ONC TEFCA RECOGNIZED COORDINATING ENTITY

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

Version 1.0

January 17, 2025

Applicability: QHINs, Participants, Subparticipants

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.

Security requirements specific to QHINs are contained in Section 12 of the Common Agreement and in the QHIN Security Requirements for the Protection of TEFCA Information SOP.

General security requirements for Participants and Subparticipants are contained in Section 8 of the Participant/Subparticipant Terms of Participation (ToP).

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

Security requirements specific to Individual Access Services (IAS) Providers are contained in the ToP and in the Individual Access Services (IAS) Implementation SOP.

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.

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

Individual: has the meaning assigned to such term at 45 CFR § 171.202(a)(2).

Workforce Member(s): any employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

3 PURPOSE

This SOP establishes additional security requirements that QHINs, Participants, and Subparticipants must implement to help protect the security of TEFCA Information (TI). This SOP does not encompass all security requirements that apply to QHINs, Participants, and Subparticipants. The CA, ToP, other SOPs, and the QHIN Technical Framework (QTF) also stipulate security requirements and/or standards that may not be explicitly covered in this SOP.

Nothing in this SOP supersedes, modifies, or otherwise alters Applicable Law.

4 PROCEDURE

4.1 Assigned Security Official

Participant/Subparticipant shall appoint an assigned security official, such as a Chief Information Security Officer (CISO) or other individual with executive-level responsibility for the organization's information security. If the Participant/Subparticipant is a HIPAA Covered Entity or Business Associate, the Assigned Security Official may be the same individual as required per 45 CFR 164.308(a)(2)[1].

Timeline to adopt: This requirement is effective as of the publication date of this SOP.

4.2 Authentication

4.2.1 Authentication for Individuals and Workforce Members

Each QHIN, Participant, and Subparticipant ***should*** require that Individuals and Workforce Members who are authorized users of systems which access or process TI or Protected Health Information (PHI), (including those who request TI or PHI, or request TI or PHI be sent to a third party) or which are otherwise used for health information exchange, be authenticated at Authenticator Assurance Level 2[2] (AAL2) for all Remote Access[3] and for all Privileged User[4] access (such as system administrator accounts or other accounts used to perform security-relevant functions).

[1] https://www.ecfr.gov/current/title-45/part-164/section-164.308#p-164.308(a)(2)
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[3] As defined by NIST, remote access is access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). See https://csrc.nist.gov/glossary/term/remote_access.
[4] As defined by NIST, a privileged user is a user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. See https://csrc.nist.gov/glossary/term/privileged_user.

Additionally, AAL2 ***should*** be implemented for access to TI or PHI, or to systems used for health information exchange originating **from an internal system** (within the organization's controlled network) **to a remote system** (outside the organization's control) **or between remote systems**.

For the avoidance of doubt, AAL2 ***should*** be implemented for:

(a) ***Remote Access*** to TI, PHI, and/or internal systems used for health information exchange; and

(b) ***Privileged User*** access to TI and/or PHI, and/or systems used for health information exchange.

The following are examples of when AAL2 standards for authentication are/are not applicable per this SOP:

- Example 1: A medical practitioner consulting with patients while on-site within their provider organization's facility *would not* be required by this SOP to authenticate to AAL2 standards for each access. This is because their access is not Remote Access and their user account is not a Privileged User account.

- Example 2: A medical practitioner accessing an externally hosted Electronic Health Record (EHR) system from within their organization's facility to query for health information *should* be authenticated to AAL2 standards under this SOP. This is because their EHR system is controlled by an external third party.

- Example 3: A system administrator accessing a server used for TEFCA Exchange who logs in with an administrator account *should* be required to authenticate to AAL2 standards for such access. This is because the access is using a Privileged User account.

- Example 4: A medical practitioner working from home who logs into their organization's network or directly accesses their organization's EHR system to query for information *should* authenticate to AAL2 standards. This is because their access is Remote Access.

- Example 5: A patient accessing their patient portal for the purposes of viewing their own health information *would not* be required by this SOP to be authenticated to AAL2 standards. This is because AAL2 standards in this SOP are not mandatory.

Note: An Individual accessing their health information through a portal or app that initiates an IAS request *is* required to authenticate to AAL2 standards as specified in Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS).

4.2.2 Re-authentication[5]

Periodic reauthentication of subscriber sessions for overall timeouts and inactivity timeouts ***should*** be performed as described in the Reauthentication Requirements for AAL2 as described in NIST SP800-63B-4[6] (draft), which is summarized below:

- An ***overall timeout*** limits the duration of an authenticated session to a specific period following authentication or a previous reauthentication. Per Sec. 5.2 of NIST SP800-63B-4 (draft), an overall timeout ***should*** be no more than ***24 hours*** at AAL2.

- An ***inactivity timeout*** terminates a session without activity from the subscriber for a specific period. Per Sec. 5.2 of NIST SP800-63B-4 (draft), the inactivity timeout ***should*** be no more than ***1 hour***.

- When either timeout expires, the session is terminated.

4.2.3 Federation

When assertions are used in a federated environment to communicate authentication and attribute information to a relying party, such assertions must be at NIST Federation Assurance Level (FAL) 2.[7]

4.3 Audit

All QHINs, Participants, and Subparticipants MUST record audit log entries of transactions conducted through their Framework Agreements which adhere to the same audit standard as required for Certified Health IT, as described in 45 CFR 170.315(d)(2), *Auditable events and tamper resistance*.[8] This includes the requirement for an audit log to record the information specified in sections 7.1.1, 7.1.2, and 7.1.6 through 7.1.9 of ASTM E2147-18, *Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*, approved May 1, 2018,[9] and changes to user privileges when health IT is in use.

Timeline to adopt: This requirement shall be implemented within six (6) months of the SOP publication date.

[5] These requirements align with the second public draft of NIST SP 800-63B r4: https://pages.nist.gov/800-63-4/sp800-63b.html#aal2reauth.
[6] NIST SP 800-63B r4 public draft: https://pages.nist.gov/800-63-4/sp800-63b.html.
[7] See NIST SP800-63C for FAL2: https://pages.nist.gov/800-63-3/sp800-63c.html#fal.
[8] https://www.ecfr.gov/current/title-45/part-170/section-170.315#p-170.315(d)(2)
[9] https://archive.org/details/gov.law.astm.E2147.18/page/n5/mode/1up

4.4 Secure Channel

All internet-facing connections established under a Framework Agreement shall utilize the Internet Engineering Task Force (IETF) Transport Layer Security (TLS) protocol,[10] version 1.2 with BCP-195,[11] or a later version of TLS, as further specified in the Secure Channel requirements of the QTF.[12] This will help enable the TLS-protected communication channel to operate with appropriate levels of protection and prohibit less secure methods.

Timeline to adopt: This requirement shall be implemented within six (6) months of the SOP publication date.

4.5 Cybersecurity Performance Goals

The U.S. Department of Health and Human Services (HHS) published Healthcare and Public Health Sector (HPH) Cybersecurity Performance Goals (CPGs)[13] to "help healthcare organizations prioritize implementation of high-impact cybersecurity practices". The CPGs are categorized into Essential and Enhanced CPGs. While voluntary, these CPGs help strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. All entities participating in TEFCA Exchange are strongly encouraged to review and adopt the Essential CPGs, and where appropriate, the Enhanced CPGs, for all critical systems and systems which permit access to health information.

Timeline to adopt: There is no requirement to formally adopt the HPH Cybersecurity Goals. To the extent that any of the HPH Cybersecurity Goals are already required by applicable law or through other policy (such as TEFCA SOPs) then the requirement from such law or policy shall prevail.

[10] 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.
[11] 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.
[12] https://rce.sequoiaproject.org/wp-content/uploads/2024/07/QTF-v2_508.pdf
[13] https://hphcyber.hhs.gov/performance-goals.html

5 VERSION HISTORY

Version	Revision Date	Section #(s) of Update
Draft 1.0	December 2022	All sections: First public draft
1.0	January 17, 2025	All sections: First public release