HL7® FHIR® Security

Education Event

Trusted Exchange Framework and Common Agreement ™ (TEFCA™) Security: What you need to know

Johnathan Coleman, CISSP, CISM, CRISC
Principal, Security Risk Solutions, Inc.
CISO, TEFCA RCE, The Sequoia Project Inc.

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

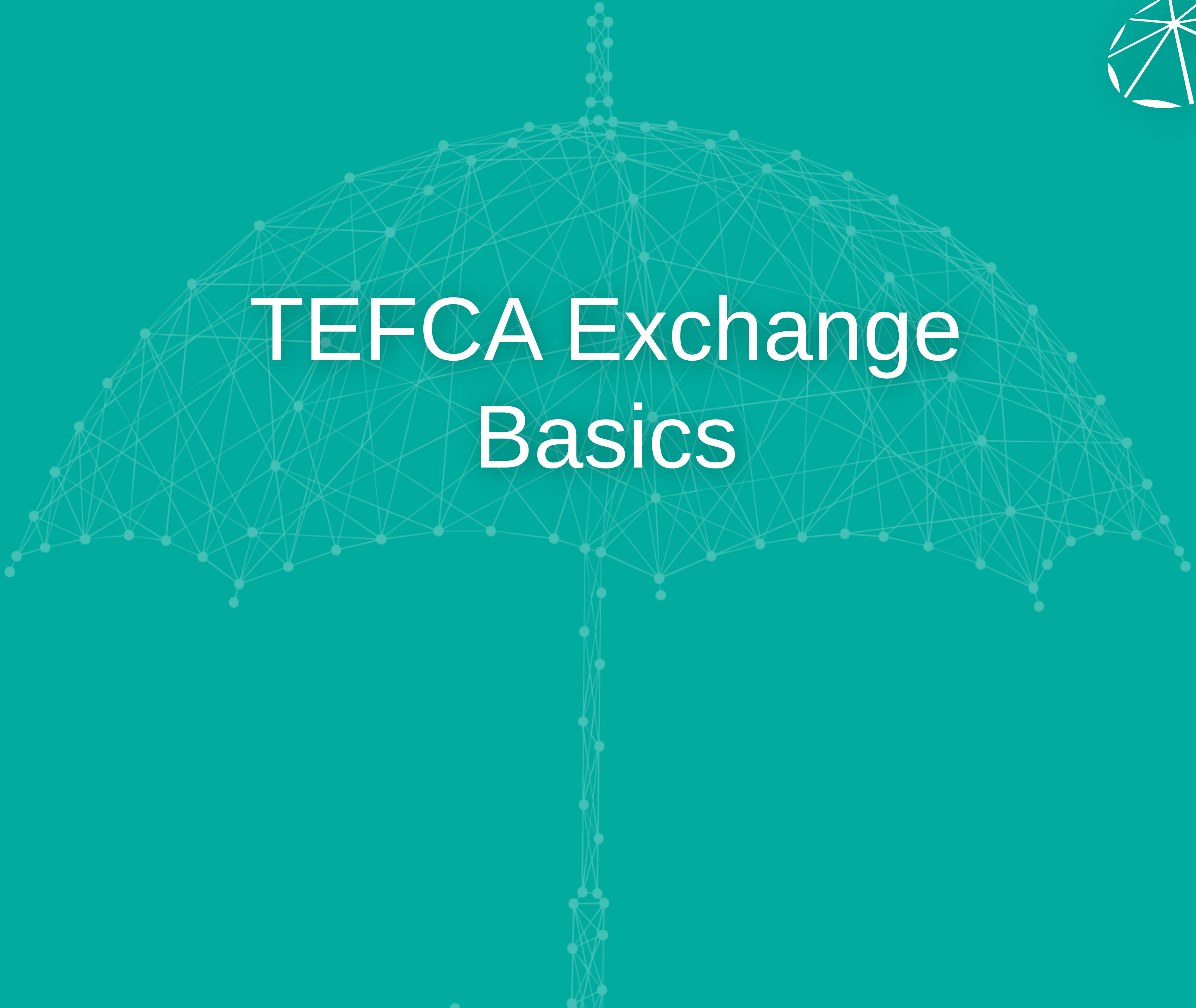
Agenda

- **TEFCA™ Exchange Basics**
- **QHIN Technical Framework (QTF) Security Requirements**
- **TEFCA Security Standard Operating Procedures (SOPs)**
  - Exchange Purposes (XP) Implementation SOP: Individual Access Services (IAS)
  - QHIN Security for the Protection of TEFCA Information (updated)
  - TEFCA Security Incident Reporting
  - Additional Security Requirements for Participants and Subparticipants
- **Questions & Answers (Q&A)**

HL7® FHIR®

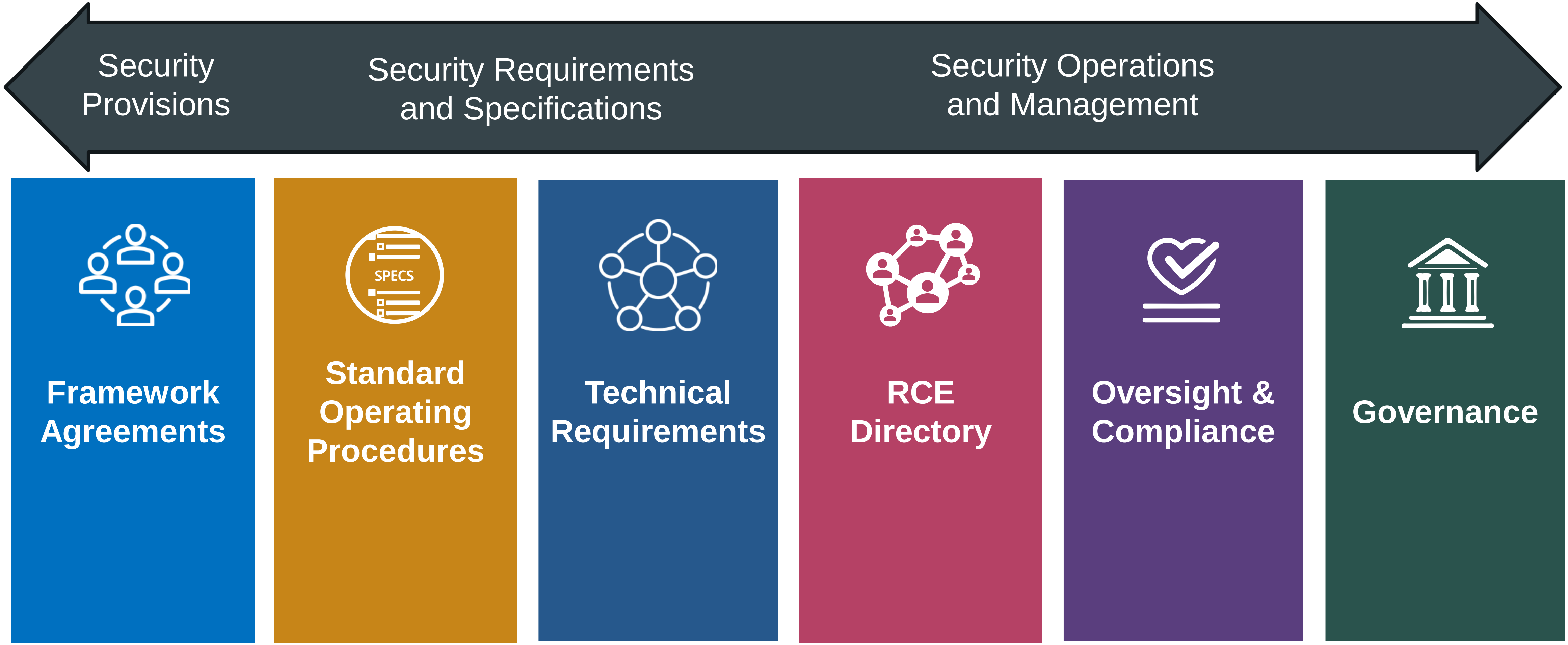
TEFCA is Ramping Up and Looking to the Future with FHIR!

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY



TEFCA Exchange Basics

TEFCA Components



Security Provisions

Security Requirements and Specifications

Security Operations and Management

Framework Agreements

Standard Operating Procedures

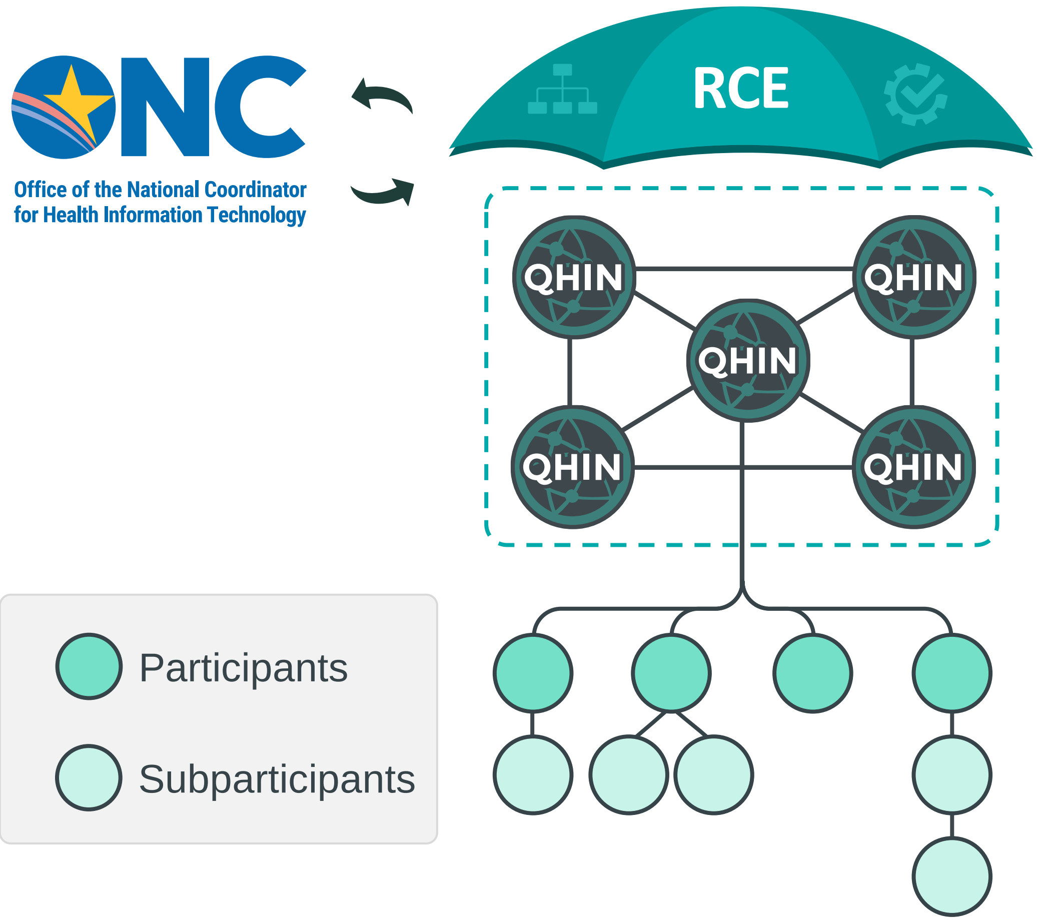
Technical Requirements

RCE Directory

Oversight & Compliance

Governance

Exchange Under TEFCA


ONC
Office of the National Coordinator for Health Information Technology
RCE
QHIN
QHIN
QHIN
QHIN
QHIN
Participants
Subparticipants

ONC 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

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/

Batch Releases

Published July 1, 2024

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

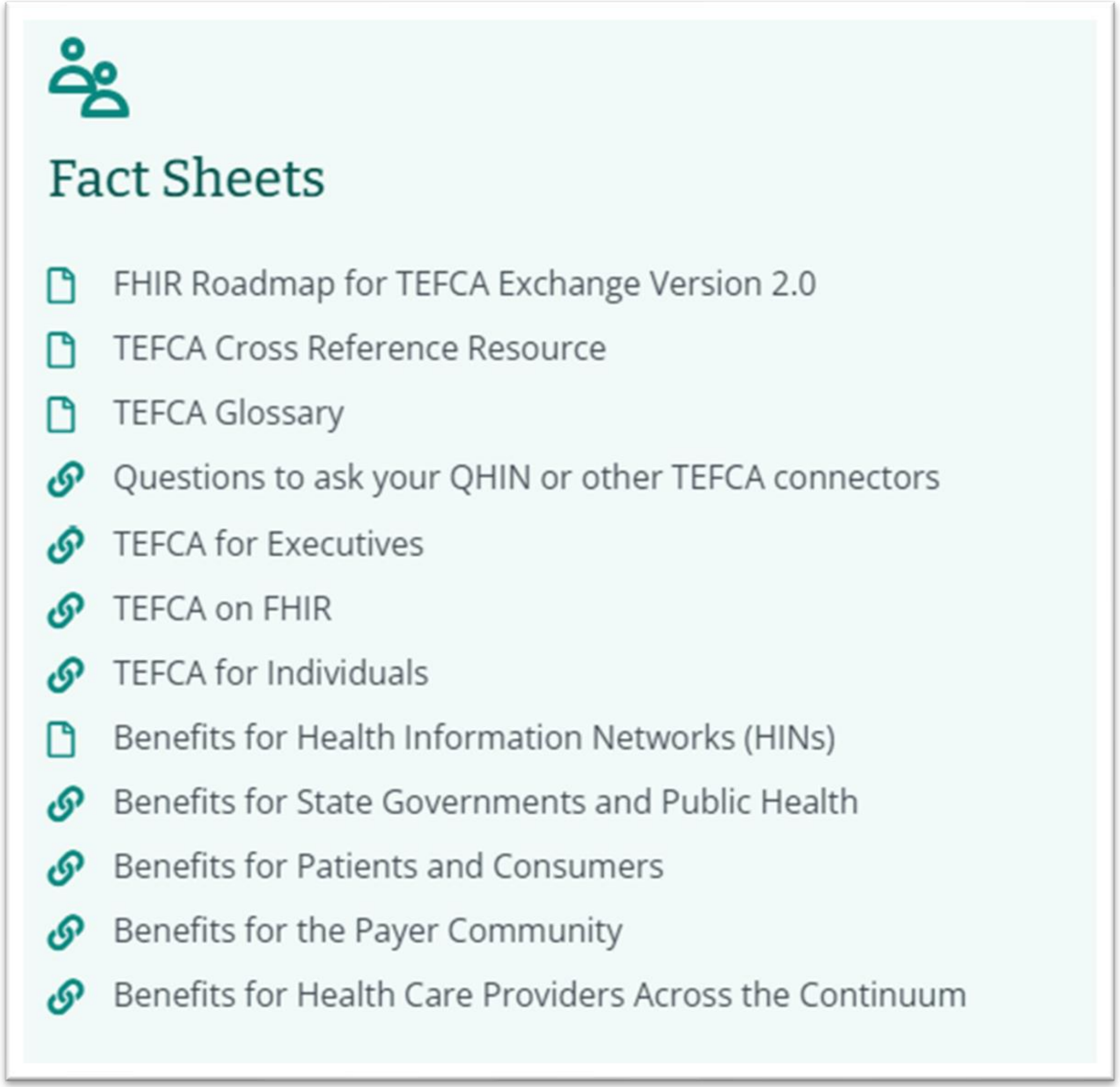
Published August 6th

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

Expected Fall 2024

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

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/

QHIN Technical Framework (QTF) 2.0 Security Requirements

The information contained in these slides is abbreviated from the QHIN Techncial Framework (QTF).
For comprehensive details and specific requirements, please refer to the complete QTF documentation.

Certificate and Cryptographic 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.

- QHINs MUST obtain X.509 version 3 Transport Level Security (TLS) server certificates
  - signature that is at least 112 bits in length,
  - public key of at least 256 bits in length;
  - such certificates MUST be obtained, installed, and used in accordance with Applicable Law, and any relevant SOPs or implementation guides adopted by the RCE.

- QHINs MUST deploy cryptographic modules certified to meet Federal Information Processing Standard Publication 140-2 or 140-3.

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

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.

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

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

- QHINs must implement the IHE ATNA 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.

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

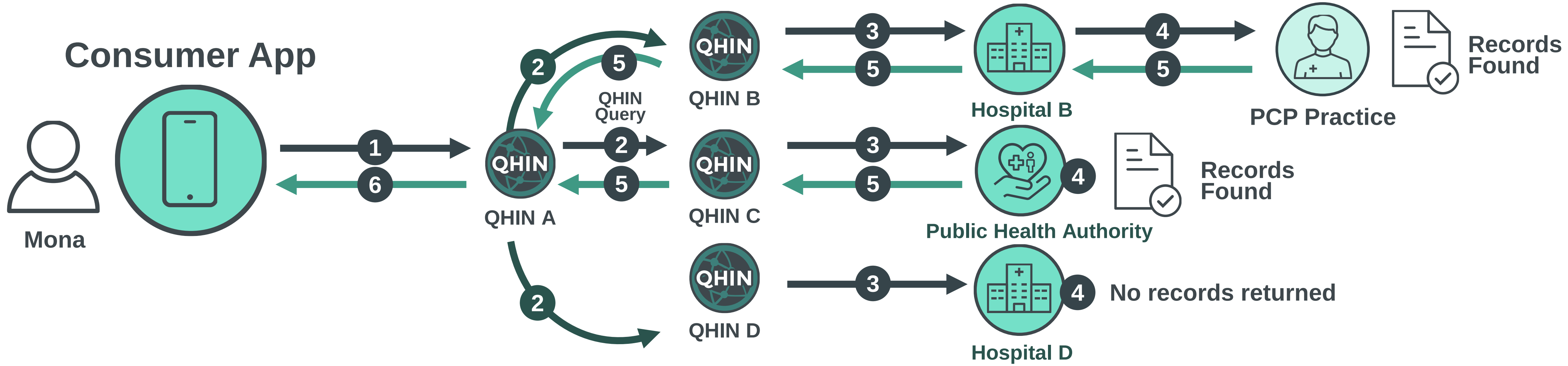
Exchange Purposes (XP) Implementation SOP: Individual Access Services (IAS)

August 6, 2024

The information contained in these slides is abbreviated from the Standard Operating Procedures (SOPs). For comprehensive details and specific requirements, please refer to the complete SOP documentation.

Example: Individual Access Services Exchange Purpose

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.

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

Sections 4.1 – 4.6 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

- All TEFCA exchange under IAS MUST use the XP code T-IAS and follow the technical requirements in the QTF and FHIR implementation SOP.
- 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

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

SOP: QHIN Security for the Protection of TEFCA Information

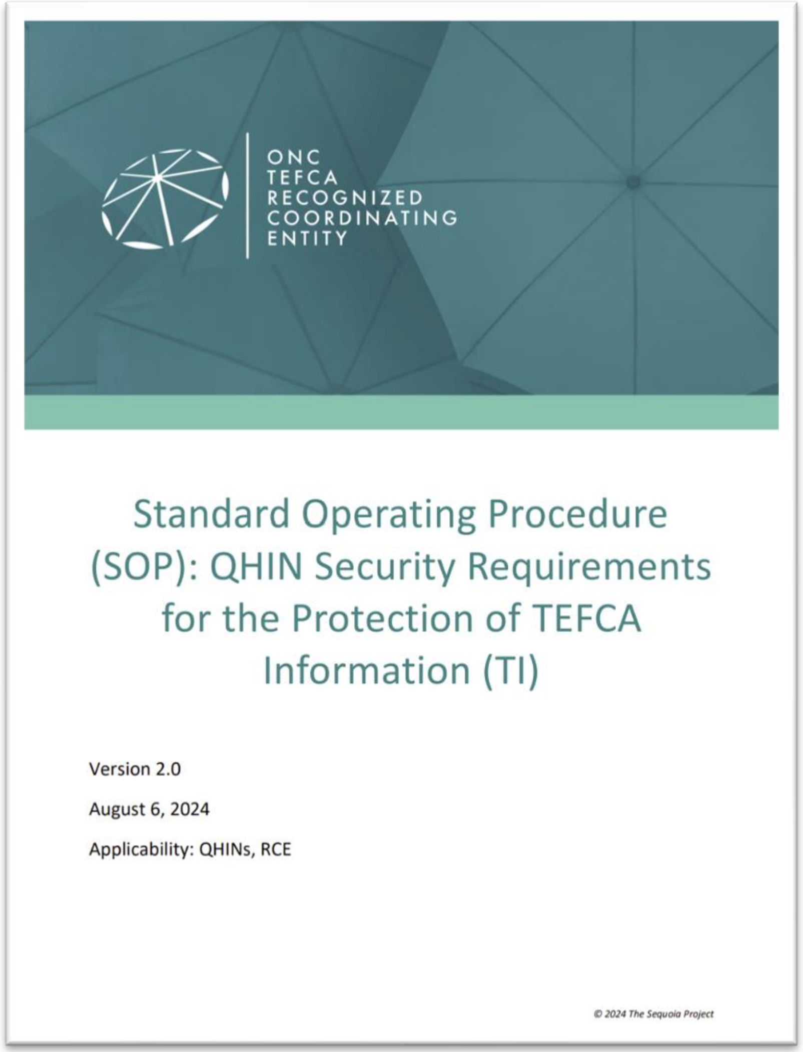
updated August 6, 2024

The information contained in these slides is abbreviated from the Standard Operating Procedures (SOPs).
For comprehensive details and specific requirements, please refer to the complete SOP documentation.

SOP – QHIN Security Requirements for the Protection of TEFCA Information

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

- **Procedure:**
  1. Implement Appropriate Security Controls
  2. Third-Party Cybersecurity Certification
  3. Annual Security Assessments Audits
  4. Reports or Summaries of Certification Assessments & Annual Technical Audits
  5. Independent Review
  6. Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation
  7. Cybersecurity Council
  8. QHIN CISO



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

QHIN Certification Requirements (summary)

1. **Implement Appropriate Security Controls:** QHINs shall:

   a. Comply with the HIPAA Security Rule as if the HIPAA Security Rule applied to Individually Identifiable Information that is TEFCA Information regardless of whether they are a Covered Entity or a Business Associate.

   b. Implement and maintain appropriate security controls for Individually Identifiable Information that are commensurate with risks to the confidentiality, integrity, and/or availability of the Individually Identifiable Information.

   c. Where appropriate, utilize Recognized Security Practices, as defined by Public Law No: 116-321 (e.g., the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities).

QHIN Certification Requirements

2. **Third-Party Cybersecurity Certification**

   a. 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

   b. As part of a QHIN's third-party cybersecurity certification, the certification scope must include:

      i. All categories of controls from the then current version of the NIST Cybersecurity Framework (CSF);

      ii. All categories from NIST SP 800-171; and

      iii. 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*

QHIN Certification Requirements*

2. **Third-Party Cybersecurity Certification (continued)**

   c. Organizations may utilize more than one assessor organization or certification body to meet the requirements identified in 4.2.b, however all requirements must still be met, and all certification bodies used to satisfy these requirements must be on the RCE-published list of currently approved certifications.

   d. Post-certification changes to the QHIN's systems are inevitable, such as those necessary to adopt new capabilities or technologies. In cases where substantial changes occur that would potentially impact the certification status of the QHIN, the new components and capabilities must be assessed to the same rigor as is required for the annual security assessment (per section 3 of the SOP). The new components or capabilities must be adopted into the assessment scope for the Designated Network's future certification/recertification efforts.

QHIN Certification Requirements*

3. Annual Security Assessments

a. Per Common Agreement Section 12.1.3, 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.

b. 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:

   i. All categories of controls in the then current version of the NIST CSF;

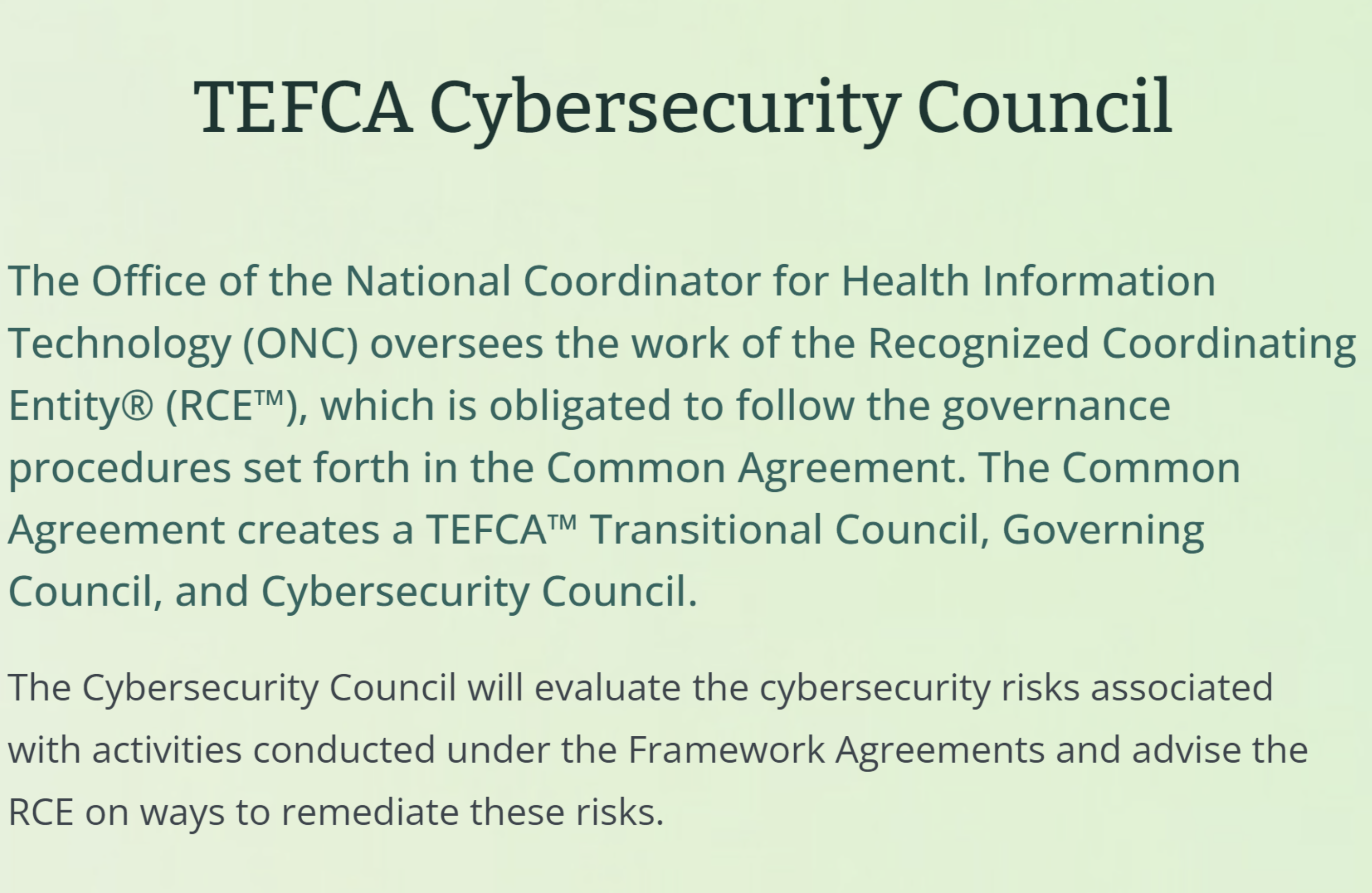
   ii. All categories of NIST SP 800-171;

   iii. Security Standards from the HIPAA Security Rule, Per 45 CFR Part 164 Subpart C - Security Standards for the Protection of Electronic Protected Health Information;

   iv. 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; and

   v. Vulnerability assessment of the internal network by conducting and reviewing vulnerability scans to identify the patch and vulnerability status of its systems and applications.

SOP: QHIN Security for the Protection of TEFCA Information



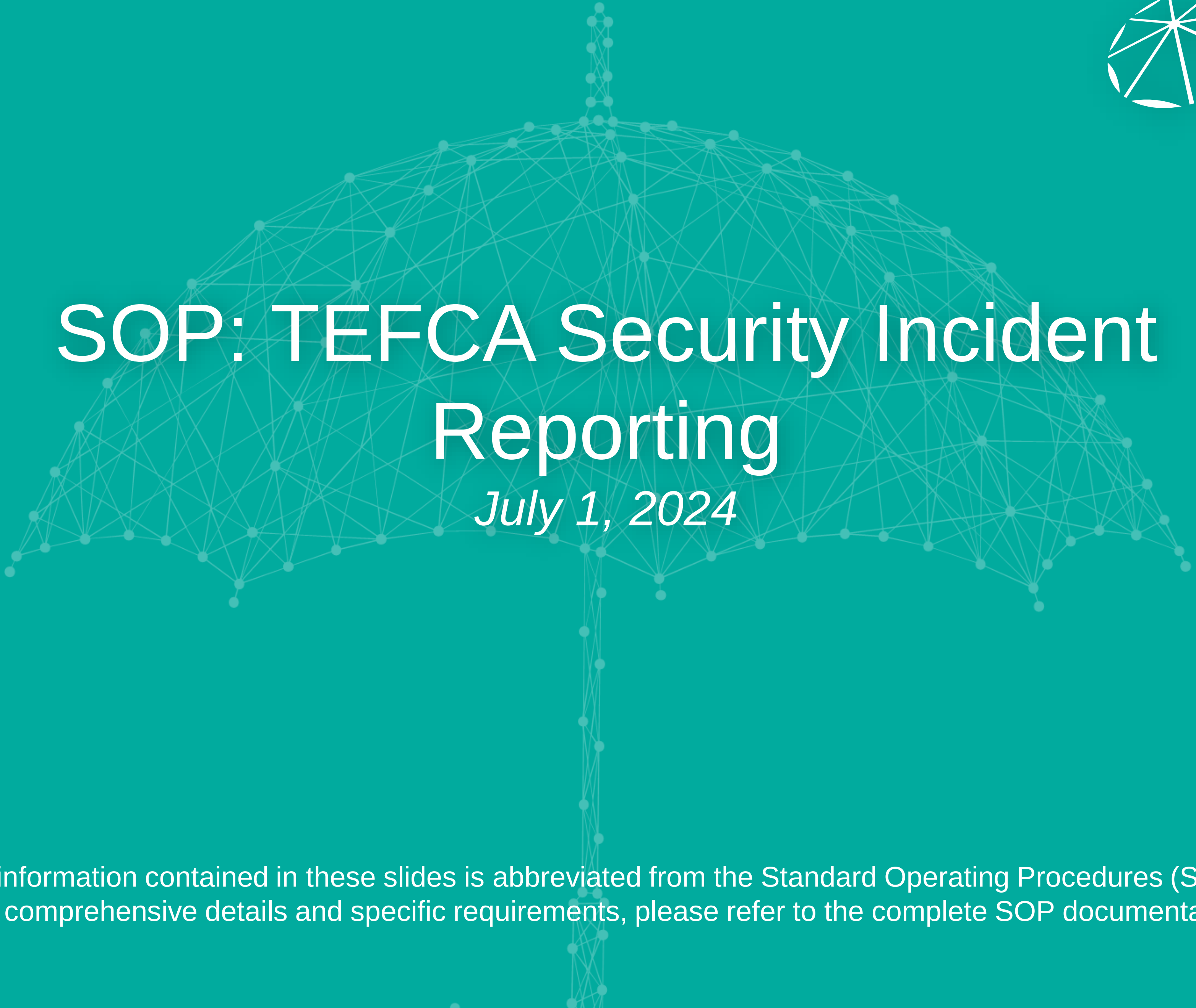
TEFCA Cybersecurity Council

The Office of the National Coordinator for Health Information Technology (ONC) oversees the work of the Recognized Coordinating Entity® (RCE™), which is obligated to follow the governance procedures set forth in the Common Agreement. The Common Agreement creates a TEFCA™ Transitional Council, Governing Council, and Cybersecurity Council.

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

https://rce.sequoiaproject.org/tefca-cybersecurity-council/

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

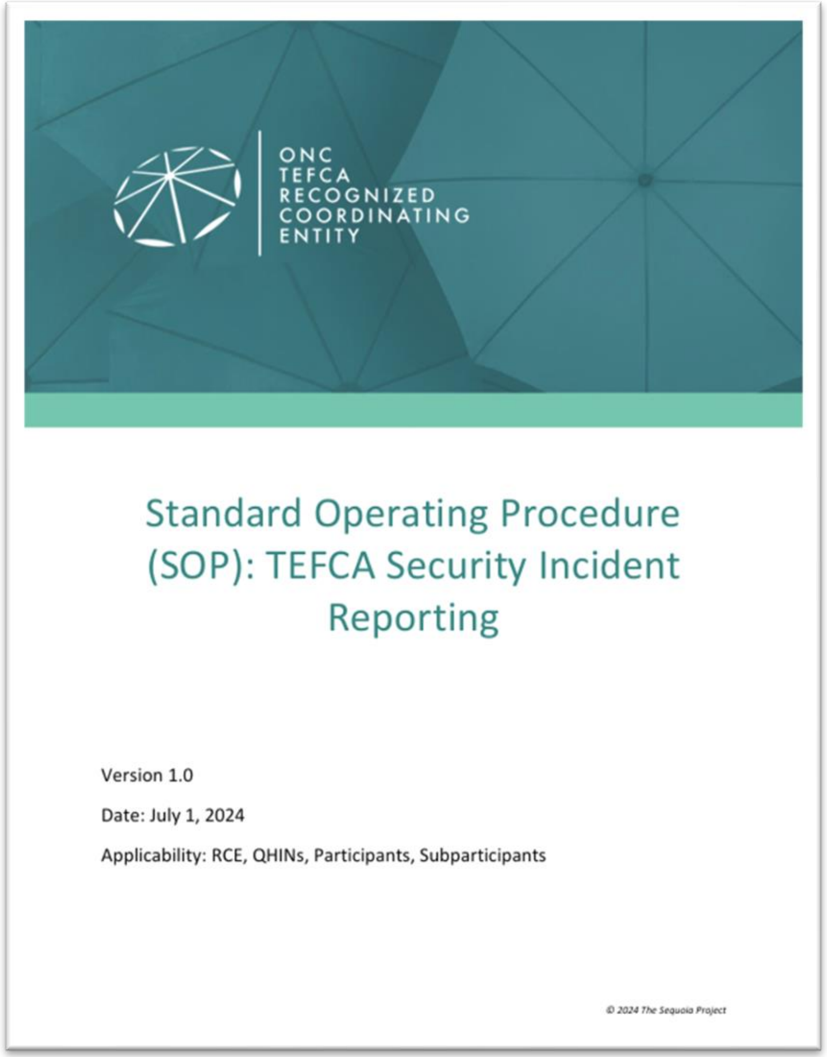


SOP: TEFCA Security Incident Reporting

July 1, 2024

The information contained in these slides is abbreviated from the Standard Operating Procedures (SOPs). For comprehensive details and specific requirements, please refer to the complete SOP documentation.

SOP: TEFCA Security Incident Reporting



Standard Operating Procedure (SOP): TEFCA Security Incident Reporting

Version 1.0

Date: July 1, 2024

Applicability: RCE, QHINs, Participants, Subparticipants

© 2024 The Sequoia Project

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.

SOP Sections:

1. Common Agreement References
2. SOP Definitions
3. Purpose
4. 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
5. 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?

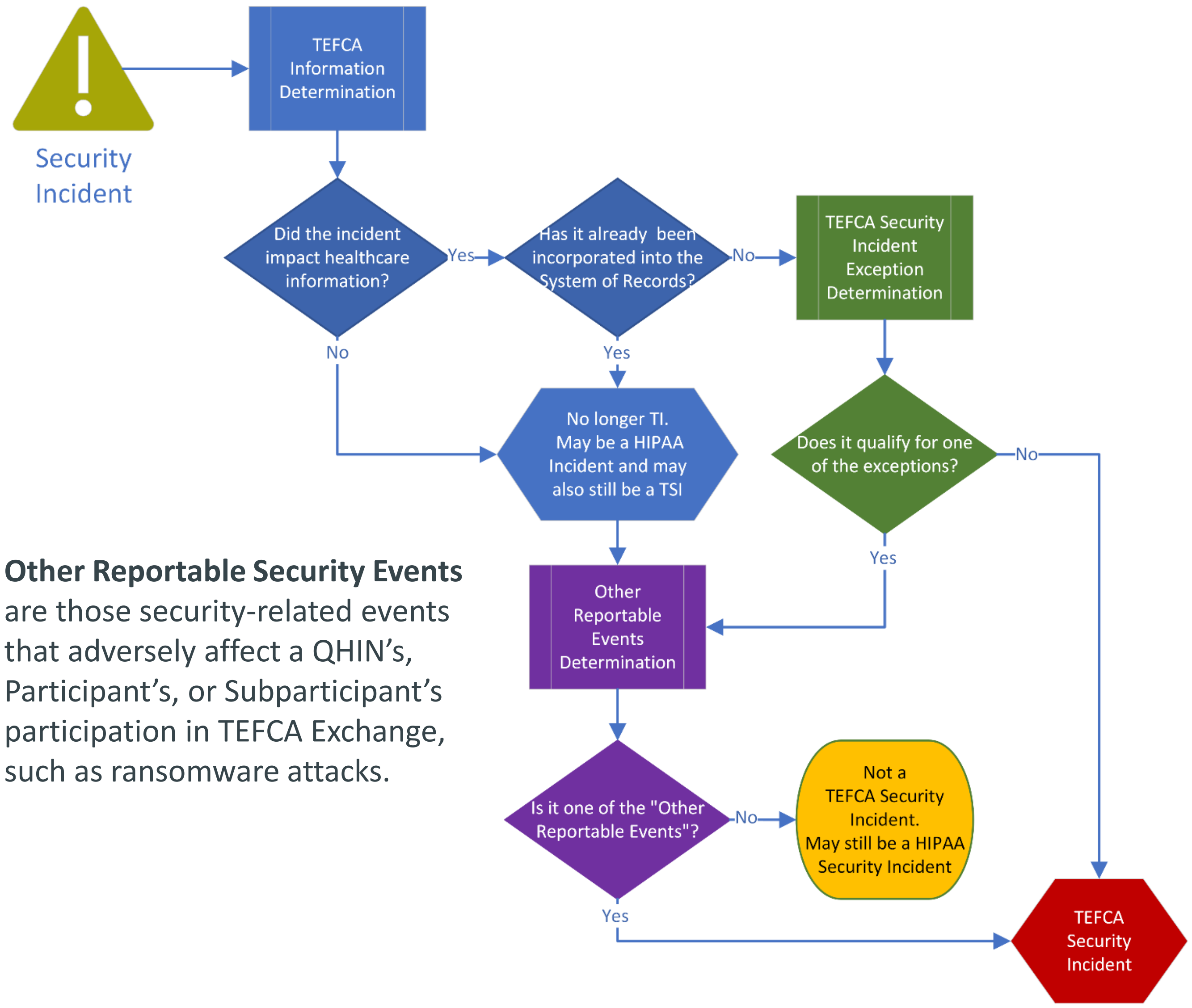
SOP: TEFCA Security Incident Reporting*

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

Has it already been incorporated into the System of Records?

No

TEFCA Security Incident Exception Determination

No

Yes

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

Not a TEFCA Security Incident. May still be a HIPAA Security Incident

Yes

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.

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:

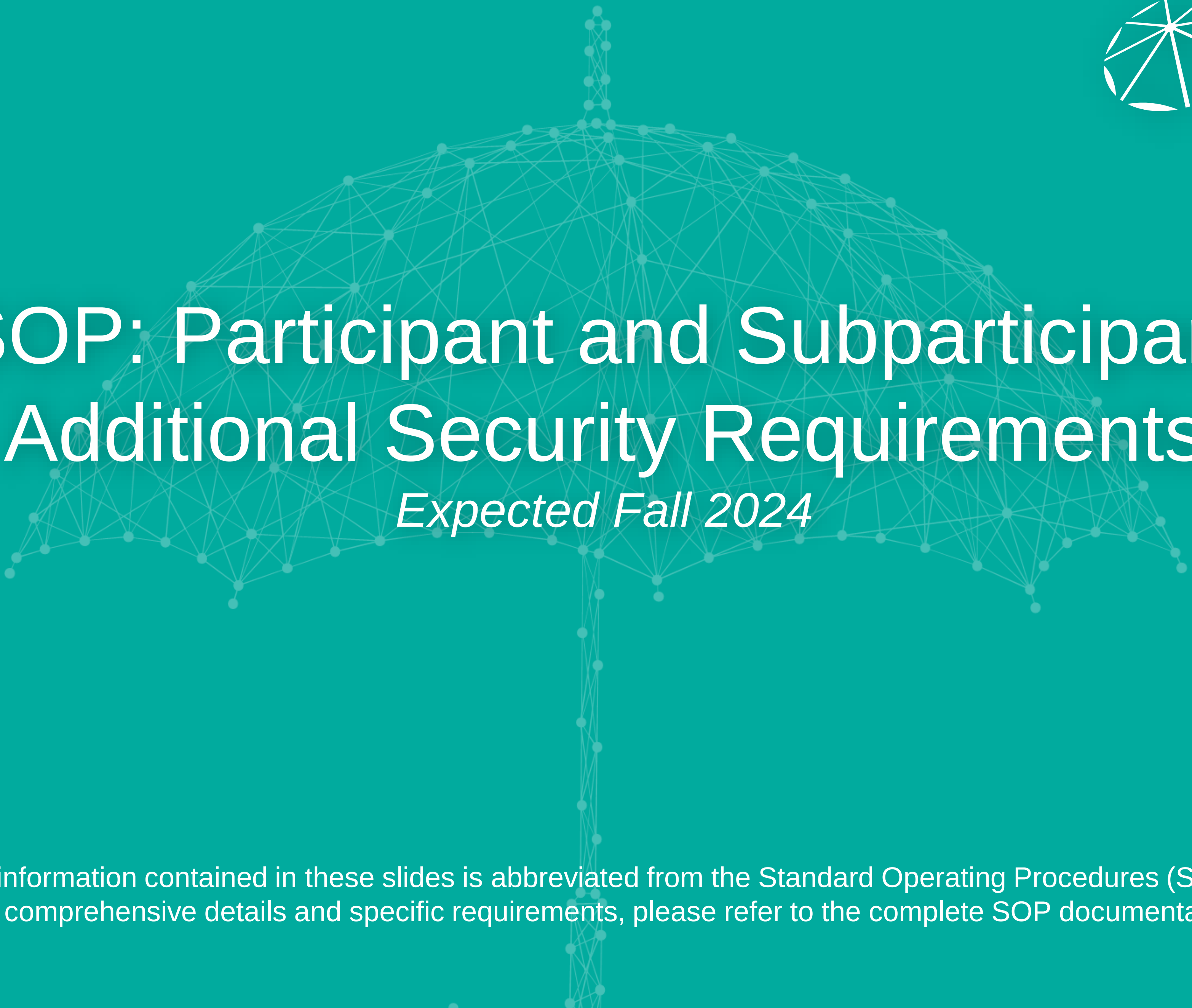
(a) An unintentional acquisition, access, Use, or Disclosure of TEFCA Information by a Workforce Member or person acting under the authority of a QHIN, Participant, or Subparticipant, if such acquisition, access, Use, or Disclosure;

- (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).

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



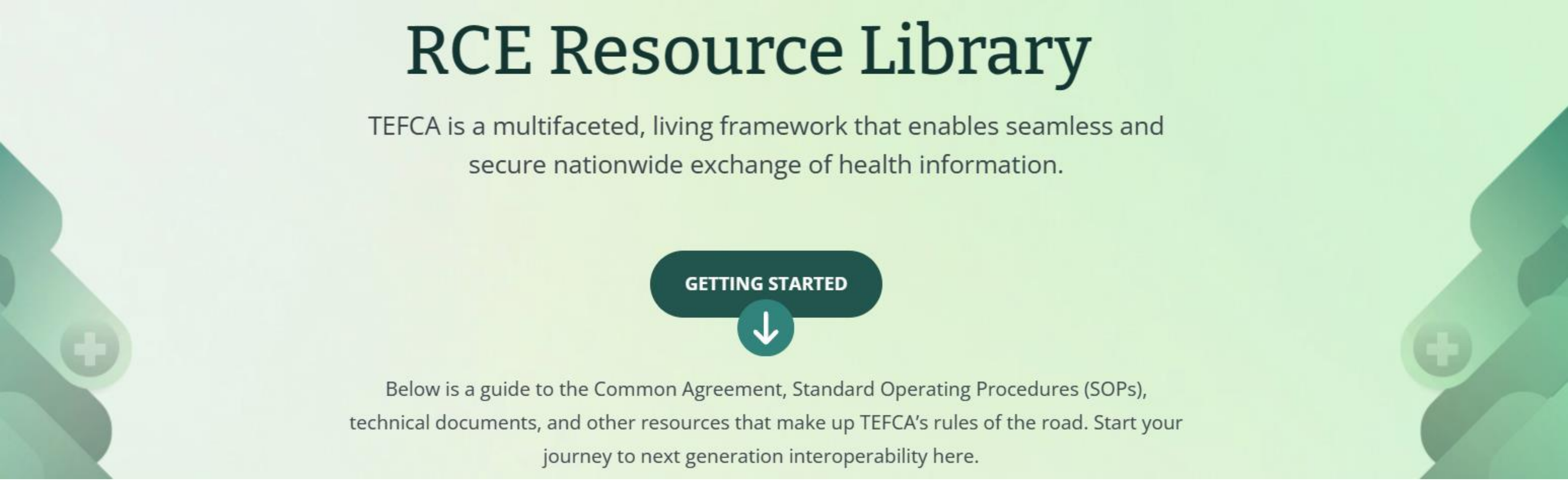
SOP: Participant and Subparticipant Additional Security Requirements

Expected Fall 2024

The information contained in these slides is abbreviated from the Standard Operating Procedures (SOPs).
For comprehensive details and specific requirements, please refer to the complete SOP documentation.

Additional Security Requirements SOP Development Timeline

- Jan 2023: First draft ot the SOP published for public comment.
  - Included proposed requirements for:
    - Authentication for Individuals and Workforce Members (AAL2)
    - Audit logging for Participants and Subparticipants (ASTM 2147)
    - Secure Channel for Participants and Subparticipants (per QTF)
- Undergoing revisions based on public feedback and comments from the TEFCA Cybersecurity Council and TEFCA Policy and Technical Advisory Group (PTAG)



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/

Thank you!

Johnathan Coleman
Principal, Security Risk Solutions, Inc.
CISO, TEFCA RCE, The Sequoia Project Inc.
Cell:(843) 442-9104
jc@securityrs.com
jcoleman@sequoiaproject.org