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

Version 2.0

August 6, 2024

Applicability: QHINs, RCE

1 Common Agreement References

The requirements set forth in this Standard Operating Procedure (SOP) are for implementation, in addition to the terms and conditions found in the Framework Agreements, the Qualified Health Information Network™ (QHIN™) Technical Framework (QTF), and applicable SOPs. The Trusted Exchange Framework and Common Agreement™ (TEFCA™) Cross Reference Resource identifies which SOPs provide additional detail on specific references from the Common Agreement.

All documents cited in this SOP can be found on the Recognized Coordinating Entity® (RCE™) website.

2 SOP Definitions

Terms defined in this Section are introduced here and can be found in the TEFCA Glossary. Capitalized terms used in this SOP have the respective meanings assigned to such term in the TEFCA Glossary.

No new definitions are introduced in this SOP.

The following defined terms from the Common Agreement are repeated here for reference.

Cybersecurity Council: the council established by the RCE to enhance cybersecurity commensurate with the risks in TEFCA Exchange, as more fully set forth in an SOP.

Threat Condition: (i) a breach of a material provision of a Framework 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 the RCE, a QHIN, Participant, or Subparticipant has reason to believe will disrupt normal TEFCA Exchange, 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; or (iv) any event that could pose a risk to the interests of national security as directed by an agency of the United States government.

TEFCA Security Incident(s):

(i) An unauthorized acquisition, access, Disclosure, or Use of unencrypted TEFCA Information (TI) using TEFCA Exchange, but NOT including any of the following:

(a) Any unintentional acquisition, access, Use, or Disclosure of TI 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).

(ii) Other security events (e.g., ransomware attacks), as set forth in an SOP, that adversely affect a QHIN's, Participant's, or Subparticipant's participation in TEFCA Exchange.

3 PURPOSE

This SOP identifies specific requirements that Qualified Health Information Networks must follow to protect the security of Trusted Exchange Framework and Common Agreement Information. It also provides specific information about the Cybersecurity Council.

The Cybersecurity & Infrastructure Security Agency (CISA) has identified the Healthcare and Public Health (HPH) Sector as part of the nation's critical infrastructure, stating:

> The HPH 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.[1]

Pursuant to the Homeland Security Act of 2002, as amended, and Presidential Policy Directive 21, U.S. Department of Health and Human Services (HHS) serves as the Sector Risk Management Agency (SRMA) for the HPH Sector. This SOP aligns with the HHS Cybersecurity Strategy[2] and adopts the relevant guidance and resources made available by HHS to the HPH Sector.

[1] https://www.cisa.gov/healthcare-and-public-health-sector
[2] https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

QHINs play an important role in advancing the exchange of health and related information and, as such, have a critical role in advancing the standards for securing such information. Each QHIN must maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule with respect to all TI even if the QHIN is not a HIPAA Covered Entity or Business Associate. In addition, QHINs must further satisfy the additional requirements and standards herein that go above and beyond what is required under the HIPAA Security Rule.

4 PROCEDURE

1. Implement Appropriate Security Controls

   QHINs shall:

   a. Per Section 12.1 of the Common Agreement, Signatory shall comply with the HIPAA Security Rule as if the HIPAA Security Rule applied to Individually Identifiable Information that is TI regardless of whether Signatory is 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[3] (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).

2. 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.

   a. The RCE will maintain and publish a list of currently approved certifications and certifying bodies which meet the RCE's security certification requirements as outlined in the SOP at https://rce.sequoiaproject.org/qhin-cybersecurity-certification.

      (i) Any third-party accreditation or certification body that can demonstrate adherence to the requirements listed in the SOP may be considered for inclusion in the RCE's list of certification bodies.

[3] https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf

(ii) Certification bodies providing services which meet these requirements may also request approval to be included in the list.

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);[4]

(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.

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 this SOP. The new components or capabilities must be adopted into the assessment scope for the Designated Network's future certification/recertification efforts.

3. Annual Security Assessments

a. Per Common Agreement Section 12.1.3: Annual Security Assessments, Signatory must obtain a third-party security assessment and technical audit no less often than annually and as further described in the applicable SOP. Within thirty (30) days of completing such an annual security assessment or technical audit, Signatory must provide evidence of completion and mitigation as specified in the applicable SOP.

b. Each QHIN must obtain a third-party security assessment and technical audit of in-scope systems on no less than an annual basis to ensure that its systems are properly defended against emergent threats. In-scope systems means any system that is critical to organizational operation and/or is required to function as a QHIN, plus all new systems, components, and applications

[4] https://www.nist.gov/cyberframework

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;[5] 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.

4. Reports or Summaries of Certification Assessments & Annual Technical Audits

a. The QHIN shall provide to the RCE an appropriate report or summary of the results of its third-party certification renewal assessments and annual technical audits within thirty (30) days of the QHIN's receipt of the report.

(i) If the certification renewal assessment and/or annual technical audit identifies any unaddressed deficiencies that meet the definition of medium severity or higher per the National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS),[6] the QHIN must take appropriate action(s) to mitigate the risk(s) of any such deficiencies.

(ii) If the QHIN is able to fully remediate any such identified deficiencies within fifteen (15) days of its receipt of the certification/audit report, the QHIN must attest to full remediation of such deficiencies when the QHIN submits its report or summary report to the RCE.

(iii) If the QHIN is not able to remediate the identified deficiencies within that timeframe, it must develop and implement an appropriate Plan of Action and Milestones (POA&M) identifying the necessary activities, resources needed, responsible party/parties, reasonable mitigation efforts and/or compensating controls, and the timetable to full remediation. The QHIN must provide a copy of its POA&M to the RCE within thirty (30) days of the QHIN's receipt of the certification/audit report.

[5] https://owasp.org/www-project-top-ten/
[6] https://nvd.nist.gov/

b. Any QHIN that is required to submit a POA&M must also provide updates to the RCE or, at the RCE's direction, to the Cybersecurity Council, every thirty (30) days thereafter regarding the QHIN's progress toward completion of the milestones identified in the POA&M, until the RCE or the RCE and the Cybersecurity Council, when the Cybersecurity Council is involved, agree(s) that the deficiencies have been fully remediated or approve(s) of any partial risk acceptance with appropriate compensating controls.

c. In addition to requiring the submission of a POA&M and routine progress updates, if the RCE determines that the findings of a QHIN's certification assessment or technical audit reflect a Threat Condition, the RCE may take other appropriate actions, including, but not limited to, suspending the QHIN's participation in QHIN-to-QHIN exchange until the Threat Condition is remediated or sufficiently mitigated, as determined by the RCE.

d. Nothing in this section shall modify or replace a QHIN's notification or reporting requirements, as set forth in the Common Agreement, for any deficiency or other finding that constitutes a TEFCA Security Incident. For the avoidance of doubt, the following may still require notification pursuant to the timing and procedures noted in the Common Agreement if it falls within the definition of TEFCA Security Incident: (i) a fully remediated assessment/audit finding that does not require submission of a POA&M; and (ii) an assessment/audit finding that does require submission of a POA&M.

5. Independent Review

a. Certification bodies and third-party assessment organizations utilized by Certification bodies or QHINs must be qualified, independent third parties.

b. QHINs must attest that they have no organizational conflict of interest with the assessment organization and that the assessments are being conducted by independent third parties.

c. Assessors must be security professionals with active or current security certifications requiring ongoing credential maintenance (e.g., security assessment credentials with continuing professional education requirements such as those certifications recognized by federal agencies as minimum requirements for conducting certain security roles).

d. Third-party assessments and certification activities are subject to quality review or sampling by the certification body to ensure consistency and quality.

6. Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation

a. The RCE shall treat reports or summaries of the security assessment, POA&Ms, and any related documentation, such as milestone updates requested by the RCE or Cybersecurity Council, as Confidential Information and will not disclose them to anyone except:

   i. To the Cybersecurity Council, at the RCE's discretion;

   ii. To the Governing Council, upon recommendation of the Cybersecurity Council;

   iii. As required by law; or

   iv. To HHS Office of the National Coordinator for Health Information Technology (ONC) in accordance with the Common Agreement and any applicable SOP.

b. To the extent the RCE believes it is able to obtain appropriate guidance from the Cybersecurity Council, or the Cybersecurity Council believes it is able to obtain appropriate guidance from the Governing Council, without revealing the identity of the QHIN to which the reports or summaries of certification assessments and annual technical audits and/or the POA&Ms apply, the RCE or the Cybersecurity Council will reasonably attempt to remove or redact such identifying information.

7. Cybersecurity Council

a. Purpose: Per Section 12.1.6 of the Common Agreement, the RCE shall establish a Cybersecurity Council, which shall evaluate the cybersecurity risks to the activities conducted under the Framework Agreements and advise the RCE on ways to remediate these risks that are commensurate with such risks.

b. Composition: The RCE Chief Information Security Officer (CISO) shall serve as the Chairperson of the Cybersecurity Council and shall be a voting member of the Cybersecurity Council. The named CISO for each Designated QHIN shall be the QHIN's Representative and voting member of the Cybersecurity Council. Each QHIN shall select a CISO from among its Participants and Subparticipants to serve as a non-voting member of the Cybersecurity Council. Participant/Subparticipant Representatives shall be individuals who are affiliated, either by employment or on a contract basis, with a Participant or Subparticipant, and who have the position of CISO for that Participant or Subparticipant organization. If the Participant or Subparticipant organization is a HIPAA Business Associate or HIPAA Covered Entity and does not have a CISO, the representative may be the "Assigned Security Official" as required by the HIPAA Security Rule. The Cybersecurity Council may invite subject matter experts (SMEs) to participate in meetings to provide input on specific issues. CISOs from Candidate QHINs are considered SMEs and are invited to participate in all Cybersecurity Council meetings as non-voting members.

c. Cybersecurity Council Meetings:The Cybersecurity Council shall meet at the request of the RCE CISO, but no less than on a quarterly basis. The Chairperson is responsible for conducting all meetings in a way that promotes efficiency, transparency, and inclusiveness of all perspectives on any matter being considered. It is expected that the actions of the Cybersecurity Council will be memorialized in some manner for future reference, but the precise manner is left to the Cybersecurity Council. By way of example only, meeting minutes, meeting notes, slide decks, or recordings could all be acceptable.

d. Quorum and VotingA simple majority, 51%, of the Cybersecurity Council members present shall constitute a quorum. Cybersecurity Council members must be present in-person or virtually to constitute a quorum. A simple majority, 51%, of the members present and voting once a quorum has been established shall constitute approval of an item by the Cybersecurity Council. Additional details concerning Quorum and Voting are specified in the approved Cybersecurity Council charter.

e. Conflicts of Interest: Individuals who serve on the Cybersecurity Council shall actively avoid any activities that could create an actual or a perceived conflict of interest with their service on the Cybersecurity Council. Please refer to the Conflict of Interest SOP for additional detail.

8. QHIN CISO

Signatory's CISO shall have responsibility for the overall security posture of Signatory's entity with respect to their participation in TEFCA. This includes technical, administrative, and physical security safeguards and documentation thereof for Signatory's organization. This role may be subcontracted, but the CISO's overall responsibilities must encompass the spectrum of security related activities for the QHIN as an organizational entity, and not be limited to the activities of a third-party such as a platform vendor.

3 VERSION HISTORY

Version #	Revision Date	Section #(s) of Update
1.0	February 2022	N/A
1.1	May 2022	Part 3, Sections 1 and 2
1.2	December 2023	Part 3 Sections: 1.b.(i), 2.a., 3.c., 4.a., 5.d., 6. Added Part 3 Sections: 1.c., 7.
2.0	June 2024	Updated throughout to reflect CA 2.0 and provide clarity and more specificity. Updated HIPAA reference in 3.2.b.(iii) and 3.3.b.(iii). Added section 3.2.d. and updated 3.3.b. to accommodate post-certification changes to the network. Updated 3.7.b to reflect changes to the Cybersecurity Council Charter