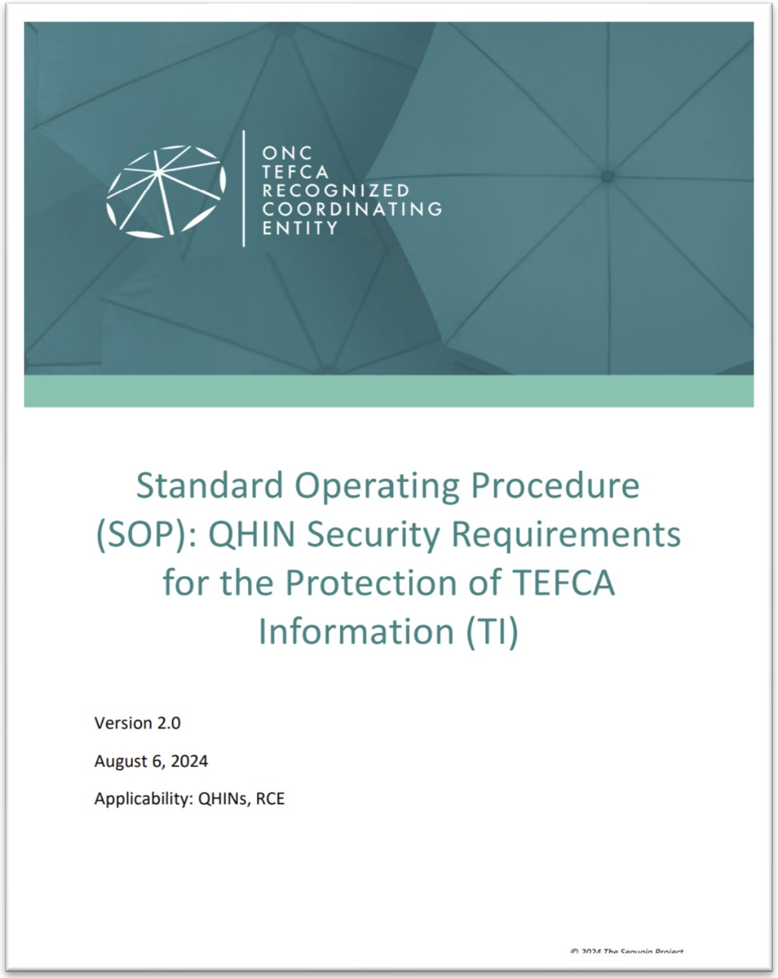
Judy Hatchett
Surscripts, LLC.
Candidate QHIN Representative

Mark Nolte
Netsmart Technologies, Inc.
Candidate QHIN Representative

The Cybersecurity Council is charged with evaluating the cybersecurity risks associated with activities conducted under the Framework Agreements and advise the RCE on ways to remediate these risks.

Security Requirements

SOP: QHIN Security Requirements for the Protection of TEFCA Information



ONC TEFCA RECOGNIZED COORDINATING ENTITY

Standard Operating Procedure (SOP): QHIN Security Requirements for the Protection of TEFCA Information (TI)

Version 2.0

August 6, 2024

Applicability: QHINs, RCE

Purpose: The SOP identifies specific requirements that QHINs must follow to protect the security of TI. It also provides specific information about the Cybersecurity Council.

Procedure:

- Implement Appropriate Security Controls
- Third-Party Cybersecurity Certification*
- Annual Security Assessments and Audits*
- Reports or Summaries of Certification Assessments & Annual Technical Audits
- Independent Review
- Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation
- Cybersecurity Council
- QHIN CISO

Security Requirements

SOP: QHIN Security Requirements for the Protection of TEFCA Information

Third-Party Cybersecurity Certification

- Every QHIN must be certified under a nationally recognized security framework from a list of pre-approved certifications/certifying bodies, found here: https://rce.sequoiaproject.org/qhin-cybersecurity-certification
- As part of a QHIN’s third-party cybersecurity certification, the certification scope must include:
  - All categories of controls from the then current version of the NIST Cybersecurity Framework (CSF)
  - All categories from NIST SP 800-171
  - Security Standards from the HIPAA Security Rule, per 45 CFR Part 164 Subpart C - Security Standards for the Protection of Electronic Protected Health Information, as may be amended

**This is a summary. Refer to the SOP for details*

Security Requirements

SOP: QHIN Security Requirements for the Protection of TEFCA Information

Annual Security Assessments

- Per the Common Agreement, QHINs must obtain an annual third-party security assessment and technical audit and provide evidence of completion and mitigation within thirty (30) days of completion

- Assessment scope must include any system critical to organizational operation, any system required to function as a QHIN, plus all new systems, components, and applications incorporated by the QHIN since certification. A QHIN's annual third-party technical audit must, at a minimum, include the following:
  - All categories of controls in the then current version of the NIST CSF
  - All categories of NIST SP 800-171
  - Security Standards from the HIPAA Security Rule, Per 45 CFR Part 164 Subpart C - Security Standards for the Protection of Electronic Protected Health Information
  - Comprehensive internet-facing penetration testing; including at a minimum, testing for the top ten web application security risks as published by the Open Worldwide Application Security Project (OWASP) – commonly known as the OWASP Top 10
  - Vulnerability assessment of the internal network by conducting and reviewing vulnerability scans to identify the patch and vulnerability status of its systems and applications

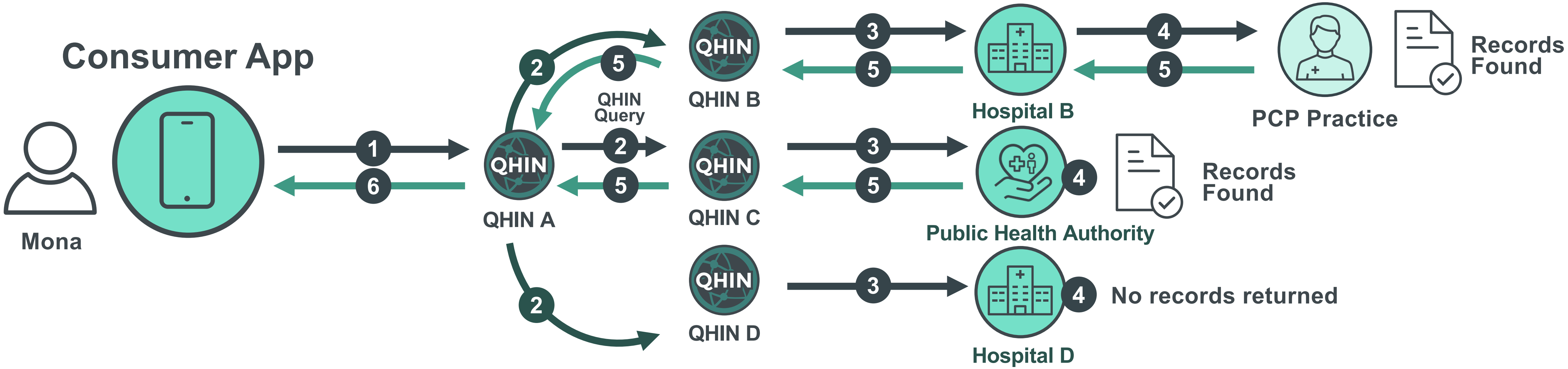
**This is a summary. Refer to the SOP for details*

SOP: Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS)

Example: Individual Access Services Exchange Purpose

TEFCA RECOGNIZED COORDINATING ENTITY

Use Case: Individual seeks her records from all her providers



1 Mona verifies her identity with a Consumer App (Participant that is an IAS Provider) and then uses it to make an Individual Access Services Request via QHIN A for Individual Access Services.

2 QHIN A initiates QHIN Query to all QHINs.

3 QHINs B, C, and D execute query methodologies to request medical records from their Participants.

4 Hospital B queries its Subparticipants, and a standalone PCP Practice (Subparticipant) finds matching medical records. Public Health Authority finds matching records. Hospital D finds no records.

5 In Response, The standalone PCP responds with the matched medical records to Hospital B, which sends them to QHIN B. The Public Health Authority sends matched records to QHIN C. QHINs B and C send medical records to QHIN A.

6 QHIN A sends medical records to Consumer App, who shares them with Mona.

This is a summary. Refer to the SOP for details

Exchange Purposes (XP) Implementation SOP: Individual Access Services (IAS)

Sections 4.1 – 4.6 of the XP Implementation SOP: IAS, are applicable to IAS Providers

SOP Sections

- 4.1. Exchange Purpose Code (XP Code)
- 4.2. QHIN Technical Framework (QTF)
- 4.3. Definitions
- 4.4. Credential Service Provider
- 4.5. IAS Provider Individual Verification
  - 4.5.1. Verification Demographics
- 4.6. Identity Token

Section Takeaways

- IAS Providers must have a Credential Service Provider (CSP) verify the patient's identity to identity insurance level 2 (IAL2)
- IAS Providers MUST authenticate Individuals to at least Authenticator Assurance Levels 2 (AAL2)
- IAS Providers MUST demonstrate that Individuals have proven their identities by including an IAL2 Claims Token in all transactions
- The demographic information used to verify the patient or representative MUST include at least the first name, last name, date of birth, address, city, state, and ZIP

**This is a summary. Refer to the SOP for details*

QHIN Technical Framework (QTF) v2.0 Security Requirements

Certificate and Crypto Module Requirements

QHINs Must:

- **Possess appropriate digital certificates** for authentication, encryption, and signing. QHIN certificates will be chained to root certificates issued by Certificate Authorities approved by the RCE.
- **Obtain X.509 version 3 Transport Level Security (TLS) server certificates** per the following:
  - signature at least 112 bits in length
  - public key at least 256 bits in length
  - certificates MUST be obtained, installed, and used in accordance with Applicable Law, and any relevant SOPs or implementation guides adopted by the RCE.
- **Deploy cryptographic modules** certified to meet Federal Information Processing Standard Publication 140-2 or 140-3

**This is a summary. Refer to the QTF for details*

Secure Channel Requirements

- QHINs must provide a secure channel to ensure transport-level security for all transactions under their domain. The specified standards for Secure Channel are:
  - IETF TLS 1.2 w/ BCP 195 or
  - IETF TLS 1.3 w/ BCP 195
- All connections using TLS MUST attempt to be negotiated as TLS 1.3 prior to falling back to TLS 1.2
- Until a future version of the QTF officially deprecates TLS 1.2, servers must support TLS 1.2 as a floor with a preference for TLS 1.3

Additional details are in QTF v2: QTF-6 through QTF-10

**This is a summary. Refer to the QTF for details*

Mutual Authentication

- The QTF specifies mutual authentication for all QHIN-to-QHIN and QHIN-to-Participant communication that is not secured with OAuth authentication.
- Specified standards for Mutual Authentication are:
  - IETF TLS 1.2 w/ BCP 195, or
  - IETF TLS 1.3 w/ BCP 195, or
  - OAuth 2.0
- When interacting with another QHIN, QHINs MUST mutually authenticate using TLS protocol version 1.2 or higher
- Authentication between QHINs and Participants MUST use TLS 1.2 or higher or OAuth 2.0

**This is a summary. Refer to the QTF for details*

User Authentication Requirements

- The QTF specifies that QHINs implement IHE XUA to support exchange of authentication information among QHINs.
- QTF-16 through 21 specify requirements for signing a SOAP header for QHIN-to-QHIN exchange and the SAML assertion requirements for QHIN Queries or QHIN Message Delivery

**This is a summary. Refer to the QTF for details*

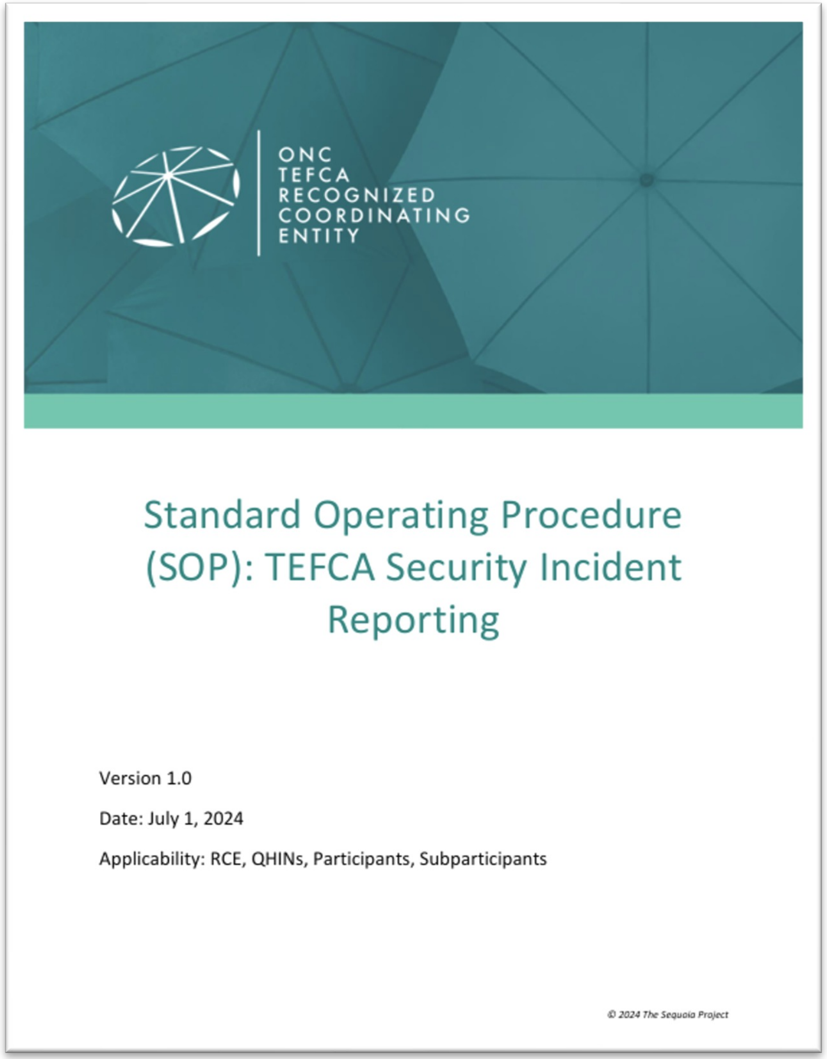
Audit Requirements:
IHE ATNA (content only) and ASTM 2147-18

- QHINs must implement the IHE ATNA (content only) profile requirements specific to event audit logging for activities and transactions between QHINs and between QHINs and Participants.
- Other elements of secure systems defined by ATNA, such as authentication, are specified elsewhere in the QTF.
  - QTF-92 A QHIN MUST be able to export all relevant audit records with format requirements as specified in the IHE ATNA profile for all activity and transaction events involving another QHIN or Participant.
  - QTF-93 A QHIN MUST follow auditing content guidance in any of the IHE transactions and profiles specified by the QTF including all codes and elements.
  - QTF-94 A QHIN MUST create and store audit records for all activity events related to the QHIN’s operation

**This is a summary. Refer to the QTF for details*

TEFCA Security Incident Reporting

SOP: TEFCA Security Incident Reporting



ONC TEFCA RECOGNIZED COORDINATING ENTITY

Standard Operating Procedure (SOP): TEFCA Security Incident Reporting

Version 1.0

Date: July 1, 2024

Applicability: RCE, QHINs, Participants, Subparticipants

Purpose: This SOP details the minimum reporting requirements for communicating TEFCA Security Incidents to the RCE, to other likely impacted QHINs, and to any likely impacted Participant and/or Subparticipant within the QHIN's network, as set forth in the Common Agreement and Terms of Participation.

Procedure

- 4.1 Confidentiality of Reports
- 4.2 General TEFCA Security Incident Reporting Requirements
- 4.3 TEFCA Security Incident Reporting for QHINs
- 4.4 TEFCA Security Incident Reporting Requirements for Participants and Subparticipants
- 4.5 TEFCA Security Incident Reporting Requirements for RCE
- 4.6 TEFCA Security Incident Report Format

Informative Guidance: TEFCA Security Incident Determination

- 5.1 Factor A: Did the incident involve TEFCA Information?
- 5.2 Factor B: Is there a permitted exception?
- 5.3 Factor C: Is the incident considered an other reportable security event?

SOP: TEFCA Security Incident Reporting*

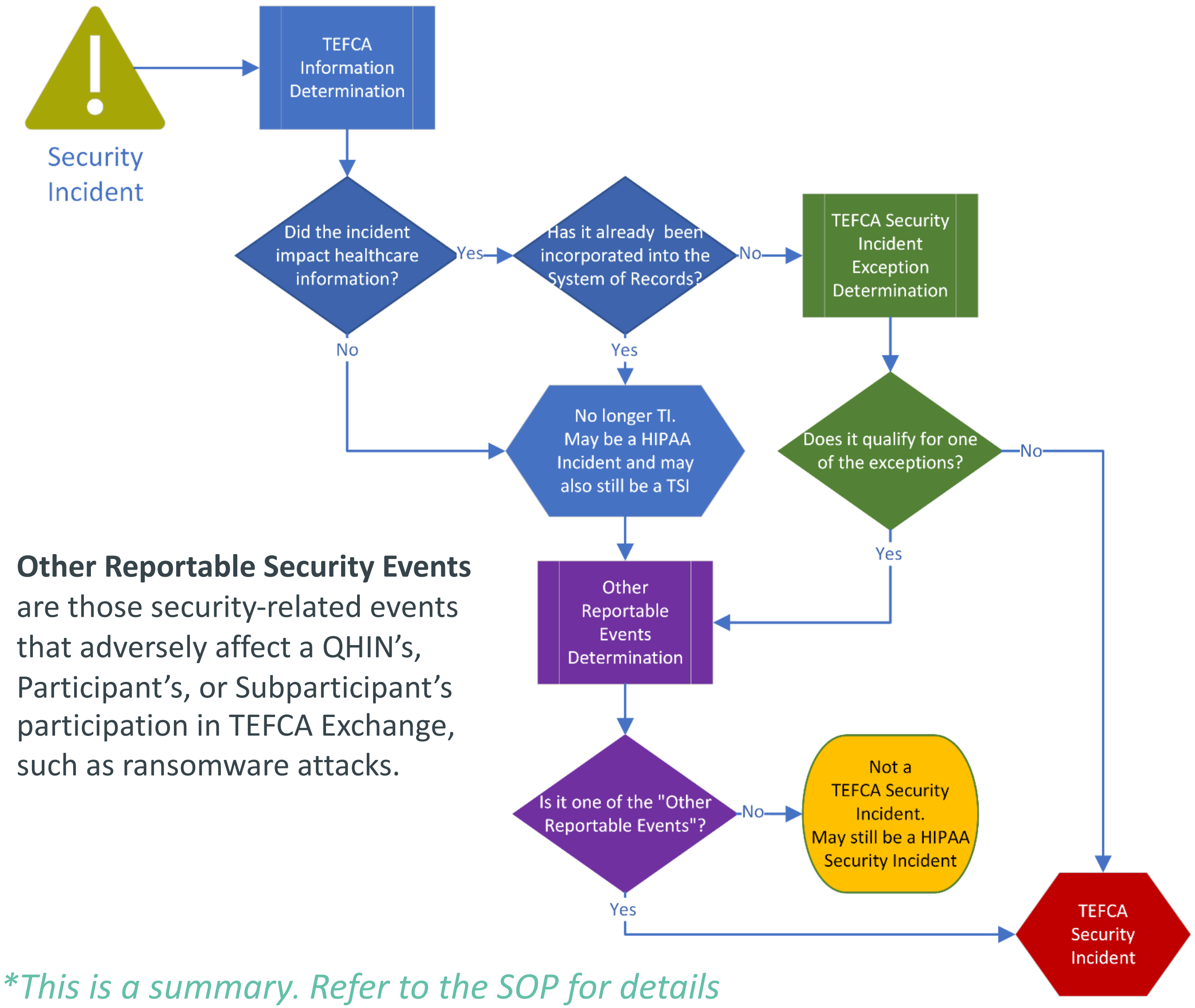
ONC TEFCA RECOGNIZED COORDINATING ENTITY

QHIN Reporting for TEFCA Security Incidents		
Report Type	**Timeline**	**Distribution**
QHIN TSI Initial Report	As soon as reasonably practicable, but not more than 72 hours after Discovery	1) If a QHIN experiences a TSI, or receives a TSI report from a downstream Participant or Subparticipant that is confirmed to be a TSI, it reports to the RCE using the TEFCA Security Incident Report form and 2) to all other QHINs likely impacted, and to Participants and Subparticipants within the reporting QHIN's network that are likely impacted.
QHIN TSI Supplemental Report	As additional pertinent information becomes available, and at least every 24 hours until the incident is resolved	Same as above for an initial TSI report
QHIN TSI Post-Incident Report	Required within 30 days after incident has been resolved	Affected QHIN reports to the RCE

Participant/Subparticipant Vertical Reporting for TEFCA Security Incidents		
Report Type	**Timeline**	**Distribution**
Vertical Reporting by Participants and Subparticipants.	For the Discovering entity: As soon as reasonably practicable, but not more than 72 hours after Discovery For the entity receiving a report from another entity: When vertically reporting a TEFCA Security Incident, the receiving entity has one business day to forward the report to their upstream entity and to likely affected downstream entities	1) To Upstream QPS any suspected or actual TEFCA Security Incident, and 2) To any likely affected Downstream Subparticipant for any actual TEFCA Security Incident they experience or has been reported to them by their Upstream QPS

**This is a summary. Refer to the SOP for details*

SOP: TEFCA Security Incident Reporting*


Security Incident
TEFCA Information Determination
Did the incident impact healthcare information?
Yes
No
Has it already been incorporated into the System of Records?
No
Yes
TEFCA Security Incident Exception Determination
No longer TI. May be a HIPAA Incident and may also still be a TSI
Does it qualify for one of the exceptions?
No
Yes
Other Reportable Events Determination
Is it one of the "Other Reportable Events"?
No
Yes
Not a TEFCA Security Incident. May still be a HIPAA Security Incident
TEFCA Security Incident

Other Reportable Security Events are those security-related events that adversely affect a QHIN's, Participant's, or Subparticipant's participation in TEFCA Exchange, such as ransomware attacks.

**This is a summary. Refer to the SOP for details*

EXCEPTIONS: An unauthorized acquisition, access, Disclosure, or Use of unencrypted TEFCA Information using TEFCA Exchange, is **NOT** a TEFCA Security Incident if **ANY** of the exceptions (a) through (c) apply:

(a) An unintentional acquisition, access, Use, or Disclosure of TEFCA Information by a Workforce Member or person acting under the authority of a QHIN, Participant, or Subparticipant, if such acquisition, access, Use, or Disclosure;

(i) was made in good faith,

(ii) was made by a person acting within their scope of authority,

(iii) was made to another Workforce Member or person acting under the authority of any QHIN, Participant, or Subparticipant, and,

(iv) does not result in further acquisition, access, Use, or Disclosure in a manner not permitted under Applicable Law and the Framework Agreements.

(b) 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.

(c) A Disclosure of TI that has been de-identified in accordance with the standard at 45 CFR § 164.514(b).

Educational Resources and Upcoming Events

Security Specific Resources

Privacy and Security SOPs

- IAS Provider Requirements
- QHIN Cybersecurity Certification
- QHIN Cybersecurity Coverage
- QHIN Security Requirements for the Protection of TEFCA Information Version 2.0
- TEFCA Security Incident Reporting

Download online resources exclusive to the RCE at
https://rce.sequoiaproject.org/tefca-and-rce-resources/

Join Us for a FHIR Over TEFCA Security Education Event: Preparing for the Future of Secure Health Data Exchange

Secure and scalable data-sharing protocols are critical components for TEFCA^{TM} nationwide data exchange. *FAST* (FHIR at Scale Taskforce), in collaboration with The Sequoia Project and HL7, is advancing security readiness with a **virtual Education Event on January 13, 2025**.

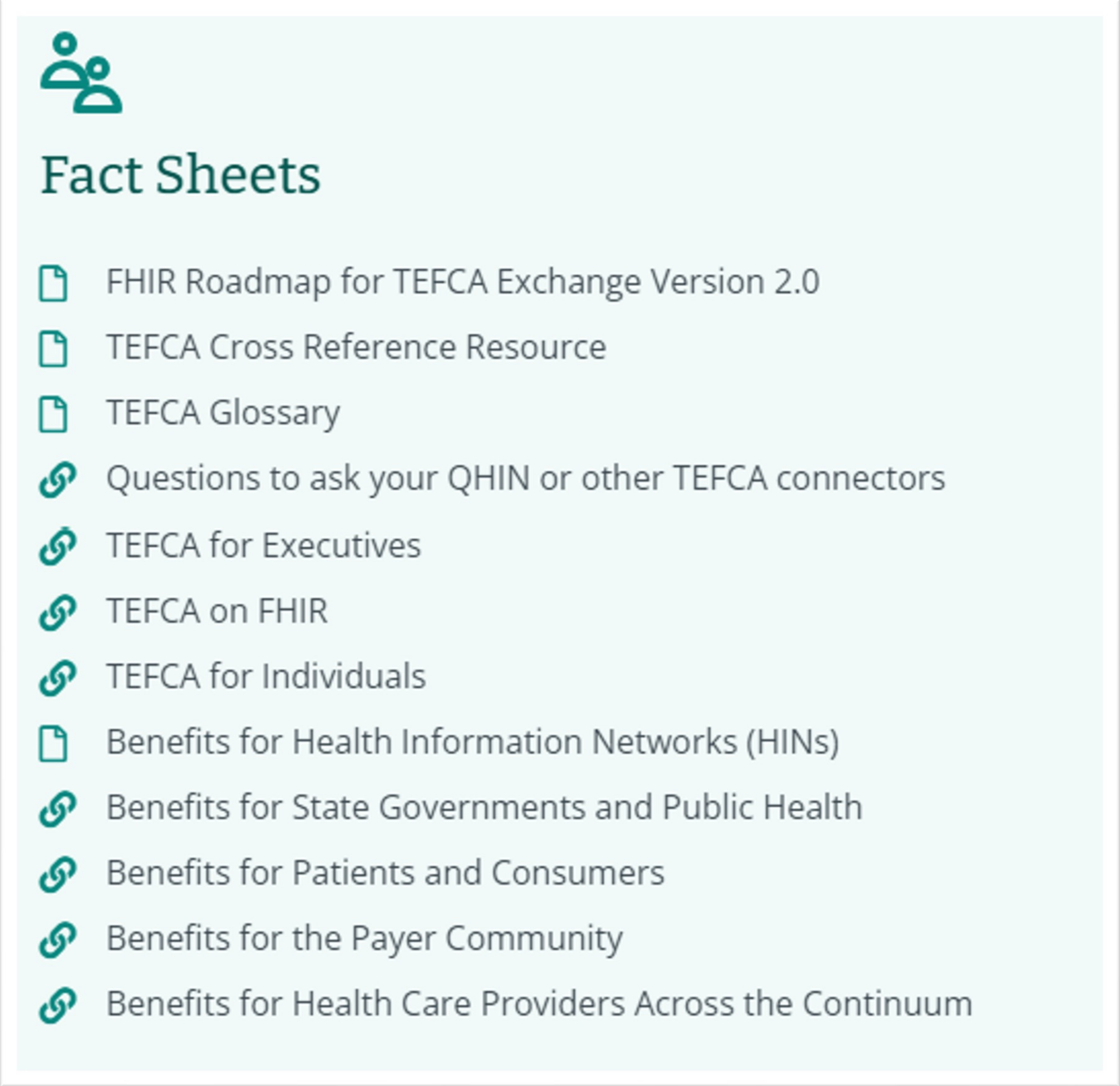
This complimentary event is designed to give healthcare organizations the insights they need to adopt and comply with the FAST Security standard for secure data exchange, focusing on the *FAST* HL7 UDAP Security for Scalable Registration, Authentication, and Authorization (*FAST* Security IG) FHIR Implementation Guide (IG) (SSRAA).

- **REGISTER HERE**

- https://us02web.zoom.us/webinar/register/WN_A8jNHgDuQbetiNb7EYs_Sw#/registration

The *FAST* Security IG will become mandatory within TEFCA by January 1, 2026, making this session an essential resource for preparing.

Updated Resources and FAQs



Fact Sheets

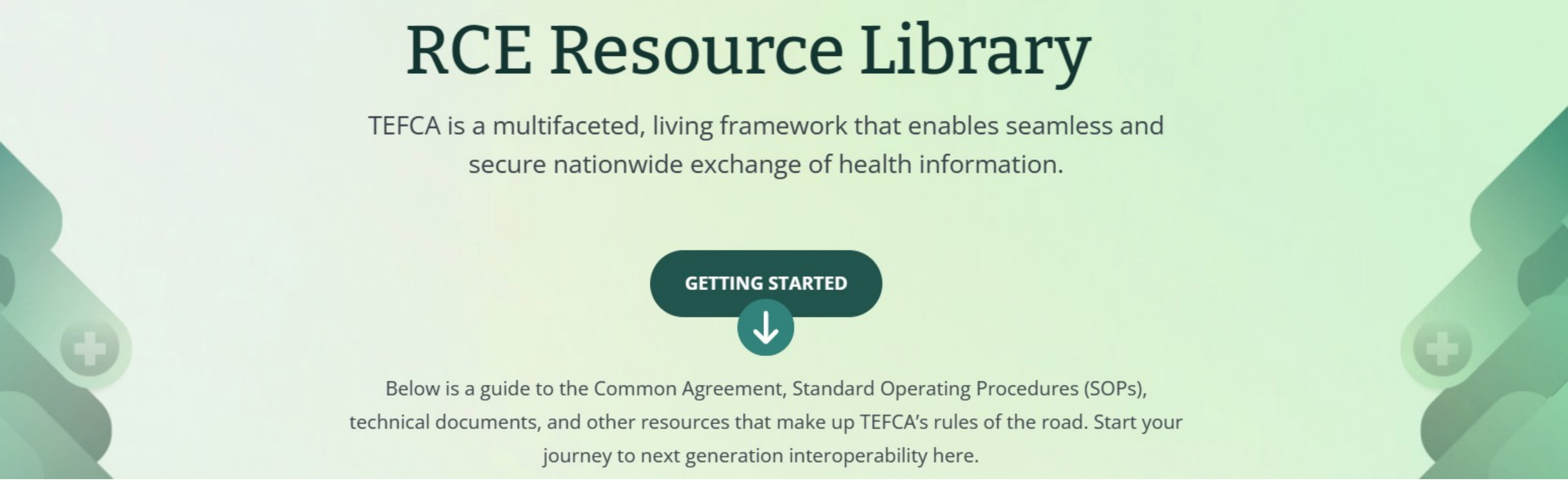
- FHIR Roadmap for TEFCA Exchange Version 2.0
- TEFCA Cross Reference Resource
- TEFCA Glossary
- Questions to ask your QHIN or other TEFCA connectors
- TEFCA for Executives
- TEFCA on FHIR
- TEFCA for Individuals
- Benefits for Health Information Networks (HINs)
- Benefits for State Governments and Public Health
- Benefits for Patients and Consumers
- Benefits for the Payer Community
- Benefits for Health Care Providers Across the Continuum

These Frequently Asked Questions address common questions and will be updated regularly.

- **What is TEFCA?**
- **How Does TEFCA Work?**
- **How Do I Participate in TEFCA Exchange?**
- **How is TEFCA Governed?**
- **How are QHINs Designated?**

https://rce.sequoiaproject.org/rce/faqs/

Additional TEFCA Resources from ASTP:
https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca



RCE Resource Library

TEFCA is a multifaceted, living framework that enables seamless and secure nationwide exchange of health information.

Below is a guide to the Common Agreement, Standard Operating Procedures (SOPs), technical documents, and other resources that make up TEFCA's rules of the road. Start your journey to next generation interoperability here.

https://rce.sequoiaproject.org/tefca-and-rce-resources/

Additional Resources:
https://www.healthit.gov/tefca

All Events Registration and Recordings:
https://rce.sequoiaproject.org/community-engagement/

Upcoming RCE Monthly Info Calls:
January 21, 12:00-1:00pm ET

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Questions & Answers

For more information:
rce.sequoiaproject.org