eHealth Exchange™

Pat Russell, Director Policy and Governance
Eric Heflin, Consultant

eHealth Exchange™

TEFCA Updates

February 11, 2025

Updates TEFCA Governance SOP

Pat Russell

eHealth Exchange™

The TEFCA Governance SOP Updates

Applies to: QHINs, Participants and Subparticipants
https://rce.sequoiaproject.org/wp-content/uploads/2025/01/TEFCA-Governance-SOP-2024-1.10.25-final-508.pdf

Purpose: The SOP provides the specifics for the formation, composition, responsibilities and terms of the Governing Council, QHIN Caucus, and Participant/Subparticipant Caucus, and sets out the way in which Advisory Groups will be established and the general rules that govern the activity of an Advisory Group

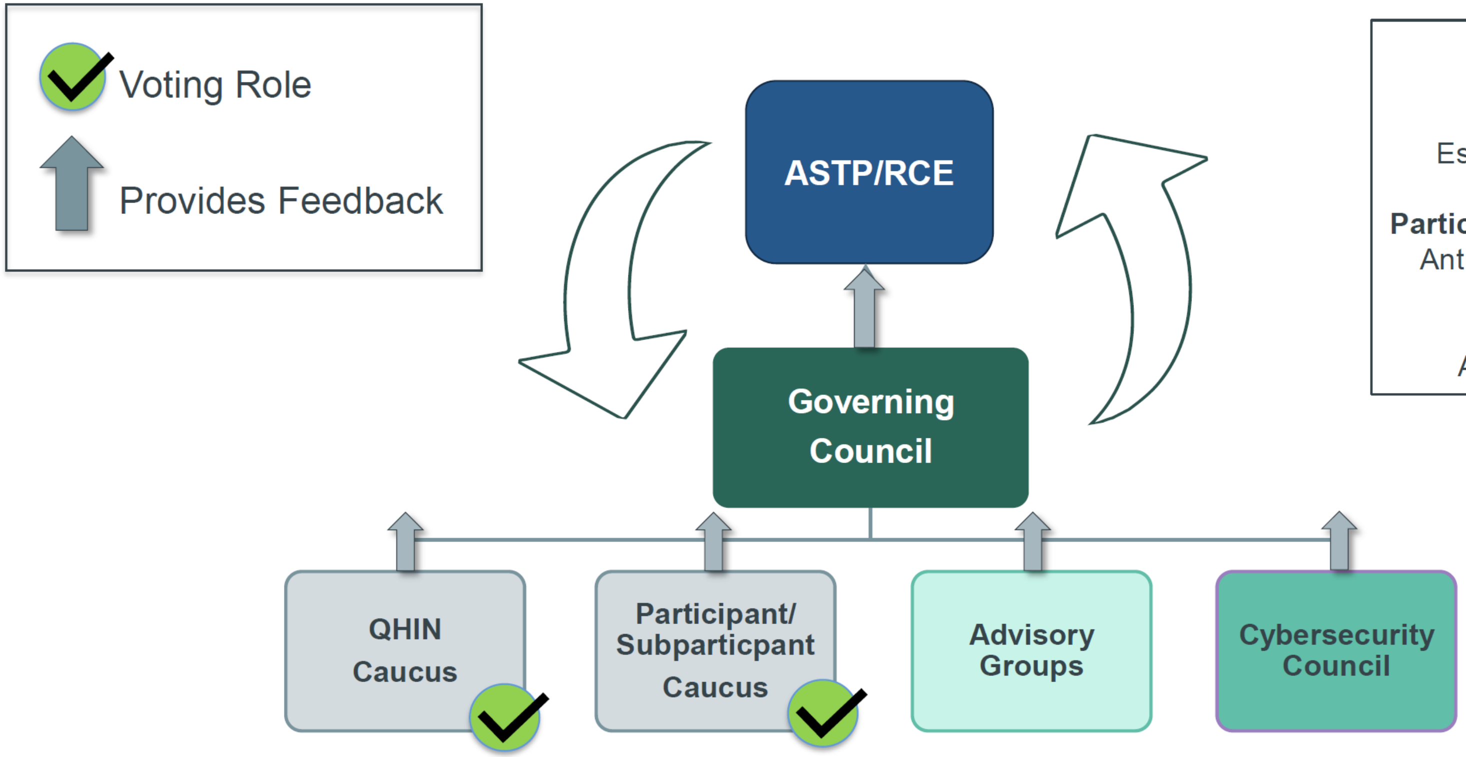
Current: Transitioning to Permanent Governance

January 2024 – Transitional Council was formed as per the Common Agreement

The Transitional Council was to be in place for 1 year

February 2025 – Governing Council expected to be formed

TEFCA Governance Roles and Voting Responsibilities



✓ Voting Role

⬆ Provides Feedback

ASTP/RCE

Governing Council

QHIN Caucus ✓

Participant/ Subparticpant Caucus ✓

Advisory Groups

Cybersecurity Council

Dates

QHIN Caucus
Established January 10, 2025

Participant/Subparticipant Caucus
Anticipated by January 31, 2025

Governing Council
Anticipated February 2025

Image from *TEFCA RCE Monthly Informational Call* materials, Jan. 21, 2025

Policies Establishing Governance

Common Agreement

The RCE shall establish a Transitional Council and then a Governing Council which will be responsible for serving as a resource to the RCE and a forum for orderly and civil discussion of any issues affecting TEFCA Exchange or other issues that may arise under the Common Agreement.

The formation, composition, responsibilities, and duration of the Transitional Council and Governing Council shall be set forth in an SOP(s)

TEFCA Governance SOP

4.1 Responsibilities
4.2 Member Expectations
4.3 Composition & Appt
4.4 Leadership
4.5 Quorum & Voting
4.6 Terms
4.7 Suspension
4.8 Removal
4.9 Vacancies
4.10 No Compensation
4.11 Conflict of Interest
4.12 Advisory Groups

Charter

Each Governance Body will create a charter to include additional details not already described in the Common Agreement and the SOP, including but not limited to:

- Schedule
- Composition, including delegates/proxies
- Appointment (i.e., nominating committees)

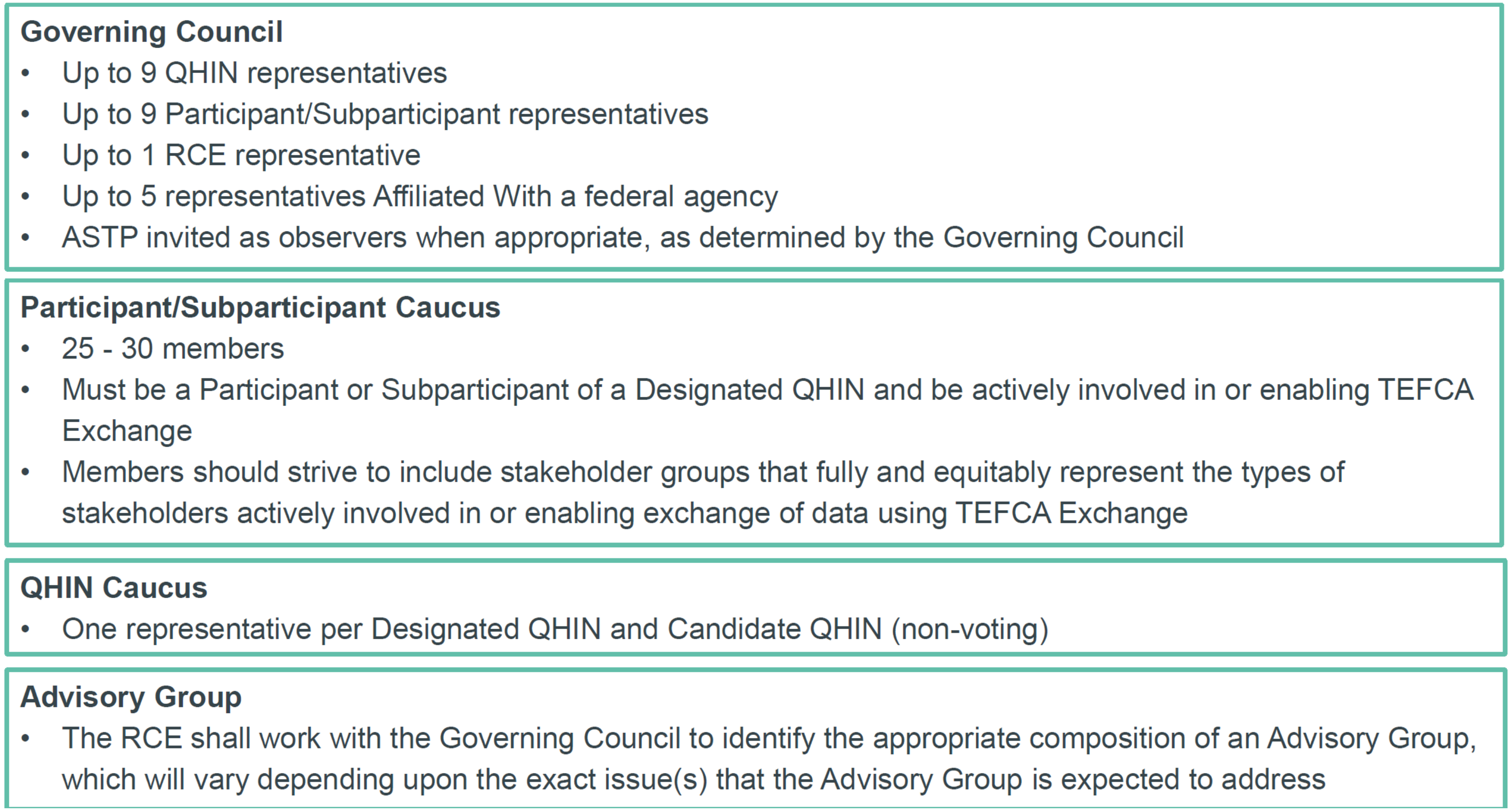
Image from *TEFCA RCE Monthly Informational Call* materials, Jan. 21, 2025

TEFCA Governance SOP – New Definitions

Affiliated With: an individual is affiliated with a QHIN, Participant, or Subparticipant if such individual is an owner, director, officer, employee, contractor, or agent of such QHIN, Participant, or Subparticipant

Governance Body(ies): The Governing Council, the QHIN Caucus, and/or the Participant/Subparticipant Caucus.

Composition of each Governing Body



Governing Council

- Up to 9 QHIN representatives
- Up to 9 Participant/Subparticipant representatives
- Up to 1 RCE representative
- Up to 5 representatives Affiliated With a federal agency
- ASTP invited as observers when appropriate, as determined by the Governing Council

Participant/Subparticipant Caucus

- 25 - 30 members
- Must be a Participant or Subparticipant of a Designated QHIN and be actively involved in or enabling TEFCA Exchange
- Members should strive to include stakeholder groups that fully and equitably represent the types of stakeholders actively involved in or enabling exchange of data using TEFCA Exchange

QHIN Caucus

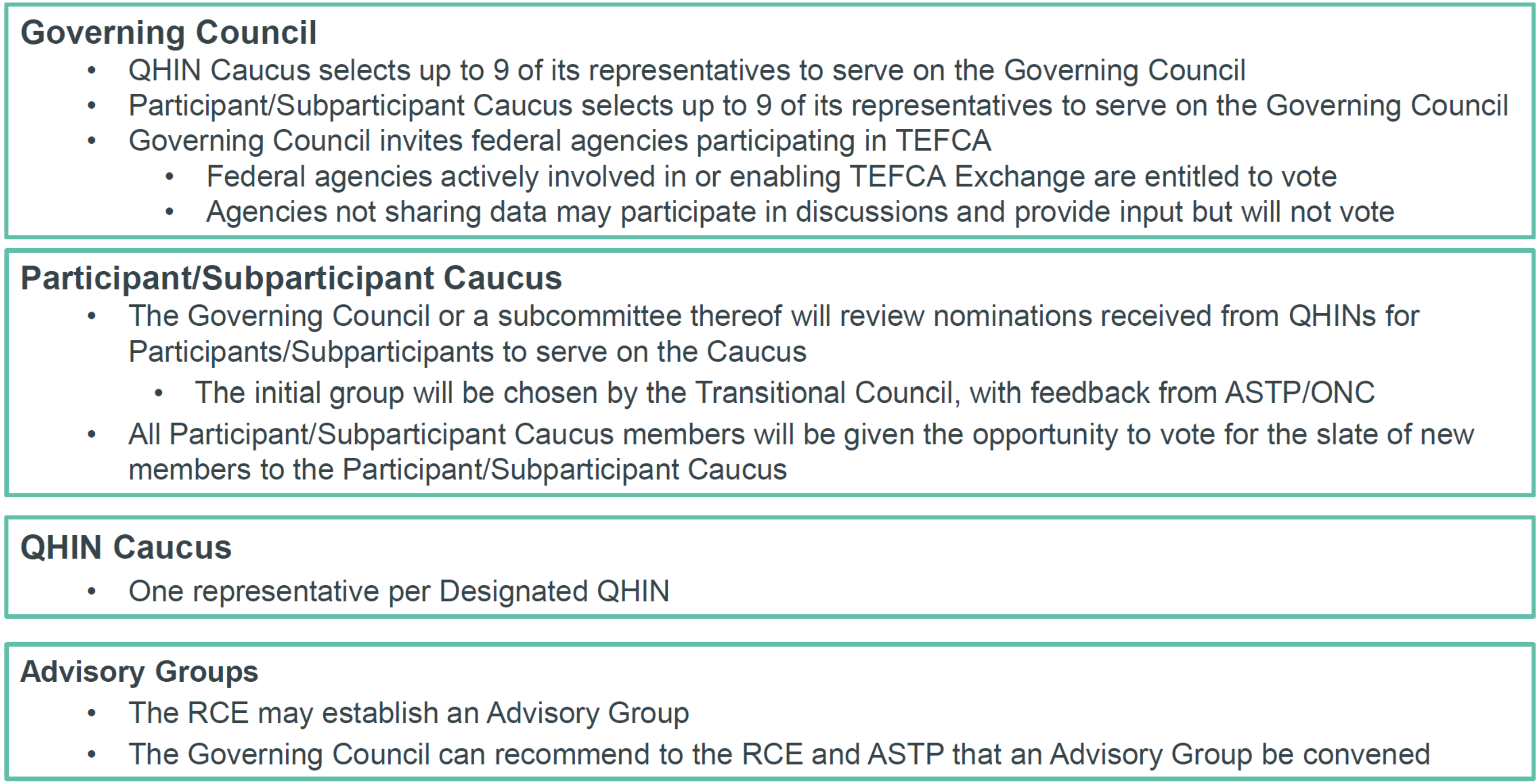
- One representative per Designated QHIN and Candidate QHIN (non-voting)

Advisory Group

- The RCE shall work with the Governing Council to identify the appropriate composition of an Advisory Group, which will vary depending upon the exact issue(s) that the Advisory Group is expected to address

Image from *TEFCA RCE Monthly Informational Call* materials, Jan. 21, 2025

Appointment to each Governing Body



Governing Council

- QHIN Caucus selects up to 9 of its representatives to serve on the Governing Council
- Participant/Subparticipant Caucus selects up to 9 of its representatives to serve on the Governing Council
- Governing Council invites federal agencies participating in TEFCA
  - Federal agencies actively involved in or enabling TEFCA Exchange are entitled to vote
  - Agencies not sharing data may participate in discussions and provide input but will not vote

Participant/Subparticipant Caucus

- The Governing Council or a subcommittee thereof will review nominations received from QHINs for Participants/Subparticipants to serve on the Caucus
  - The initial group will be chosen by the Transitional Council, with feedback from ASTP/ONC
- All Participant/Subparticipant Caucus members will be given the opportunity to vote for the slate of new members to the Participant/Subparticipant Caucus

QHIN Caucus

- One representative per Designated QHIN

Advisory Groups

- The RCE may establish an Advisory Group
- The Governing Council can recommend to the RCE and ASTP that an Advisory Group be convened

Image from *TEFCA RCE Monthly Informational Call* materials, Jan. 21, 2025

Advisory Groups

Purpose: Common Agreement (v2.1), Section 3.5, states:

The RCE, in consultation with the Transitional or Governing Council (as applicable) and ONC, may establish Advisory Groups for purposes of seeking input from distinct groups of stakeholders that are parties to or affected by TEFCA Exchange activities to better inform the governance process, provide input on certain topics, and promote inclusivity. The process for establishing Advisory Groups and selecting members is set forth in the applicable SOP.

Composition: Section 4.12.3 of the TEFCA Governance SOP, in part, states:

The RCE shall work with the Governing Council to identify the appropriate composition of an Advisory Group, which will vary depending upon the exact issue(s) that the Advisory Group is expected to address. The group is to be diverse, have the appropriate expertise, availability and be objective.

Additional Elements of the SOP

Includes procedures for:

- ✓ Quorum and Voting
- ✓ Terms of Governing Body Representatives
- ✓ Suspension and Removal
- ✓ Vacancies

Updates to Exchange Purposes (XPs) SOP 4.0

Pat Russell

eHealth Exchange™

Updates to XP SOP 4.0

Applies to: QHINs, Participants, Subparticipants

https://rce.sequoiaproject.org/wp-content/uploads/2025/01/SOP-Exchange-Purposes_CA-v2_v4-508.pdf

Purpose: The Common Agreement permits QHINs, Participants, and Subparticipants to utilize TEFCA Exchange only for authorized XPs. This SOP defines the authorized XPs and identifies any XPs for which a Response is required pursuant to the Common Agreement, as well as when fees are prohibited or permitted. More information on implementation of each XP may be found in an XP implementation SOP, as applicable.

The Purpose of the Update: Provide greater flexibility for QHINs and other TEFCA connected entities to use XPs that are currently optional for response, such as Health Care Operations, Payment or Government Benefits Determination. All other requirements are maintained. Added new Section 4.7.

Updates to XP SOP 4.0, continued

New Section 4.7:

- ✓ For all XP codes that require a Response pursuant to the Exchange Purposes SOP, the non-discrimination provisions in Section 6.2.2 of the Common Agreement and Section 2.2.2 of the Participant/Subparticipant Terms of Participation (ToP) shall apply.

- ✓ For each Non-Required XP Code, Section 6.2.2 of the Common Agreement and Section 2.2.2 of the ToP shall not apply to TEFCA Exchange conducted for such Non-Required XP Code. For these Non-Required XP Codes, QHINs, Participants, and Subparticipants MAY determine their own exchange partners. For the avoidance of doubt, TEFCA Exchange conducted for any Non-Required XP Code remains subject to all other applicable provisions of the Framework Agreements, SOPs, and QTF.

NEW TEFCA SOP

QHIN, Participant, and Subparticipant Additional Security Requirements

Eric Heflin

eHealth Exchange™

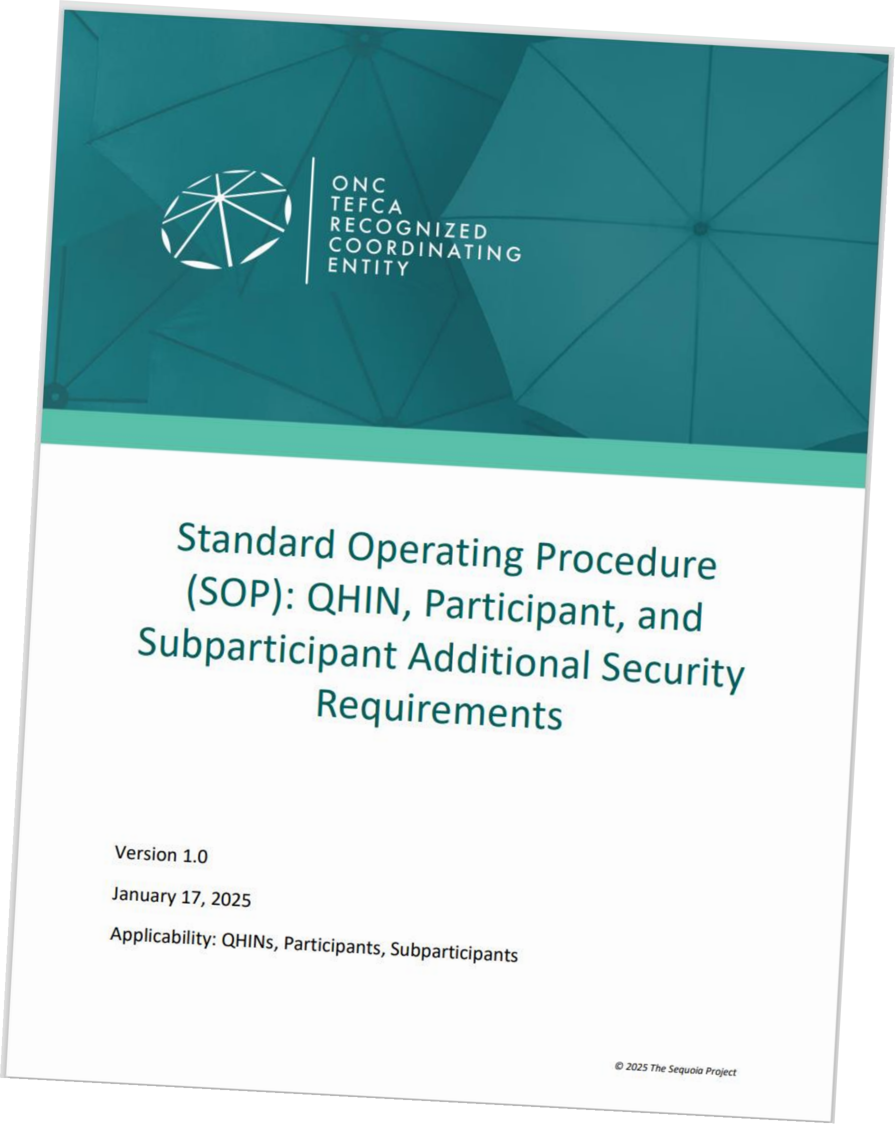
NEW TEFCA SOP - QHIN, Participant, and Subparticipant Additional Security Requirements

Applies to: QHINs, Participants, Subparticipants

https://rce.sequoiaproject.org/wp-content/uploads/2025/01/SOP-QHIN-Participant-and-Subparticipant-Additional-Security-Requirements-508.pdf

Dated: Jan 17, 2025

Purpose: “This SOP establishes additional security requirements that QHINs, Participants, and Subparticipants must implement to help protect the security of TEFCA Information (TI).”



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

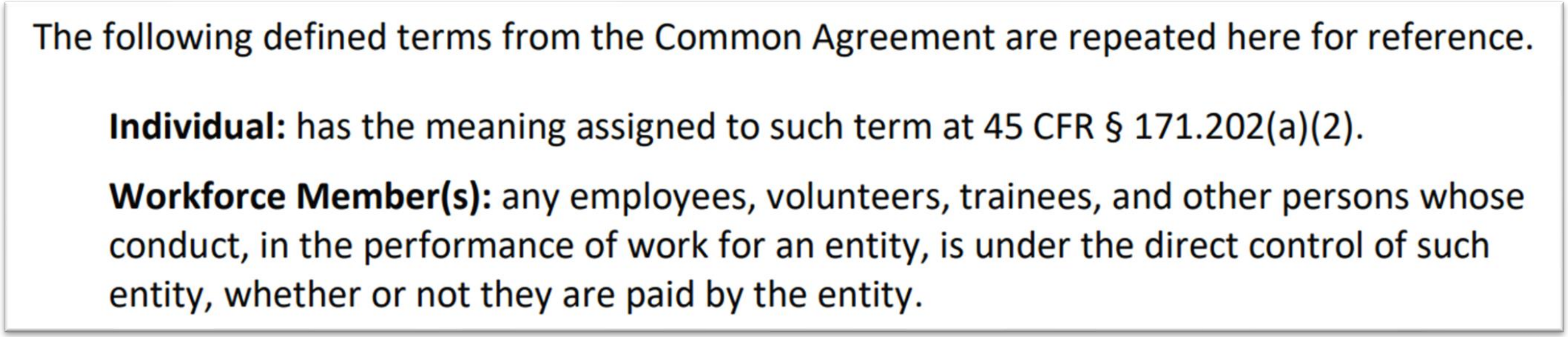
© 2025 The Sequoia Project

New Component of a Suite of Related Security Requirements

- Directly references:
  - QHINs security requirements 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.
  - See: SOP: QHIN, Participant, and Subparticipant Additional Security Requirements, p. 3

Terms

- Introduces no new defined terms
- Cites the following existing terms:

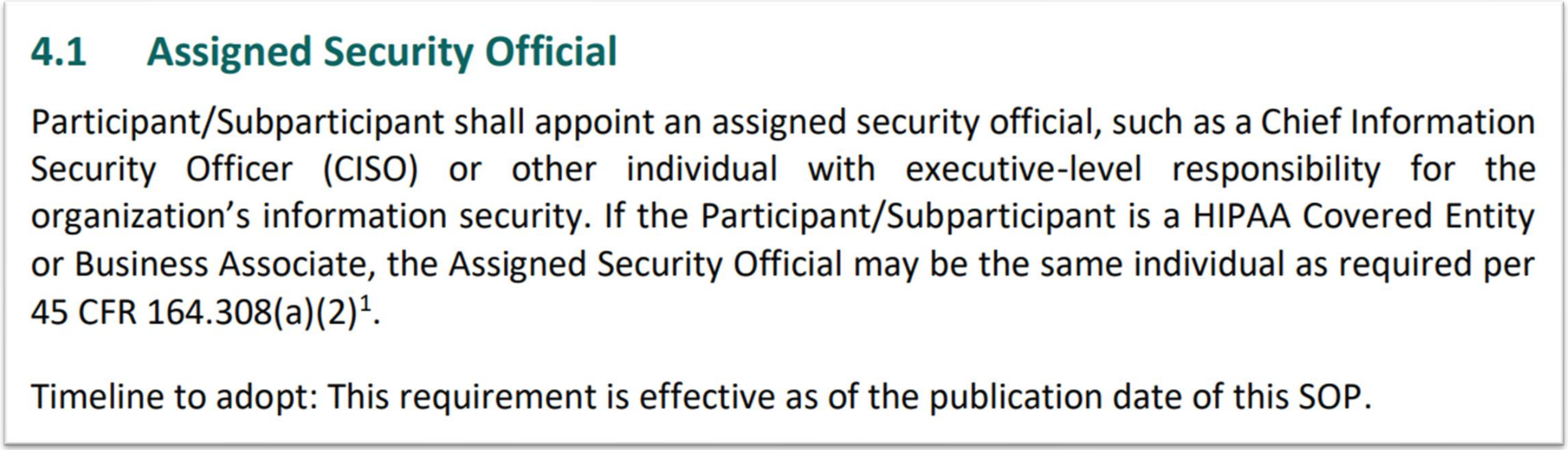


The following defined terms from the Common Agreement are repeated here for reference.

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.

Assigned Security Official



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].

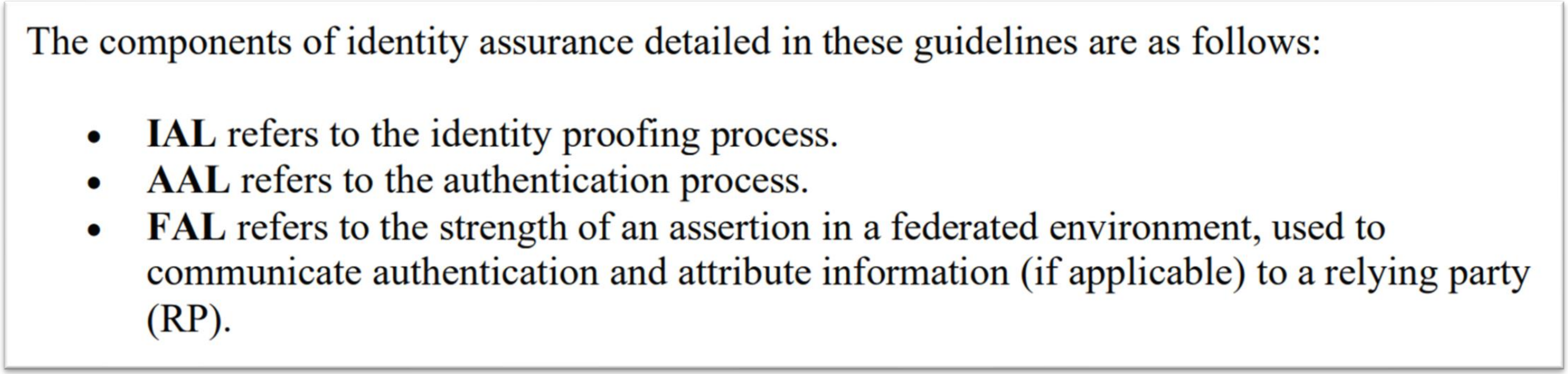
Timeline to adopt: This requirement is effective as of the publication date of this SOP.

Base Standards

- NIST SP 800-63-3 (final release)
  - Identify Assurance Levels
  - Authorization Assurance Levels
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- NIST SP 800-63b-R4 (second public draft)
  - https://pages.nist.gov/800-63-4/sp800-63b.html#aal2reauth
- NIST SP 800-63c (final release)
  - Federated Assurance Levels
  - https://pages.nist.gov/800-63-3/sp800-63c.html#fal
- Other NIST Defined Terms
  - Remote Access https://csrc.nist.gov/glossary/term/remote_access
  - Privileged User https://csrc.nist.gov/glossary/term/privileged_user

Background (from NIST)

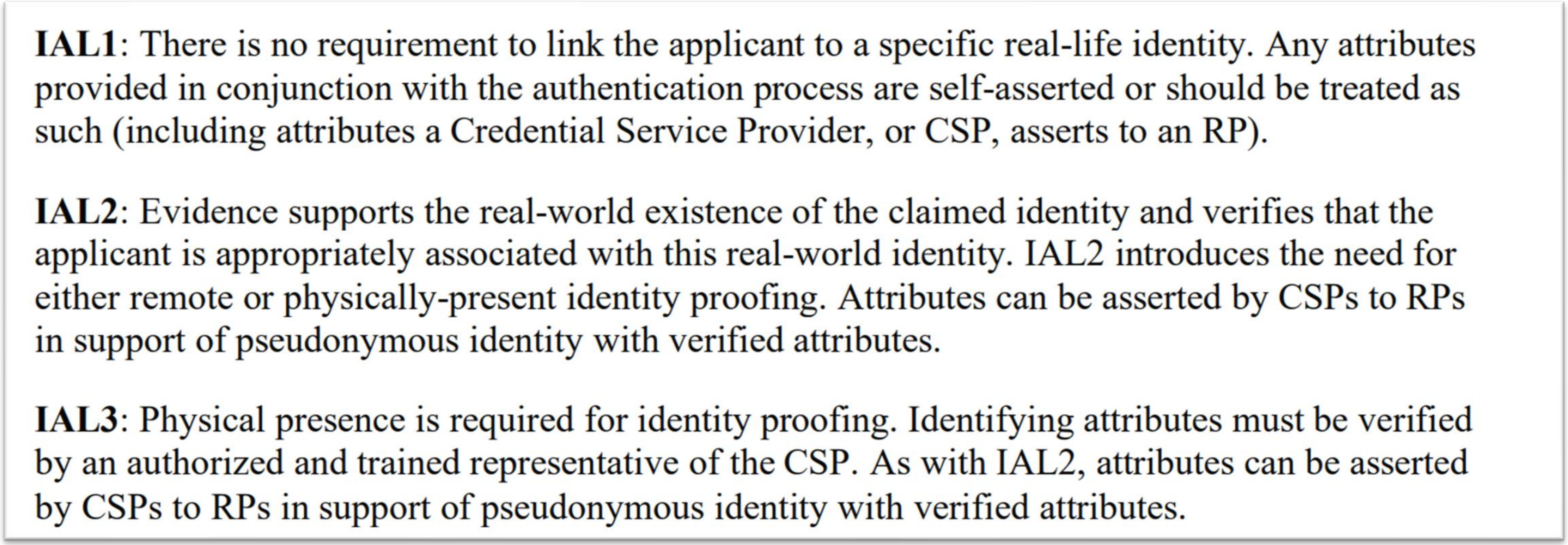
- NIST SP 800-63-3 Defines:



The components of identity assurance detailed in these guidelines are as follows:

- **IAL** refers to the identity proofing process.
- **AAL** refers to the authentication process.
- **FAL** refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

Identity Assurance Levels

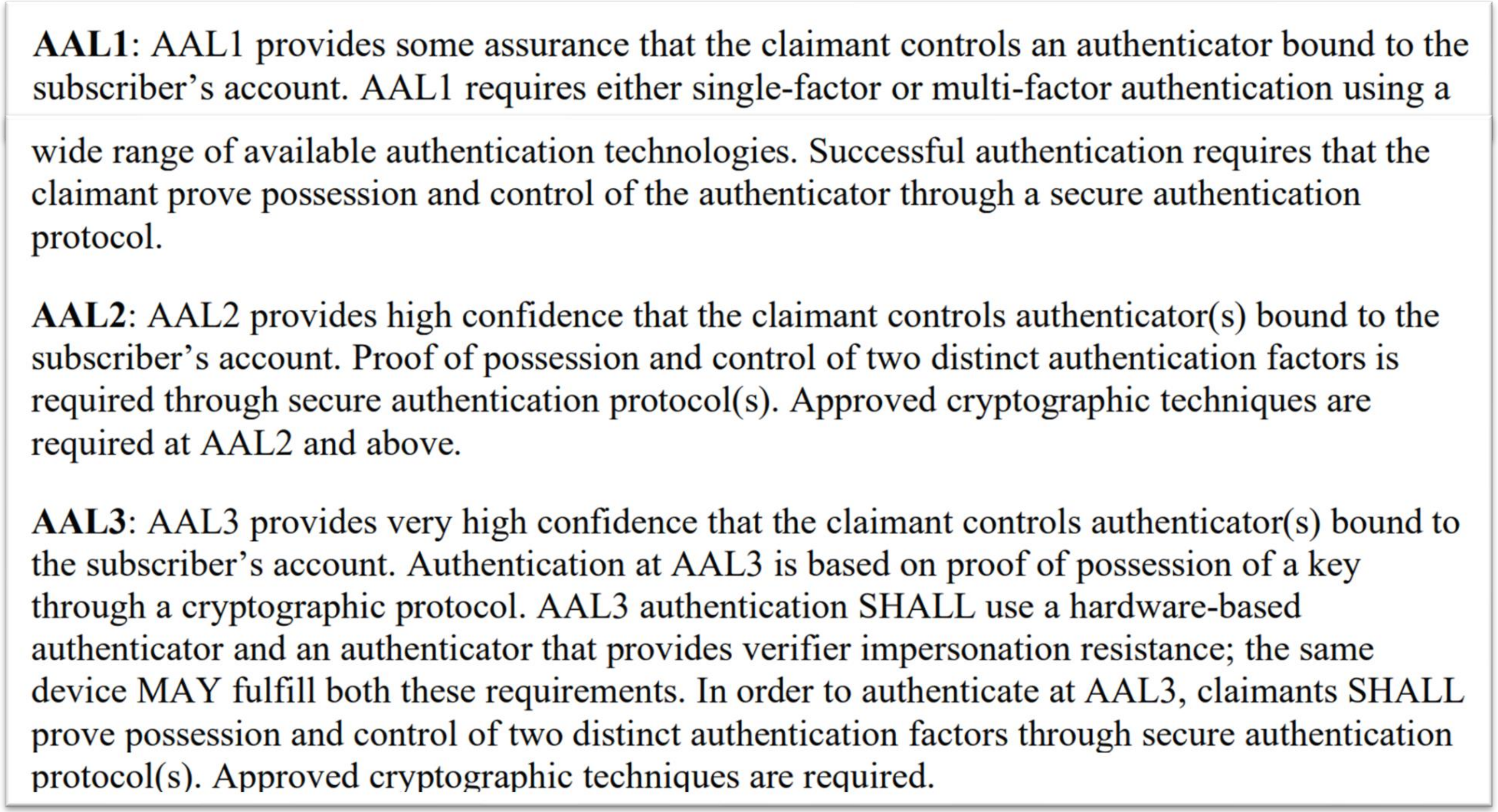


IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).

IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

Authentication Assurance Levels

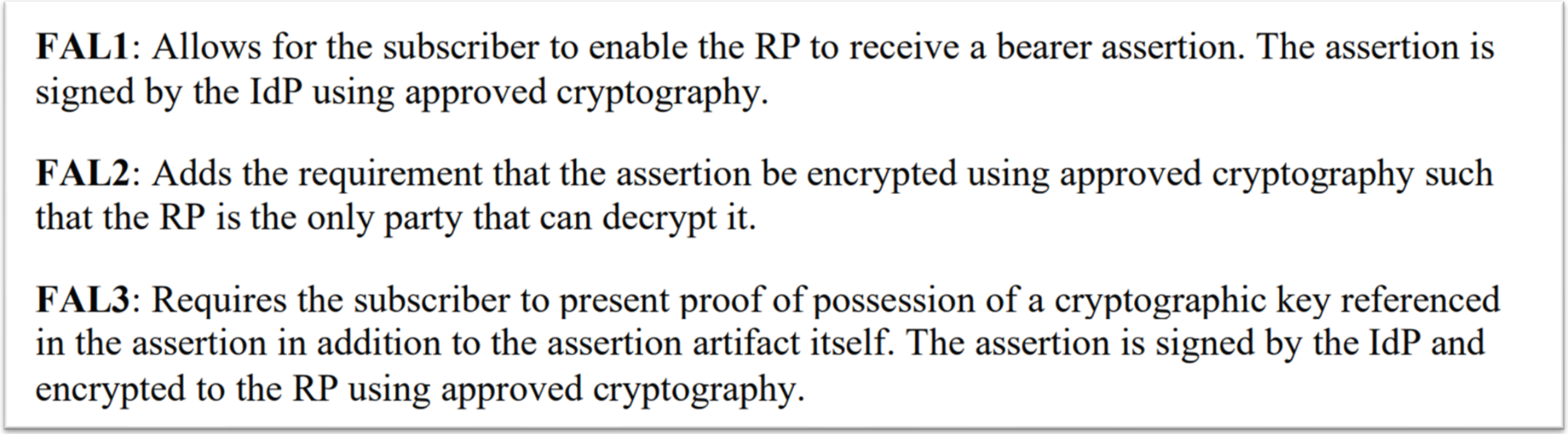


AAL1: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

Federation Assurance Levels

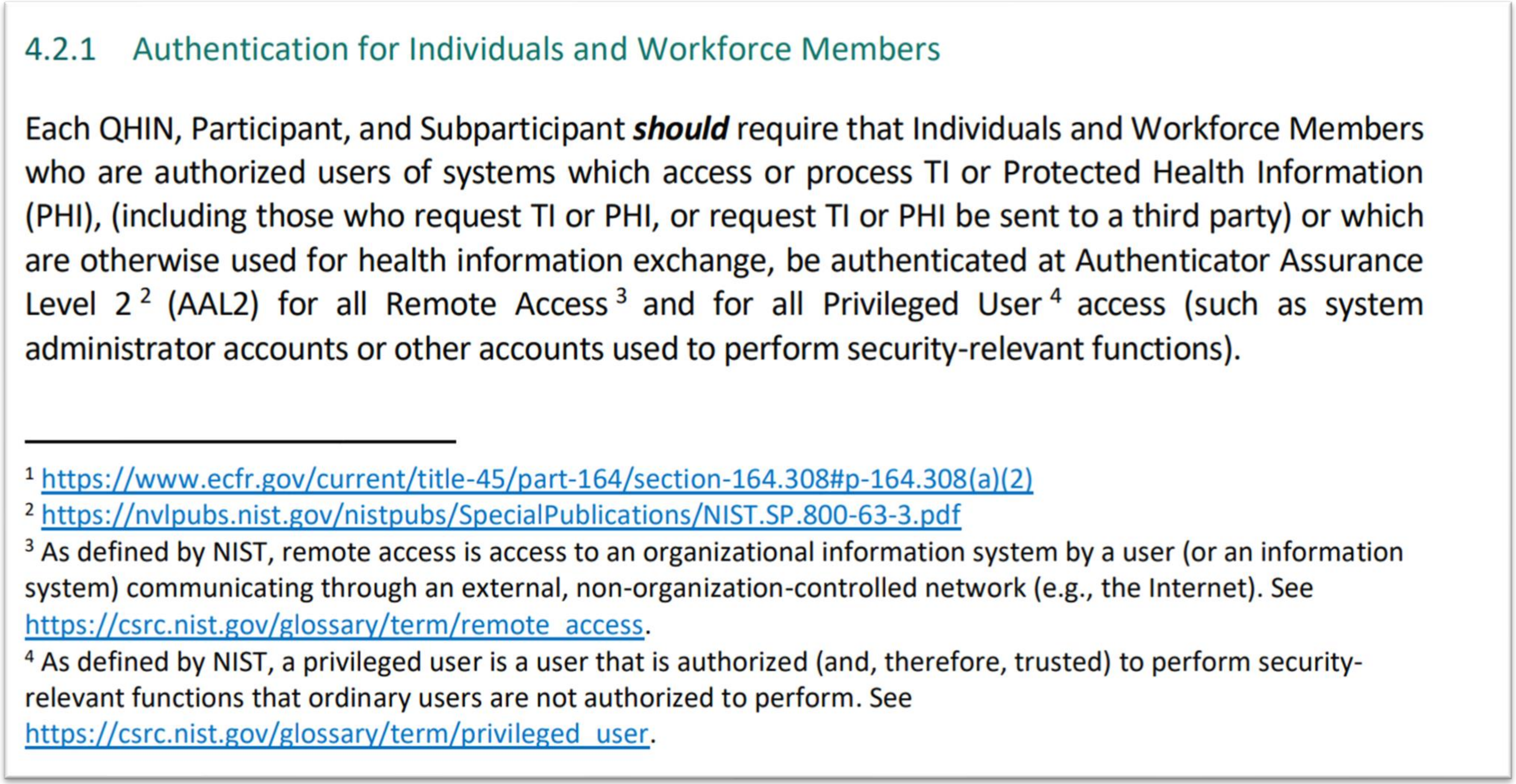


FAL1: Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.

FAL2: Adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.

FAL3: Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

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).

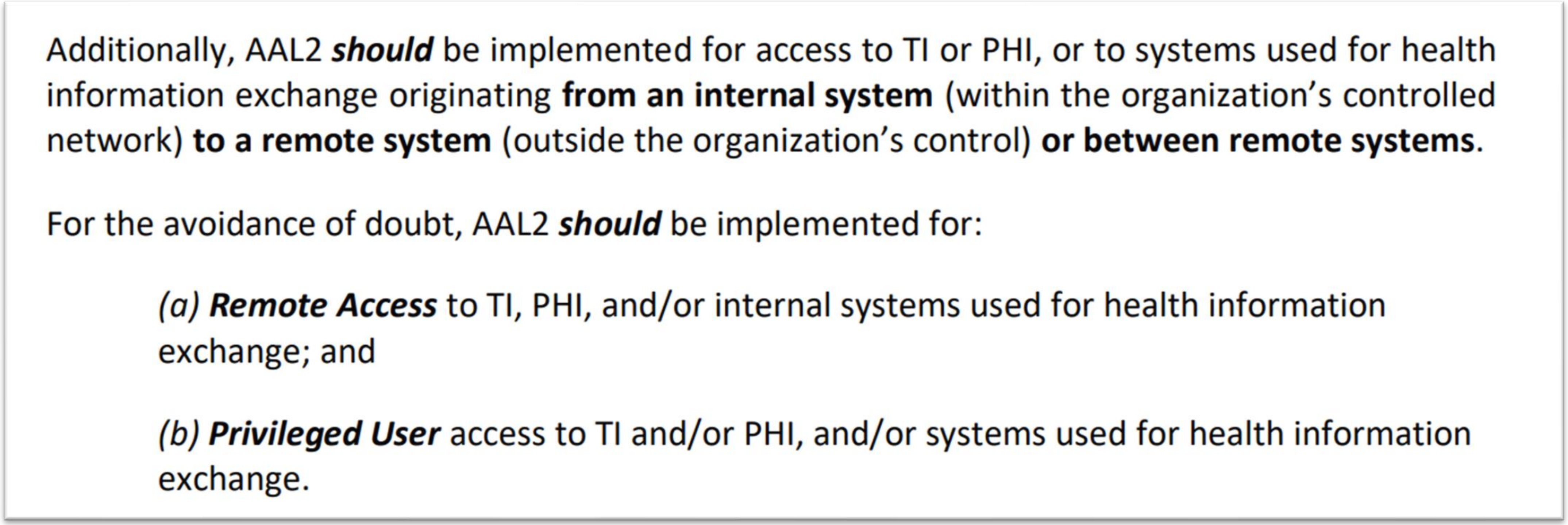
[1] https://www.ecfr.gov/current/title-45/part-164/section-164.308#p-164.308(a)(2)

[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.

Remote and Privileged Access



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.

Authentication Assurance Level Examples

- **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.

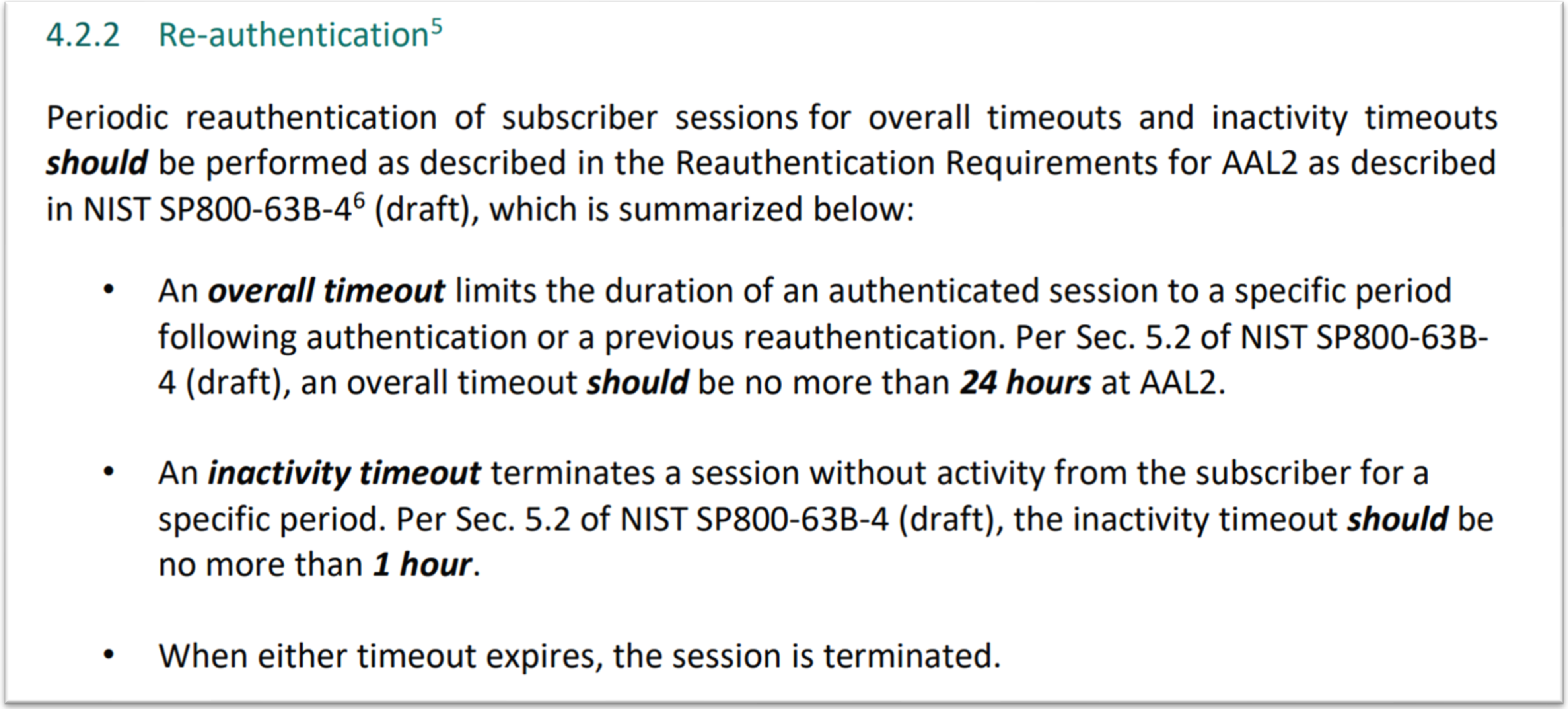
Authentication Assurance Level Examples

- **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.

Individual Access

- 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).

Re-Authentication



4.2.2 Re-authentication[5]

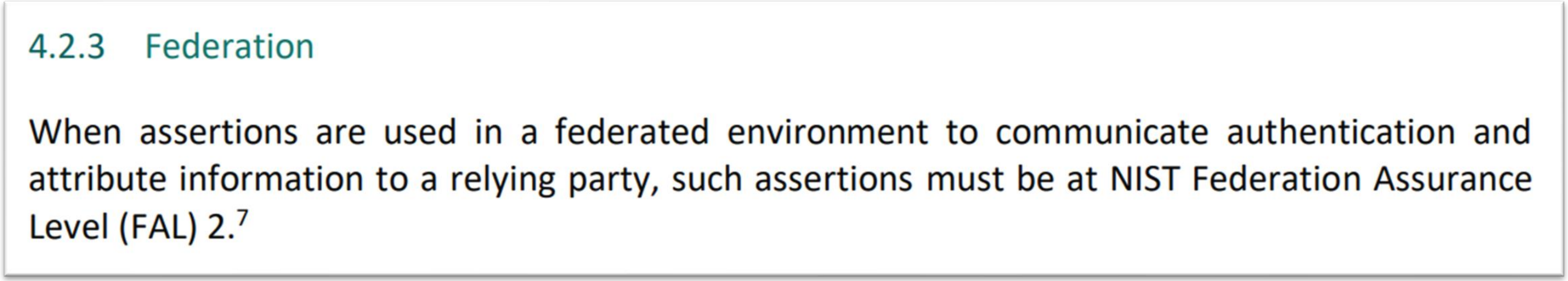
Periodic reauthentication of subscriber sessions for overall timeouts and inactivity timeouts ***should*** be performed as described in the Reauthentication Requirements for AAL2 as described in NIST SP800-63B-4[6] (draft), which is summarized below:

- 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.

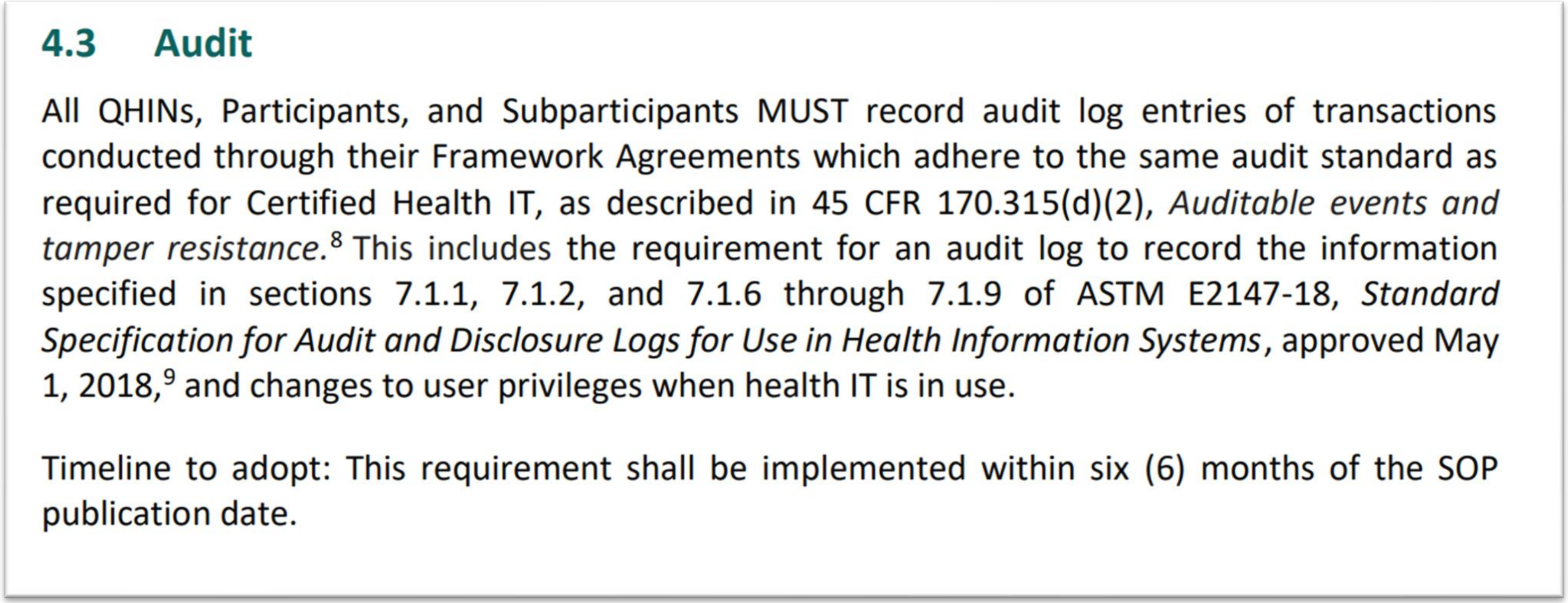
Federated Authentication



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]

Audit Requirements

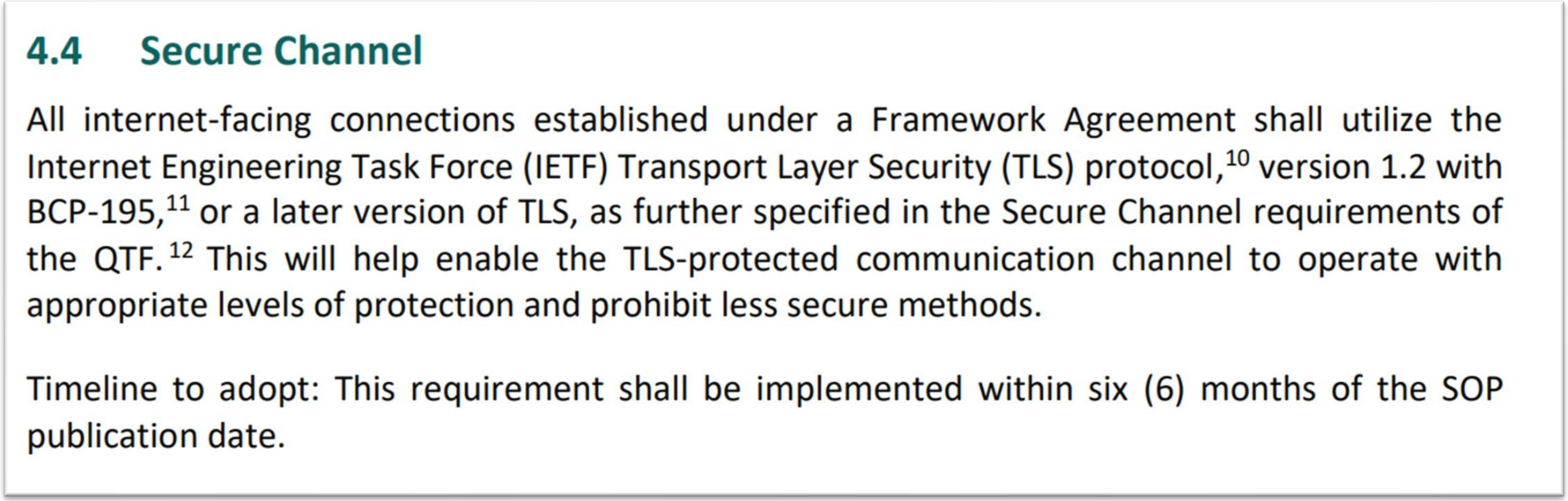


4.3 Audit

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.

Secure Channel (TLS)

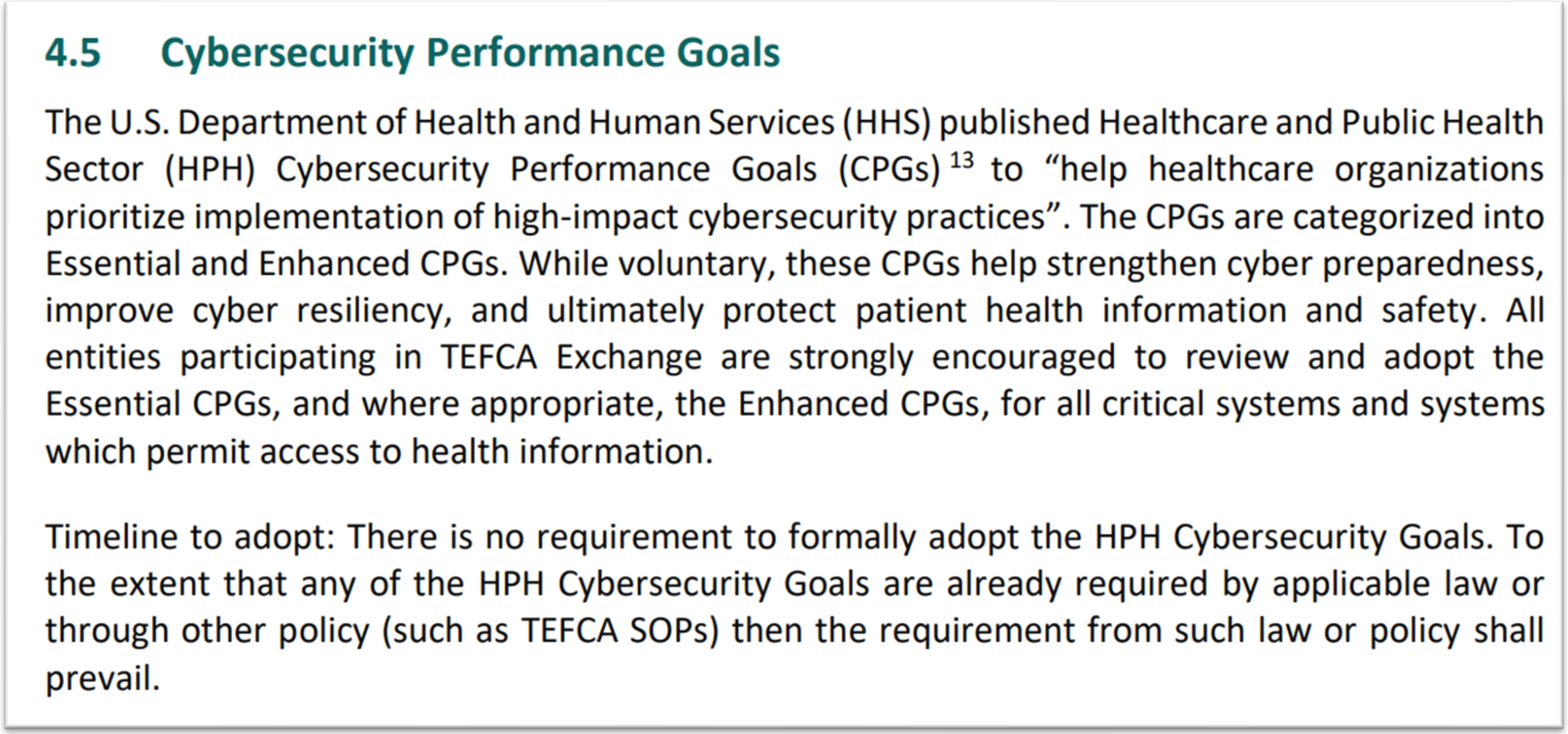


4.4 Secure Channel

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.

HHS Cybersecurity Performance Goals

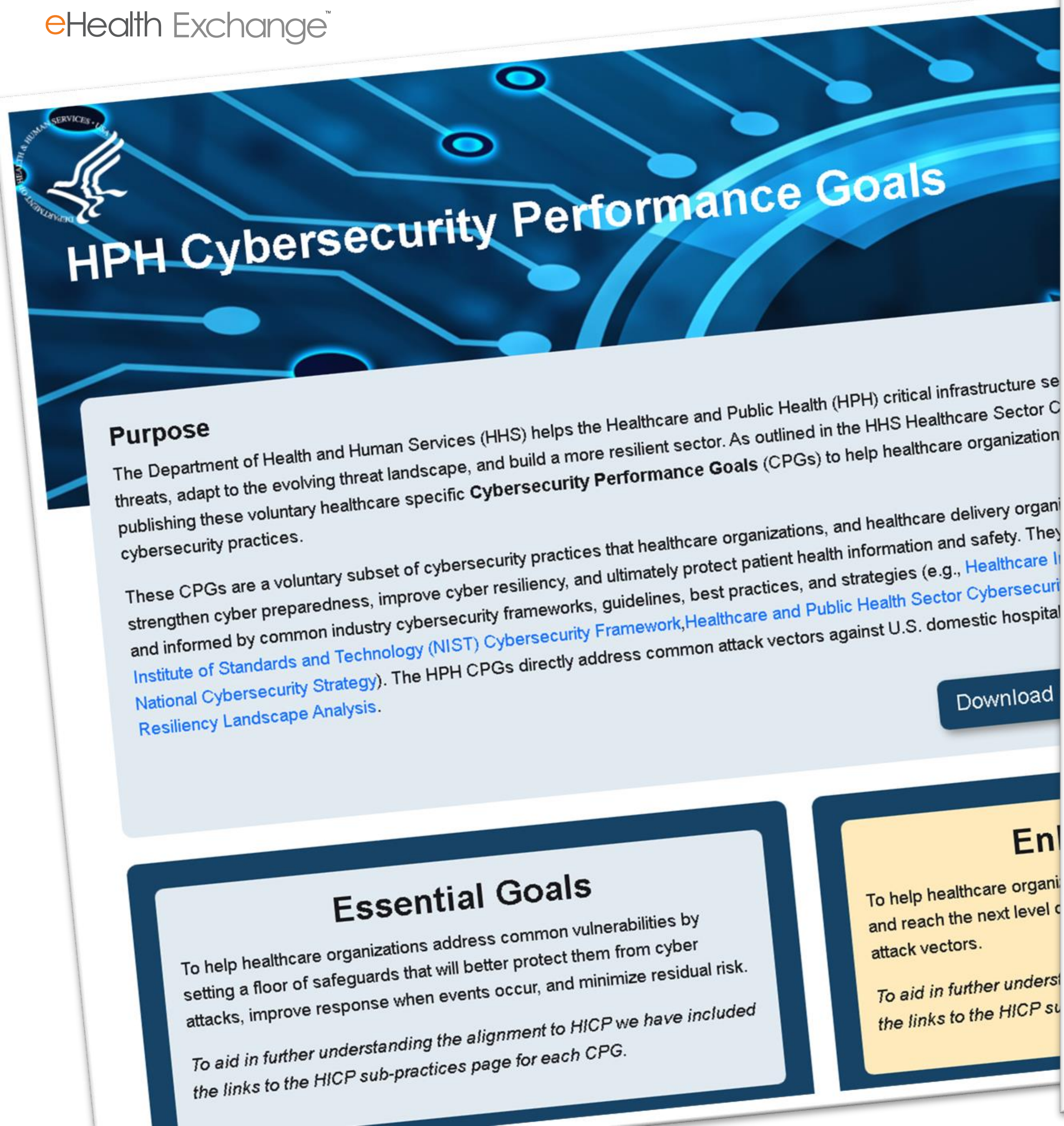


4.5 Cybersecurity Performance Goals

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.

See also: https://hhscyber.hhs.gov/performance-goals.html



HPH Cybersecurity Performance Goals

Purpose

The Department of Health and Human Services (HHS) helps the Healthcare and Public Health (HPH) critical infrastructure se
threats, adapt to the evolving threat landscape, and build a more resilient sector. As outlined in the HHS Healthcare Sector C
publishing these voluntary healthcare specific **Cybersecurity Performance Goals** (CPGs) to help healthcare organization
cybersecurity practices.

These CPGs are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organi
strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They
and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., Healthcare I
Institute of Standards and Technology (NIST) Cybersecurity Framework,Healthcare and Public Health Sector Cybersecuri
National Cybersecurity Strategy). The HPH CPGs directly address common attack vectors against U.S. domestic hospital
Resiliency Landscape Analysis.

Download

Essential Goals

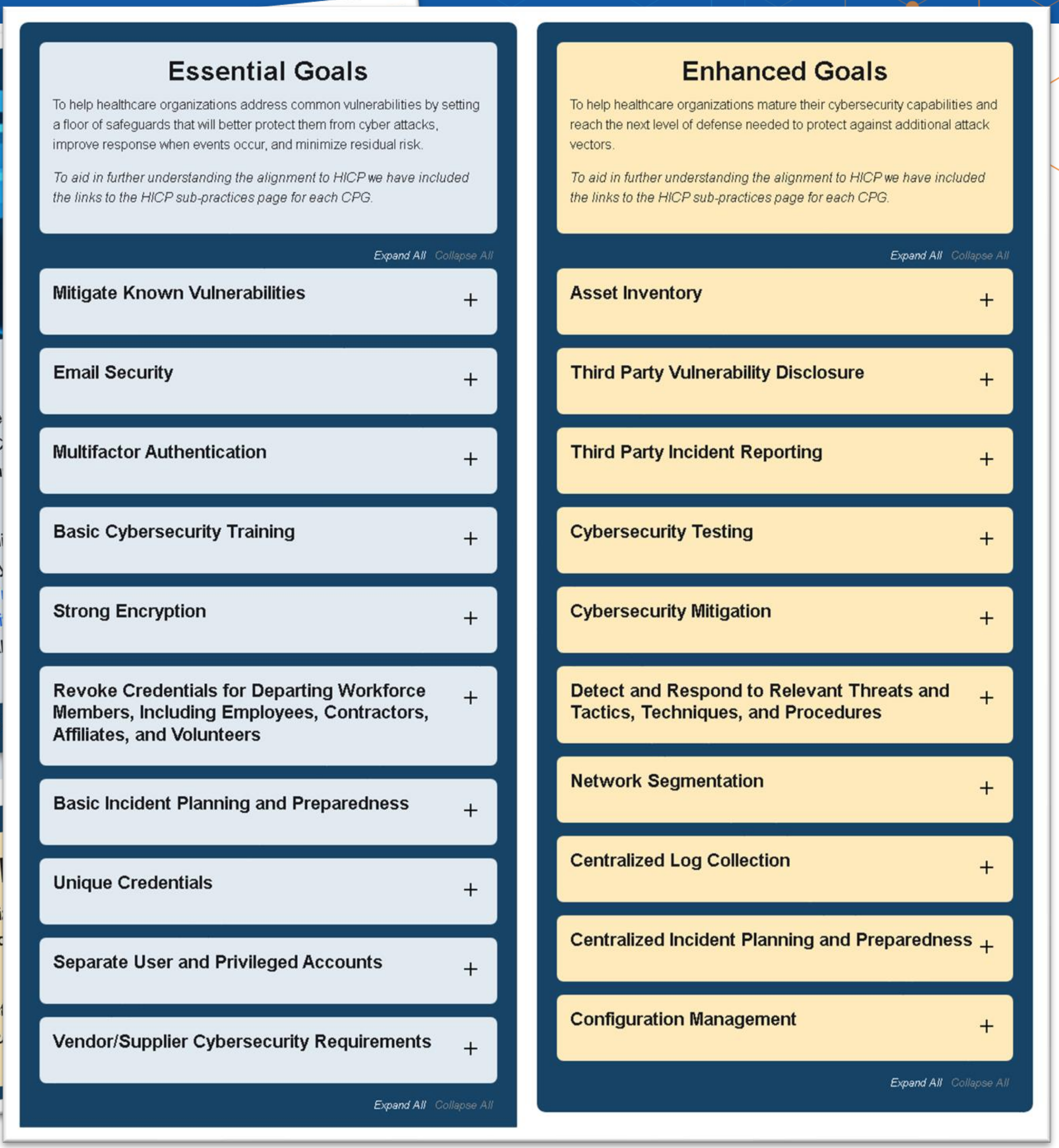
To help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyber attacks, improve response when events occur, and minimize residual risk.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

En

To help healthcare organi
and reach the next level c
attack vectors.

To aid in further unders
the links to the HICP su



Essential Goals

To help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyber attacks, improve response when events occur, and minimize residual risk.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Expand All *Collapse All*

- Mitigate Known Vulnerabilities +
- Email Security +
- Multifactor Authentication +
- Basic Cybersecurity Training +
- Strong Encryption +
- Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers +
- Basic Incident Planning and Preparedness +
- Unique Credentials +
- Separate User and Privileged Accounts +
- Vendor/Supplier Cybersecurity Requirements +

Expand All *Collapse All*

Enhanced Goals

To help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Expand All *Collapse All*

- Asset Inventory +
- Third Party Vulnerability Disclosure +
- Third Party Incident Reporting +
- Cybersecurity Testing +
- Cybersecurity Mitigation +
- Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures +
- Network Segmentation +
- Centralized Log Collection +
- Centralized Incident Planning and Preparedness +
- Configuration Management +

Expand All *Collapse All*

Questions?

eHealth Exchange™

ehealthexchange.org