ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Standard Operating Procedure (SOP): QHIN, Participant, and Subparticipant Additional Security Requirements

Applicability: QHINs, Participants, Subparticipants

1 Common Agreement References

The specifications set forth in this Standard Operating Procedure (SOP) are required for implementation in addition to the mandatory flow-down terms and conditions found in the Common Agreement (CA) and in accordance with the CA Section 12.1.4.

Capitalized terms used below without definitions shall have their respective meanings assigned to such terms in the Common Agreement and the QHIN Technical Framework.

2 Purpose

This 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.

3 Definitions

"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.

4 Standard

Per the Common Agreement Section 12.1.4 Participants and Subparticipants (Required Flow-Down): Signatory shall require in its Participant-QHIN Agreements that its Participants implement and maintain, and require their Subparticipants to implement and maintain, appropriate security controls for TI that are commensurate with risks to the confidentiality, integrity, and/or availability of the TI. If any Participant or Subparticipant is a Non-HIPAA-Entity (NHE), it shall be required to comply with the HIPAA Security Rule provisions with respect to all Individually Identifiable information that the Participant or Subparticipant reasonably believes is TI as if such information were Protected Health Information and the Participant or Subparticipant were a Covered Entity or Business Associate. Signatory shall further require that its Participants implement and maintain, and that its Participants require their Subparticipants to implement and maintain, any additional security requirements that may be set forth in an SOP applicable to

Participants and Subparticipants. Such compliance shall be enforced as part of the Participants' and Subparticipants' obligations pursuant to the Framework Agreements.

This SOP defines additional specificity for all Workforce members of QHINs, Participants, Subparticipants, and their subcontractors for user authentication, system security event logging, and secure channels which communicate TEFCA information.

Other security requirements specific to QHINs are contained in the SOP: QHIN Security Requirements for the Protection of TI.

Additional technical security requirements applicable to QHINs and Participants (where specified) are contained in the QTF.

Specific requirements for Individual Access Services (IAS) Providers for Individual identity verification are contained in the SOP: Individual Access Services (IAS) Implementation.

5 Procedure

Authentication. Each QHIN, Participant, and Subparticipant shall require that Workforce members and Individuals who are authorized users are authenticated in accordance with the following requirements:

(i) Workforce members. Each QHIN, Participant, and Subparticipant shall require that Workforce members who are authorized users of systems which access TI or Protected Health Information (PHI), (including those who request TI or PHI, or request TI or PHI be sent to a third party) be authenticated at Authenticator Assurance Level (AAL) 2[1]. Note that for AAL2, authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators. NIST SP 800-63B describes permitted authenticator types [2] for AAL2. 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[3].

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

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[2] See NIST SP800-63B for AAL2 types: https://pages.nist.gov/800-63-3/sp800-63b.html#aal2types
[3] See NIST SP800-63C for FAL2: https://pages.nist.gov/800-63-3/sp800-63c.html#fal

Audit. All QHINs, Participants, and Subparticipants MUST record audit log entries of transactions conducted through their Framework Agreements which adhere to ASTM E2147-18[4], "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[5], version 1.2 with BCP-195[6], 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.

[4] ASTM E2147 – 18 *Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems* – available at https://www.astm.org/e2147-18.html

[5] Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246) is available at: https://tools.ietf.org/html/rfc5246 and The Transport Layer Security (TLS) Protocol Version 1.3 (IETF RFC 8446) is available at https://tools.ietf.org/html/rfc8446

[6] *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* (IETF BCP 195) - available at: https://tools.ietf.org/html/bcp195

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 $5,101,000 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.