Standard Operating Procedure (SOP): TEFCA Security Incident Reporting

Version 1.0

Date: July 1, 2024

Applicability: RCE, 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.

Common Agreement 2.0 References:

CA 12.3: TEFCA Security Incident Reporting. Signatory shall report to the RCE and to all QHINs that are likely impacted, whether directly or by nature of one of the other QHIN's Participants or Subparticipants, any TEFCA Security Incident, as set forth in the applicable SOP(s). Such report must include sufficient information for the RCE and others affected to understand the nature and likely scope of the TEFCA Security Incident. Signatory shall supplement the information contained in the report as additional relevant information becomes available and cooperate with the RCE, and with other QHINs, Participants, and Subparticipants that are likely impacted by the TEFCA Security Incident.

CA 12.3.1: Receiving TEFCA Security Incident Report. Signatory shall implement a reporting protocol by which other QHINs can provide Signatory with a report of a TEFCA Security Incident.

CA 12.3.2: Vertical Reporting of TEFCA Security Incident(s). Signatory shall report a TEFCA Security Incident to its Participants and Subparticipants as required by an applicable SOP.

CA 12.3.3: Compliance with Notification Under Applicable Law. Nothing in this Section 12.3 shall be deemed to modify or replace any breach notification requirements that Signatory may have under the HIPAA Rules, the FTC Rule, or other Applicable Law. To the extent Signatory is already required by Applicable Law to notify a Participant, Subparticipant, or another QHIN of an incident that would also be a TEFCA Security Incident, this Section 12.3 does not require duplicative notification.

Participant/Subparticipant Terms of Participation (ToP) References:

ToP 8.2: TEFCA Security Incident Reporting.

ToP 8.2.1: Reporting to Upstream QPS. You shall report to Upstream QPS any suspected TEFCA Security Incident, as set forth in the applicable SOP(s). Such report must include sufficient information for Upstream QPS and others affected to understand the nature and likely scope of the TEFCA Security Incident. You shall supplement the information contained in the report as

additional relevant information becomes available and cooperate with Upstream QPS and, at the direction of Upstream QPS, with the RCE, and with other QHINs, Participants, and Subparticipants that are likely impacted by the TEFCA Security Incident.

ToP 8.2.2: Reporting to Subparticipants. You shall report any TEFCA Security Incident experienced by or reported to You to Your Subparticipants as required by an applicable SOP.

ToP 8.2.3: Compliance with Notification Under Applicable Law. Nothing in this Section 8.3 shall be deemed to modify or replace any breach notification requirements that You may have under the HIPAA Rules, the FTC Rule, or other Applicable Law. To the extent You are already required by Applicable Law to notify Upstream QPS or a Subparticipant of an incident that would also be a TEFCA Security Incident, this section does not require duplicative notification.

2 SOP Definitions

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.

Breach of Unencrypted Individually Identifiable Information: the acquisition, access, or Disclosure of unencrypted Individually Identifiable Information maintained by an Individual Access Services Provider (IAS Provider) that compromises the security or privacy of the unencrypted Individually Identifiable Information.

Discover (including its correlative meanings "Discovery" and "Discovering"): the first day on which something is known to the QHIN, Participant, or Subparticipant, or by exercising reasonable diligence would have been known to the QHIN, Participant or Subparticipant.

TEFCA Information (TI): any information that is transacted through TEFCA Exchange except to the extent that such information is received by a QHIN, Participant, or Subparticipant that is a Covered Entity, Business Associate, or Non-HIPAA Entity (NHE) that is exempt from compliance with the Privacy section of the applicable Framework Agreement and is incorporated into such recipient's system of records, at which point the information is no longer TI with respect to such recipient and is governed by the HIPAA Rules and other Applicable Law.

TEFCA Security Incident(s):

(i) An unauthorized acquisition, access, Disclosure, or Use of unencrypted 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.

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, its Participant, or their 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.

3 PURPOSE

This SOP details the minimum reporting requirements for communicating TEFCA Security Incidents to the RCE, to other potentially impacted QHINs, and to any potentially impacted Participant and/or Subparticipant within the QHIN's network, as set forth in the Common Agreement and Terms of Participation.

This reporting will help enable the RCE to assess the overall security risks facing TEFCA Exchange and empower QHINs to take timely action to mitigate risks such as those from a compromised system of another QHIN, Participant, or Subparticipant.

Upon receipt of a TEFCA Security Incident Report, the RCE's TEFCA Cybersecurity Incident Response Team will convene and facilitate appropriate activities to help communicate threats to the broader TEFCA community. Activities may include the RCE convening the full Cybersecurity Council, or an executive session of a subset of the Cybersecurity Council and/or representatives from affected QHINs and/or Participants and/or Subparticipants to protect Confidential Information. Other activities, which may be conducted by the RCE, include supporting timely development and implementation of response and mitigation efforts across QHINs, reviewing and sharing Health Sector Cybersecurity Coordination Center (HC3) Threat Briefs and other sector alerts for any specific guidance or mitigation recommendations, and taking action it deems necessary to minimize the potential for further harm in response to a Threat Condition.

This SOP does not specify how or when entities must provide breach notification to individuals who may be affected by a security incident, which is specified in Common Agreement Section 12.3.3: Compliance with Notification Under Applicable Law, Section 10.5.2: IAS Incident Notice to Affected Individuals, Terms of Participation Section 8.2.3: Compliance with Notification Under Applicable Law, and applicable SOPs.

Section 5 of this SOP provides informative guidance to help organizations determine whether a security incident is a TEFCA Security Incident. Ultimately, each entity is responsible for determining whether a security incident (or, where applicable, a suspected security incident) is a TEFCA Security Incident and therefore subject to TEFCA Security Incident reporting procedures.

4 PROCEDURE

4.1 Confidentiality of Reports

TEFCA Security Incident Reports are considered Confidential Information as defined in the Common Agreement and must be treated as such. This does not, however, preclude a Confidential Information Recipient from redisclosing the content of a TEFCA Security Incident report as required by this SOP.

4.2 General TEFCA Security Incident Reporting Requirements

TEFCA Security Incident reports must include sufficient information for the RCE and others who may be affected to understand the nature and likely scope of the TEFCA Security Incident.

The initial report must not be delayed on the basis of incomplete information. Timely reporting is critical to reducing the potential for harm to others.

TEFCA Security Incident reporting does not supersede or replace any other reporting requirement imposed on QHINs, Participants, or Subparticipants under Applicable Law or contract. While TEFCA Infrastructure is not a Federal Government Information System and is therefore not subject to reporting requirements under the Federal Information Security

Modernization Act (FISMA), some TEFCA entities may themselves be subject to FISMA or may have other additional security incident reporting requirements beyond those required for TEFCA purposes.

To the extent that an entity is already required by Applicable Law or contract to report a security incident to a Participant, Subparticipant, or another QHIN of an incident that would also be a TEFCA Security Incident, this SOP does not require duplicative reporting to those entities.

An entity that has experienced a TEFCA Security Incident may additionally elect to report TEFCA Security Incidents to other parties, including, but not limited to, federal agencies or law enforcement, if deemed appropriate or necessary. Reporting organizations may elect to additionally report TEFCA Security Incidents to:

- The Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3);
- The Cybersecurity and Infrastructure Security Agency's (CISA's) online Incident Reporting System; and/ or
- CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870.

The FBI encourages organizations to report information concerning suspicious or criminal activity to their local FBI Field Office.

4.3 TEFCA Security Incident Reporting for QHINs

4.3.1 Who to report to:

Per section 12.3 of the Common Agreement, QHINs shall report to the RCE and to all QHINs that are likely impacted, whether directly or by nature of one of the other QHIN's Participants or Subparticipants, any TEFCA Security Incident.

For actual TEFCA Security Incidents reported to a QHIN by one of its Participants or Subparticipants, the QHIN must report upstream to the RCE even if no other QHINs are likely impacted. Reporting to the RCE is permitted, but not required, for incident reports received by the QHIN from a Participant or Subparticipant that the QHIN determines is not a TEFCA Security Incident.

Additionally, per section 12.3.2 of the Common Agreement, QHINs shall report a TEFCA Security Incident to its Participants and Subparticipants that are likely impacted by the TEFCA Security Incident.

4.3.2 How to report:

TEFCA Security Incidents that are reported to the RCE must be submitted by QHINs to the RCE's TEFCA Cybersecurity Incident Response Team (TEFCA-CIRT) at TEFCA-CIRT@sequoiaproject.org. Alternatively, this email address may be used to provide notification of availability of an incident report that can be received by the RCE using secure means.

Per Section 12.3.2 of the Common Agreement, QHINs shall implement a reporting protocol by which other QHINs can provide them with notification of a TEFCA Security Incident.

The timelines in Table 1 set forth the report types and associated timelines for QHINs to report TEFCA Security Incidents to the RCE and other likely impacted QHINs, Participants, and Subparticipants.

TABLE 1: QHIN TEFCA SECURITY INCIDENT (TSI) REPORTING TIMELINES

Reporting for TEFCA Security Incidents		
Report Type	**Timeline**	**Distribution**
QHIN TSI Initial Report	As soon as reasonably practicable, but not more than 72 hours after Discovery	1) If a QHIN experiences a TSI, or receives a TSI report from a downstream Participant or Subparticipant that is confirmed to be a TSI, it reports to the RCE using the TEFCA Security Incident Report form (or provides notice of the availability of a report) to TEFCA-CIRT@sequoiaproejct.org; and 2) to all other QHINs likely impacted, and to Participants and Subparticipants within the reporting QHIN's network that are likely impacted.
QHIN TSI Supplemental Report	As additional pertinent information becomes available, and at least every 24 hours until the incident is resolved	Same as above for an initial TSI report
QHIN TSI Post-Incident Report	Required within 30 days after incident has been resolved	Affected QHIN reports to the RCE

QHINs must supplement the information contained in the report as additional relevant information becomes available and cooperate with the RCE, and with other QHINs, Participants, and Subparticipants that are likely impacted by the TEFCA Security Incident.

4.4 TEFCA Security Incident Reporting Requirements for Participants and Subparticipants

Per Section 8.2.1 of the ToP, Participants, and Subparticipants shall report to their Upstream QHIN, Participant, or Subparticipant, any suspected TEFCA Security Incident.

Per Section 8.2.2 of the ToP, Participants and Subparticipants shall also report any TEFCA Security Incident they experience, or is reported to them, to any of their downstream Subparticipants which may be likely impacted.

Participants and Subparticipants must cooperate with Upstream QHIN, Participant, or Subparticipant (QPS), and at the direction of Upstream QPS, with the RCE, and with other QHINs, Participants, and Subparticipants that are likely impacted by the TEFCA Security Incident.

The timelines in Table 2 set forth the report types and associated timelines for Participants and Subparticipants to report TEFCA Security Incidents to their Upstream QPS and to likely impacted downstream Subparticipants.

TABLE 2: PARTICIPANT/SUBPARTICIPANT TEFCA SECURITY INCIDENT REPORTING REQUIREMENTS

Participant/Subparticipant Vertical Reporting for TEFCA Security Incidents		
Report Type	**Timeline**	**Distribution**
Vertical Reporting by Participants and Subparticipants.	For the Discovering entity: As soon as reasonably practicable, but not more than 72 hours after Discovery For the entity receiving a report from another entity: When vertically reporting a TEFCA Security Incident, the receiving entity has one business day to forward the report to their upstream entity and to likely affected downstream entities	1. To Upstream QPS any suspected or actual TEFCA Security Incident, and 2. To any likely affected Downstream Participant or Subparticipant for any actual TEFCA Security Incident they experience or has been reported to them by their Upstream QPS

4.5 TEFCA Security Incident Reporting Requirements for RCE

The RCE must report to all likely impacted QHINs any TEFCA Security Incidents discovered by the RCE in relation to any services supporting TEFCA Exchange, operated or contracted by the RCE.

The timelines in Table 3 set forth the report types and associated timelines for the RCE to report TEFCA Security Incidents to likely impacted QHINs.

TABLE 3: RCE TEFCA SECURITY INCIDENT REPORTING REQUIREMENTS

RCE Reporting for TEFCA Security Incidents		
Report Type	**Timeline**	**Distribution**
TEFCA Security Incident Report	As soon as reasonably practicable, but not more than 72 hours after Discovery	RCE sends report to any likely impacted QHIN

4.6 TEFCA Security Incident Report Format

TEFCA Security Incident Reports from QHINs to the RCE or the RCE to QHINs must use the form maintained by the RCE and provided to TEFCA entities through the Cybersecurity Council. Additional reporting formats, such as emails or briefings, can be used to provide more situational awareness to key stakeholders and exchange information about the incident that will enable others to better identify, contain, respond, and recover from a TEFCA Security Incident.

Reporting QHINs may use the TEFCA Security Incident Report form when providing notice to other QHINs, and to Participants and Subparticipants that are likely impacted, or they may use a format of their choice provided that the information being reported is substantially similar and provides the recipient with the available information needed to minimize the potential for harm.

When reporting an actual or suspected TEFCA Security Incident to an Upstream QPS, Participants and Subparticipants may use the TEFCA Security Incident Report form that QHINs are required to use when a QHIN reports a TEFCA Security Incident to the RCE. Participants and Subparticipants may use alternate reporting formats provided the reports contain substantially similar content. Note, Participants and Subparticipants are not required to report directly to the RCE.

The following information should be included in a TEFCA Security Incident Report to the extent the information is known at the time the report is communicated:

- Contact information;
- A description of the events giving rise to the report;
- Other details reasonably relevant to the security posture of those likely impacted;
- Impact Determination (see Table 4: Impact Description Table);
    - Functional Impact
    - Information impact
    - Recoverability Impact
- Attack vector, if possible (see Table 5: Attack Vectors); and
- Mitigation details, if possible.

4.6.1 Impact Determination

The tables below must be used to categorize the potential impact of a TEFCA Security Incident and must be included in the appropriate TEFCA Security Incident Report. Definitions for the impact categories are adapted from the Federal Incident Notification Guidelines1 published by the Cybersecurity and Infrastructure Security Agency (CISA).

TABLE 4: IMPACT DETERMINATION

Impact Description		
Functional Impact	High	Entity has lost the ability to provide some or all critical services to all system users; or Entity has lost the ability to conduct TEFCA Exchange with one or more QHINs; or Entity has lost the ability to conduct TEFCA Exchange with one or more of their Participants/Subparticipants.
	Medium	Entity has lost the ability to provide one or more critical services to some Participants/Subparticipants, or has one or more Participant/Subparticipant within their network who has lost the ability to participate in TEFCA Exchange.
	Low	Entity has experienced a loss of efficiency but can still provide all critical services to all users with minimal effect on performance.
	None	Entity has not experienced loss in ability to provide all services to all users.
Information Impact	Proprietary	The confidentiality of Confidential Information, such as proprietary information, intellectual property, or trade secrets was compromised.
	Privacy	The confidentiality of Individually Identifiable Information or Personal Health Information (PHI) was compromised.
	Integrity	The integrity of information was modified without authorization. This includes unauthorized system configuration changes.
	None	No information was exfiltrated, modified, deleted, or compromised.
Recoverability Impact	Regular	Time to recover is predictable with existing resources.
	Supplemented	Time to recover is predictable with additional resources. Greater than 8 hours are needed to recover.
	Extended	Time to recovery is unpredictable. Additional resources and outside help are needed. Greater than 24 hours are needed to recover.
	Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data was exfiltrated and posted publicly).
	Not Applicable	Incident does not require recovery.

[1] Federal Incident Notification Guidelines available at: https://www.cisa.gov/federal-incident-notification-guidelines

4.6.2 Attack Vectors

To help consistently communicate incidents, the following high-level set of attack vectors and descriptions, as adapted from NIST SP 800-61r2, should be used where possible. Multiple attack vectors may be included in a single incident report.

TABLE 5: ATTACK VECTORS

Attack Vectors		
Attack Vector	**Description**	**Example**
Unknown	Method of attack is unidentified.	This option is acceptable if the attack vector)is unknown upon initial report. The attack vector may be updated in a follow-up report.
Brute Force	An attack that employs brute force methods to compromise networks or services.	A brute force attack against an authentication mechanism, such as passwords or digital signatures.
Denial Of Service	An attack that uses repeat/ systematic methods to compromise, degrade, or destroy systems, networks, or services.	A denial of service intended to impair or deny access to an application.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email/Phishing	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack method that does not fit into any other vector.	

5 Informative Guidance: TEFCA Security Incident Determination

In the event of a security incident, entities should carefully review their Framework Agreement to determine whether the incident is a TEFCA Security Incident and if they are required to report the incident. The guidance provided in this section assumes entities are not exempt from reporting TEFCA Security Incidents.

Only TEFCA Security Incidents are required to be reported through the TEFCA Security Incident Report process as described in this SOP. Additional reporting of non-TEFCA Security Incidents is permitted, but not required.

To determine whether a security incident is a TEFCA Security Incident, entities should consider the following factors:

- Factor A: Did the incident involve TEFCA Information? (Section 5.1)
- Factor B: Is there a permitted exception? (Section 5.2)
- Factor C: Is the incident an other security event that adversely affects participation in TEFCA Exchange? (Section 5.3)

If TEFCA Information is involved in a security incident (Factor A) *and* there is no permitted exception (Factor B), then the security incident is likely to be a TEFCA Security Incident. If an exception from Factor B applies to the TEFCA Information, entities must also consider Factor C to determine if the incident is still reportable as a TEFCA Security Incident.

If TEFCA Information is not involved (Factor A), and none of the exceptions (Factor B) apply, entities should consider Factor C to determine if the incident is still reportable as a TEFCA Security Incident.

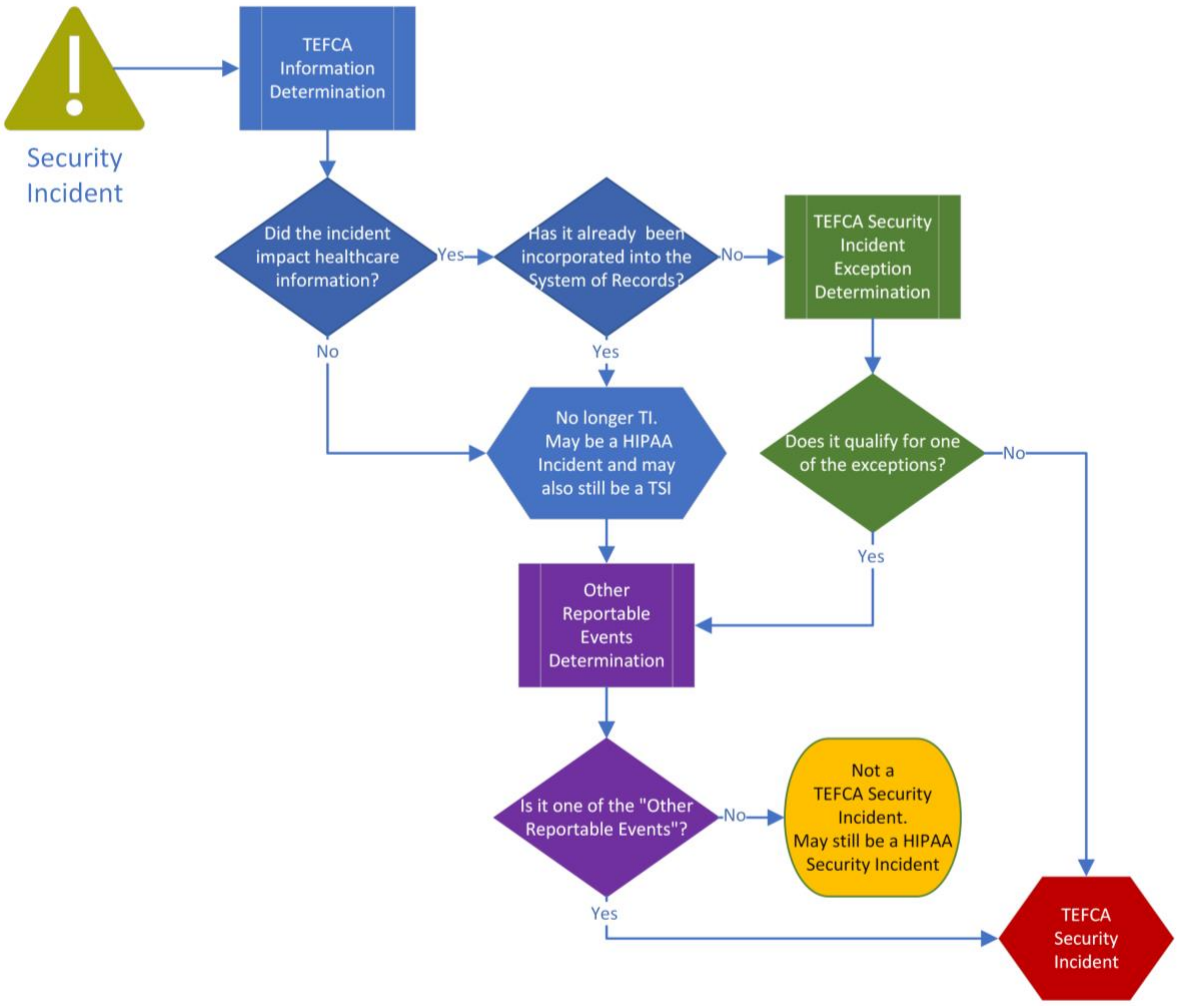
The decision tree included in Figure 1 can be used to help guide the TEFCA Security Incident determination process.

FIGURE 1: TEFCA SECURITY INCIDENT DETERMINATION PROCESS

Factor A: TEFCA Information Determination

Factor B: TEFCA Security Incident Exception Determination

Factor C: Other Reportable Events Determination



5.1 Factor A: Did the incident involve TEFCA Information?

In the event of a security incident, entities should review the definition of TEFCA Information and make a determination as to whether TEFCA Information was involved. The Common Agreement considers information to no longer be TEFCA Information once it has been incorporated into a recipient's system of records. This Factor applies to HIPAA Covered Entities and Business Associates, and to Non-HIPAA Entities who are exempt from compliance with the Privacy section of their applicable Framework Agreement.

System of records: It is the responsibility of each TEFCA organization to identify which system(s) it considers to be its system of records. For example, a system of records would include the information system(s) containing information that is used to make decisions about individuals[2], such as a Designated Record Set (as defined in 45 CFR 164.501) or information contained within an electronic health record system.

[2] U.S. Department of Health and Human Services' Health Information Privacy Frequently Asked Questions available at: https://www.hhs.gov/hipaa/for-professionals/faq/2042/what-personal-health-information-do-individuals/index.html

5.2 Factor B: Is there a permitted exception?

HIPAA Entities and Non-HIPAA Entities: Per the definition of TEFCA Security Incident, an unauthorized acquisition, access, Disclosure, or Use of unencrypted TEFCA Information using TEFCA Exchange, is **NOT** a TEFCA Security Incident if **ANY** of the exceptions (a) through (c) apply:

(a) An unintentional acquisition, access, Use, or Disclosure of TEFCA Information 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).

Non-HIPAA Entities: Per Section 8.1 of the Participant/Subparticipant Terms of Participation, Non-HIPAA Entities shall comply with the HIPAA Security Rule provisions with respect to all Individually Identifiable Information as if such information were Protected Health Information and they were a Covered Entity or Business Associate. In addition, per Section 12.4 of the Common Agreement, Non-HIPAA Entities (that are not otherwise exempt from Section 12.4) must encrypt all Individually Identifiable Information they maintain, both in transit and at rest, regardless of whether such information is TEFCA Information. For these Non-HIPAA Entities, there is no exception for a Breach of Unencrypted Individually Identifiable Information. **A Breach of Unencrypted Individually Identifiable Information by a Non-HIPAA Entity is considered a Threat Condition and must be reported as if it were a TEFCA Security Incident.**

5.3 Factor C: Is the incident considered an other reportable security event?

Per the definition of TEFCA Security Incident, other reportable security events are those security-related events that adversely affect a QHIN's, Participant's, or Subparticipant's participation in TEFCA Exchange. Confidentiality, integrity, and availability are the basic tenets of information security and should be considered when determining if an incident is considered an "other reportable security event" under TEFCA. Security events that may adversely affect participation in TEFCA are those events that are not already addressed through Factors A and B, but may impact the confidentiality, integrity, or availability of TEFCA Information or otherwise adversely affect an entity's ability to participate in TEFCA exchange. These events may be internal or external, and may or may not include human actors. Examples include:

(a) Ransomware attacks or receipt of a plausible ransom notice;

(b) Ongoing Denial of Service attacks which affect connectivity for an extended period of time;

(c) Persistent and/or widespread connectivity disruptions due to a security incident;

(d) System issues causing data corruption; or

(e) Voluntarily pausing participation in TEFCA Exchange as a precautionary measure relating to a security incident (e.g. to determine the scope or prevalence of a security incident).

Reporting of incidents that have no confirmed functional or information impact such as passive scans, phishing attempts, attempted access, or thwarted exploit attempts are not required to be reported but may be submitted voluntarily.

6 VERSION HISTORY

Version #	Revision Date	Section #(s) of Update
1.0	July 1, 2024	N/A