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

Rev. 1 (updated as of May 2022)

Applicability: QHINs, RCE

1 COMMON AGREEMENT REFERENCES

CA Section 12.1.2:

Cybersecurity Certification. Signatory shall 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.

CA 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. Signatory must also provide evidence of compliance with this section and, if applicable, of appropriate mitigation efforts in response to the findings of the security assessment and/or technical audit within thirty (30) days to the RCE as specified in the SOP.

CA Section 12.1.5:

Security Resource Support to Participants. Signatory shall make available to its Participants: (i) security resources and guidance regarding the protection of TI applicable to the Participants' participation in the QHIN under the applicable Framework Agreement; and (ii) information and resources that the RCE or Security Council makes available to Signatory related to promotion and enhancement of the security of TI under the Framework Agreements.

CA Section 12.1.6:

Chief Information Security Officer. The RCE shall designate a person to serve as the Chief Information Security Officer (CISO) for activities conducted under the Framework Agreements. This may be either an employee or independent contractor of the RCE. The RCE's CISO will be responsible for monitoring and maintaining the overall security posture of activities conducted under the Framework Agreements and making recommendations to all QHINs regarding changes to baseline security practices required to address changes to the threat landscape. Signatory agrees that it, and not the RCE, is ultimately responsible for the security posture of Signatory's network and the activities conducted by Signatory under the Participant-QHIN Agreements to which Signatory is a party, as well as the Participant-Subparticipant Agreements its Participants enter into and all Downstream Subparticipant Agreements that its Participants' Subparticipants enter into. Signatory shall also designate a person to serve as its CISO for purposes of Signatory's participation in QHIN-to-QHIN exchange. The RCE shall establish a Cybersecurity Council to enhance cybersecurity commensurate with the risks of the activities conducted under the Framework Agreements as more fully set forth in an SOP.

Capitalized terms used below without definitions shall have the respective meanings assigned to such terms in the Common Agreement.

2 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.

3 STANDARD

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.[1]

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 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. 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 certifying bodies which meet the RCE's security certification requirements as outlined in the SOP.

        (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.

[1] https://www.cisa.gov/healthcare-and-public-health-sector (accessed April 28, 2022).

(ii) Interested parties should refer to the official RCE-published list of currently approved certifications available at https://rce.sequoiaproject.org/qhin-cybersecurity-certification.

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

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

(i) 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;

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

(iii) Verify Common Agreement requirements for technical audits and assessments are met.

2. Annual Technical Audits – Each QHIN must obtain a third-party 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. A QHIN's annual third-party technical audit must, at a minimum, include the following:

a. Adoption of the NIST CSF, specifically 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, including review of the results of vulnerability scans and review of patch and vulnerability management records of its systems and applications

e. Include 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; and

f. Utilize methodologies and security controls consistent with Recognized Security Practices, as defined by Public Law No: 116-321[2] (e.g., NIST Special Publications, CMS Guidelines, ONC HIPAA Security Risk Assessment (SRA) Tool, etc.)

3. Reports or Summaries of Certification Assessments & Annual Technical Audits – The QHIN shall provide to the RCE an appropriate report or summary of the results of its certification renewal assessments and annual technical audits within thirty (30) days of the QHIN's receipt of the report. If the certification renewal assessment and/or annual technical audit identifies any unaddressed deficiencies that meet the definition of moderate impact or high impact, the QHIN must take appropriate action(s) to mitigate the risk(s) of any such deficiencies. 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. 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 fifteen (15) days of the QHIN's receipt of the certification/audit report.

a. Any QHIN that is required under Section 3 of this SOP 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.

b. 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, as such term is defined in the Common Agreement, 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.

[2] Pub.L. 116-321 (January 5, 2021), *available at* https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.

c. Nothing in this section shall modify or replace a QHIN's notification requirements, as set forth in the Common Agreement, for any deficiency or other finding that constitutes a TEFCA Security Incident, as such term is defined by the Common Agreement. 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.

4. Independent Review – Certification bodies and third-party assessment organizations utilized by Certification bodies or QHINs must be qualified, independent third parties.

   a. Organizations conducting assessments must attest (in the assessment report) to having no organizational conflicts of interest with the certification body or the organization being assessed, and

   b. 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. Examples include certifications recognized by federal agencies as minimum requirements for conducting certain security roles).

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

5. Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation – 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:

   a. To the Cybersecurity Council, at the RCE's discretion;
   b. To the Governing Council, upon recommendation of the Cybersecurity Council;
   c. As required by law; or
   d. As requested by ONC in furtherance of the RCE's obligations under the Cooperative Agreement.

   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.

6. Cybersecurity Council – 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. 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 QHIN Caucus shall select five CISOs from among the QHINs to serve as voting members of the Cybersecurity Council. The Participant/Subparticipant Caucus shall select five CISOs from among the Participants and Subparticipants to serve as non-voting members of the Cybersecurity Council. The Cybersecurity Council shall meet at the request of the RCE CISO, but no less than on a quarterly basis. The Cybersecurity Council may invite subject-matter experts to participate in meetings to provide input on specific issues.

   a. Cybersecurity Council Meetings. Meetings of the Cybersecurity Council shall be conducted in an organized and orderly manner. 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.

   b. Quorum and Voting. A simple majority, 51%, of the Cybersecurity Council members 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.

   c. 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.

This program is supported by the Office of the National Coordinator for Health Information Technology (ONC) of the U.S. Department of Health and Human Services (HHS) under grant number 90AX0026, Trusted Exchange Framework and Common Agreement - Recognized Coordinating Entity (RCE) Cooperative Agreement Program, in the amount of $2,919,000 with 100 percent funded by ONC/HHS. This information or content and conclusions are those of the author and should not be construed as the official position or policy of, nor should any endorsements be inferred by ONC, HHS or the U.S. Government.