Carequality
Annual Meeting 2022
Grand Hyatt Washington

Securing Health Information Exchange for the Public Good

Johnathan Coleman

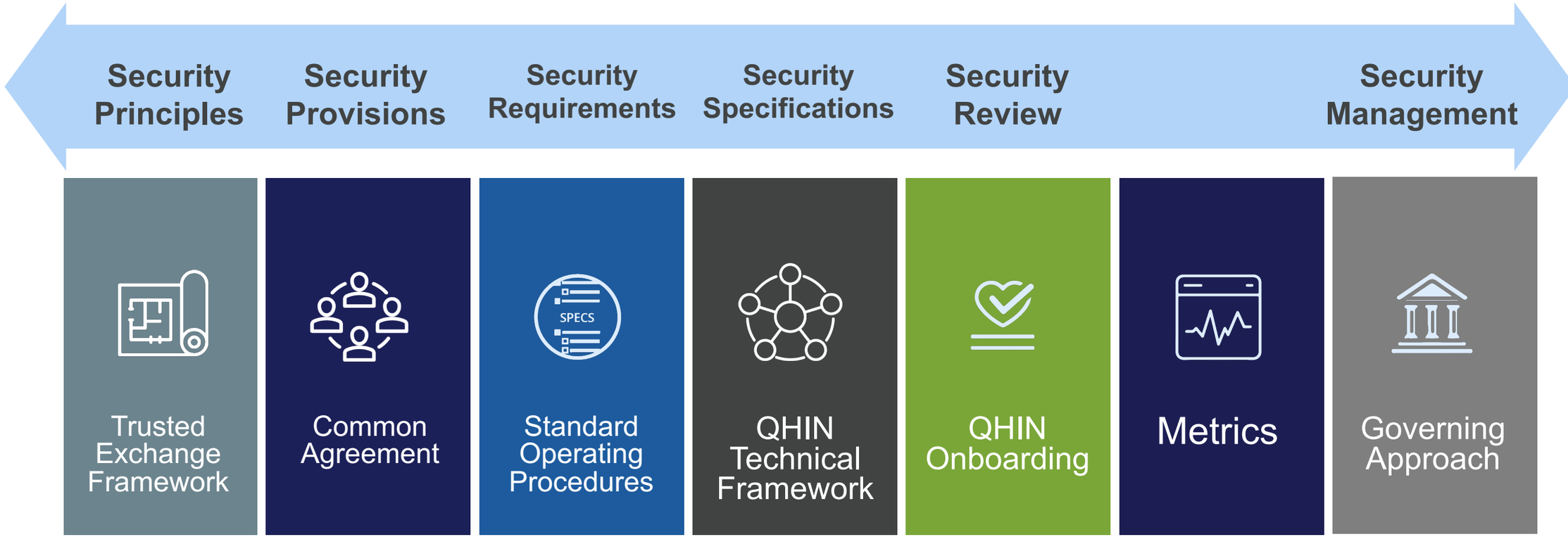
carequality

Agenda

- Components of TEFCA Security
  - Security principles of the TEF
  - Security sections of the CA
  - Standard Operating Procedures:
    - QHIN Security for the Protection of TEFCA Information
    - QHIN, Participant, and Subparticipant Additional Security Requirements (*DRAFT)*
  - Other TEFCA Security Related Resources
- Q&A

Components of TEFCA Security

TEFCA Components



The Trusted Exchange Framework

The Trusted Exchange Framework (TEF)

The **TEF** describes a common set of non-binding, foundational principles for trust policies and practices that can help facilitate exchange among health information networks (HINs).

- Principle 1 — Standardization
- Principle 2 — Openness and Transparency
- Principle 3 — Cooperation and Non-Discrimination
- **Principle 4 — Privacy, Security, and Safety**
- Principle 5 — Access
- Principle 6 — Equity
- Principle 7 — Public Health

The Trusted Exchange Framework (TEF)

Principle 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

- 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.
- Within the context of applicable law, HINs should enforce policies concerning individuals' ability to consent to the access, exchange, or use of their digital health information.

The Common Agreement

CA Security Requirements – Summary (Continued)

HIPAA Security Rule*

QHINs, Participants and Subparticipants, generally, will have to comply with requirements of the HIPAA Security Rule, even if they are not a Covered Entity or a Business Associate. This is a required flow-down from QHINs.

Cybersecurity Coverage*

QHINs will need insurance (or financial reserves to self-insure) for cyber risk and technology errors and omissions, per the Cybersecurity Coverage SOP.

Cybersecurity Certification*

QHINs will need to achieve and maintain third-party certification to an industry-recognized cybersecurity framework demonstrating compliance with all relevant security controls, as set forth in the applicable SOP (under development).

**This is a summary only - Refer to Common Agreement for the specific requirements*

CA Security Requirements – Summary (Continued)

Annual Security Assessment*

QHINs must obtain an annual third-party security assessment and technical audit. QHINs will need to provide evidence to the RCE that the assessment has taken place and of any appropriate mitigation efforts within thirty (30) days.

Other Security Flow-down Requirements*

QHINs will require Participants and Subparticipants to implement and maintain any additional applicable security requirements that may be set forth in an SOP.

**This is a summary only - Refer to Common Agreement for the specific requirements*

CA Security Requirements – Summary (Continued)

Security Resource Support to Participants *

QHINs will make available to Participants:

- Security resources and guidance regarding the protection of TEFCA Information applicable to their participation in the QHIN.
- Information and resources that the RCE or Cybersecurity Council makes available to the QHIN related to promotion and enhancement of the security of TEFCA Information.

Chief Information Security Officer *

The RCE CISO will be responsible for monitoring and maintaining the overall security posture of activities conducted under the Framework Agreements, and for making recommendations to QHINs regarding changes to baseline security practices. However, QHINs and not the RCE, are ultimately responsible for the security posture of their networks and activities, as well as for their downstream agreements.

**This is a summary only - Refer to Common Agreement for the specific requirements*

CA Security Requirements – Summary (Continued)

TEFCA Security Incident Notifications*

- Within five (5) calendar days after determining that a TEFCA Security Incident has occurred, QHINs will notify the RCE and to all QHINs that are likely impacted. The notification must include sufficient information for the RCE and others affected to understand the nature and likely scope of the TEFCA Security Incident.
- Requirements for reporting TEFCA Security Incidents extend to Participants and Subparticipants by way of the “Vertical Reporting” provisions.

Compliance with Notification Under Applicable Law *

All breach notification requirements that exist under the HIPAA Rules, the FTC Rule, and/or other Applicable Law still apply, but duplicative notification is not required.

**This is a summary only - Refer to Common Agreement for the specific requirements*

SOP: QHIN Security for the Protection of TEFCA Information

Rev. 1 (updated as of May 2022)

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. Third-Party Cybersecurity Certification
  2. Annual Technical Audits
  3. Reports or Summaries of Certification Assessments & Annual Technical Audits
  4. Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation
  5. Cybersecurity Council

The Cybersecurity & Infrastructure Security Agency (CISA) has identified the healthcare and public health sector as part of the nation's critical infrastructure, stating: The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure

https://www.cisa.gov/healthcare-and-public-health-sector#:~:text=The%20Healthcare%20and%20Public%20Health,disease%20outbreaks%2C%20and%20natural%20disasters.

Third-Party Cybersecurity Certification

- Every QHIN must be certified under a nationally recognized security framework from a list of pre-approved certifications/certifying bodies developed by the RCE.
- The RCE will maintain and publish a list of certifying bodies which meet the RCE's security certification requirements
    a) Any third-party accreditation or certification body that can demonstrate adherence to the requirements listed in the SOP may be considered for inclusion
    b) Interested parties should refer to the official RCE-published list of currently approved certifications available at https://rce.sequoiaproject.org/qhin-cybersecurity-certification
    c) Certification bodies providing services that meet these requirements, but that have not yet been utilized by a designated QHIN, may also request approval to be included

Third-Party Cybersecurity Certification Ctd.

- As part of a QHIN's third-party cybersecurity certification process, the certification body must:

  a) Ensure assessments are conducted in accordance with the NIST Cybersecurity Framework (CSF), specifically all categories in the CSF and NIST 800-171 are required, with assessments conducted using NIST 800-53 moderate as a reference

  b) Review the QHIN's HIPAA security analysis (consistent with §164.308(a)(1)(ii)(A))

  c) Verify Common Agreement requirements for technical audits and assessments are met

Annual Technical Audits

Each QHIN must obtain a third-party technical audit of in-scope systems on no less than an annual basis. A QHIN's annual third-party technical audit must include the following:

a) Adoption of the NIST CSF: All categories in the CSF and NIST 800-171 are required, with technical audits conducted using NIST 800-53 moderate as a reference

b) Requirements of the HIPAA Security Rule, including HIPAA security analysis (consistent with §164.308(a)(1)(ii)(A))

c) Comprehensive internet-facing penetration testing

d) Internal network vulnerability assessment

e) A review of security requirements from the Common Agreement, security related SOPs, and other security requirements as may be required by the RCE at time of assessment

f) Utilize methodologies and security controls consistent with Recognized Security Practices, as defined by Public Law No: 116-321

Refer to the SOP for more details

DRAFT SOP:
QHIN, Participant, and Subparticipant Additional Security Requirements

Feedback is requested and available until January 13, 2023

DRAFT SOP: QHIN, Participant, and Subparticipant Additional Security Requirements

Purpose:

- The SOP identifies specific **authentication**, **audit**, and **secure channel** requirements that QHINs, Participants, and Subparticipants must follow to help protect the security of TEFCA Information (TI).
- This SOP does not encompass all security concerns that apply to QHINs, Participants, and Subparticipants.
- The CA, other SOPs, and the QHIN Technical Framework (QTF) also stipulate security requirements or standards that may not be explicitly covered in this SOP.

DRAFT SOP: QHIN, Participant, and Subparticipant Additional Security Requirements

Authentication:

Each QHIN, Participant, and Subparticipant shall require that Workforce members and Individuals who are authorized users are authenticated as follows:

(i) **Workforce members** who are authorized users of systems which access TI or PHI, (including those who request TI or PHI, or request TI or PHI be sent to a third party) shall be authenticated at Authenticator Assurance Level (AAL)2 (which requires either a multi-factor authenticator or a combination of two single-factor authenticators).
When assertions are used in a federated environment to communicate authentication and attribute information to a relying party, such assertions shall be at NIST Federation Assurance Level (FAL) 2

(ii) **Individuals**. Each QHIN, Participant, and Subparticipant shall require that Individuals are authenticated at AAL2.

*"**Workforce**" means employees, volunteers, trainees, and other persons whose conduct in the performance of their work is under the direct control of the QHIN, Participant, or Subparticipant, whether or not they are paid by the QHIN, Participant or Subparticipant.*

DRAFT SOP: QHIN, Participant, and Subparticipant Additional Security Requirements

Audit:

All QHINs, Participants, and Subparticipants MUST record audit log entries of transactions conducted through their Framework Agreements which adhere to ASTM E2147-18, “Standard Specification for Audit and Disclosures Logs” as a minimum requirement.

Secure Channel:

All internet-facing connections established under a Framework Agreement shall utilize the Internet Engineering Task Force (IETF) Transport Layer Security (TLS) protocol, version 1.2 with BCP-195, or a later version of TLS, to establish a secure channel and shall be conformant with requirements specified in QTF 007, 008, 009. This will help enable the TLS-protected communication channel to operate with appropriate levels of protection and prohibit less secure methods.

Other TEFCA Security Related Resources

Other Security Related Resources

SOPs and TEFCA Resources:

- SOP: QHIN Cybersecurity Coverage
- SOP: QHIN Security Requirements for the Protection of TI Rev. 1 (updated as of May 2022)
- QHIN Technical Framework (QTF)
- QHIN Technical Trust Requirements
- List: QHIN Cybersecurity Certifications
- List: Credential Service Provider (CSP) Approval Organizations

Other Resources Under Development:

- DRAFT SOP: QHIN, Participant, and Subparticipant Additional Security Requirements
- SOP: Individual Access Service (IAS) Provider Privacy and Security Notice
- SOP: Other Security Incidents and Reportable Events

Your Comments and Questions

Thank you for your participation

carequality

carequality.org