Effective Date: XX/XX/XXXX
Last Revision Date: NA
QHIN Governance Committee Approval Date: xx/xx/xxxx

8300 Boone Blvd., Suite 500, Vienna, Virginia, 22182

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

Scope and Authority

This Protocol addresses the organization and operation of the QHIN Governance Committee (QGC) which will perform the functions of the eHealth Exchange QHIN Designated Network Governing Body (DNGB) as that term is defined in the QHIN Onboarding and Designation SOP. The eHealth Exchange Coordinating Committee, which is the governing body of the eHealth Exchange, has established the QGC as a standing subcommittee with the authority specified in the Onboarding and Designation SOP, the eHealth Exchange QHIN TEFCA Terms and Conditions and this Protocol.

In accordance with eHealth Exchange Operating Policy & Procedures (OPP) #10 (Participant Opt-Out of New Data Sharing Agreements), this protocol applies to all Participants that do not opt-out of the eHealth Exchange QHIN and are thus bound by the TEFCA Terms and Conditions.

Purpose

The primary purpose of this protocol is to provide standardized and clear methods and procedures for Participants to report any suspected TEFCA Security Incident. The privacy, security, and integrity of TEFCA Information are essential. To help maintain the privacy, security, and integrity of TEFCA Information and promote trust among QHINs, Participants, and Subparticipants, each eHealth Exchange QHIN Participant has agreed to notify certain other Participant, Subparticipants, the eHealth Exchange QHIN Chief Information Security Officer (CISO), and the QHIN Governance Committee of a TEFCA Security Incident. This protocol sets forth the procedure by which the eHealth Exchange Participant, the eHealth Exchange CISO, and the QHIN Governance Committee will fulfill their respective TEFCA Security Incident obligations under the TEFCA Terms & Conditions.

The QHIN Governance Committee will have responsibility, oversight, control, and final decision-making authority over each of the Governance Functions: (i) Technical framework of the Designated Network; (ii) The resolution of disputes regarding use of eHealth Exchange QHIN; (iii) eHealth Exchange QHIN Security Incident(s); (iv) enforcement of eHealth Exchange QHIN Participant compliance with all flow-down requirements, and: (v) change management to implement changes for the eHealth Exchange QHIN.

Protocol

This protocol addresses the requirements of reporting any suspected TEFCA Security Incident and the procedures to be followed. TEFCA Security Incidents, as defined in the TEFCA Terms & Conditions, are very serious incidents with potential for serious impact on QHINs, QHIN Participants/Subparticipants, and/or the individuals whose Protected Health Information (PHI) is transmitted via the eHealth

Effective Date: XX/XX/XXXX
Last Revision Date: NA
QHIN Governance Committee Approval Date: xx/xx/xxxx

8300 Boone Blvd., Suite 500, Vienna, Virginia, 22182

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

Exchange QHIN. A TEFCA Security Incident shall be treated as "Discovered" consistent with 45 C.F.R. § 164.404(a)(2) as if the TEFCA Security Incident were a breach (as defined in 45 C.F.R. § 164.402) and regardless whether the Participant and/or the Subparticipant, as applicable, is a Covered Entity or Business Associate under HIPAA. Thus, each eHealth Exchange QHIN Participant has the obligation to identify, notify, investigate, and mitigate any known or suspected TEFCA Security Incident. When a TEFCA Security Incident is Discovered, the eHealth Exchange QHIN Participant must notify the QHIN Governance Committee and any affected QHINs of the TEFCA Security Incident in accordance with the procedures herein.

The QHIN Governance Committee or its Designee, Healtheway, Inc. (d/b/a/ "The eHealth Exchange" and its "eHealth Exchange QHIN support staff"), will conduct periodic reviews to evaluate and identify improvements to the TEFCA Security Incident notification process.

Procedure

1. TEFCA Security Incident Notification Contact List
    a. eHealth Exchange QHIN Participants shall provide eHealth Exchange QHIN support staff appropriate points of contact for TEFCA Security Incident Notification and shall promptly notify the eHealth Exchange QHIN support staff if those points of contact change.
    b. eHealth Exchange QHIN support staff shall maintain a list of QHIN Governance Committee Members as well as Participant contacts for TEFCA Security Incident Notification purposes.
    c. eHealth Exchange QHIN Participants are accountable for assuring there are mechanisms to notify appropriate individuals regarding TEFCA Security Incidents relative to the eHealth Exchange QHIN.
2. eHealth Exchange QHIN Participants shall report any TEFCA Security Incident experienced by or reported to the eHealth Exchange QHIN Participant to all of the Participant's Subparticipants. Such notification shall be in accordance with the timing and content requirements stated in #5 of this procedure.
3. eHealth Exchange QHIN Participants shall require that each Subparticipant with which it has entered into a Participant-Subparticipant Agreement:
    a. Report any TEFCA Security Incident experienced by or reported to the Subparticipant to eHealth Exchange QHIN Participant and to the Subparticipant's Downstream Subparticipants in accordance with the timing and content requirements in #5 of this procedure.
    b. Require that each Subparticipant with which the eHealth Exchange QHIN Participant enters into a Participant-Subparticipant Agreement require that is Downstream Subparticipants report any TEFCA Security Incident experienced by or reported to the Downstream Subparticipant to the Upstream Subparticipant and to its own Downstream

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

Subparticipants, in accordance with the timing and content requirements in #5 of this procedure.

4. eHealth Exchange QHIN Participants are responsible for providing notification of any TEFCA Security Incident reported to the eHealth Exchange QHIN Participant by one of its Subparticipants in accordance with the procedures outlined below.
5. Notification of TEFCA Security Incidents involving Non-Federal eHealth Exchange QHIN Participants:
    a. As soon as reasonably practicable, but no later than within five (5) calendar days of Discovering that a TEFCA Security Incident may have occurred, the eHealth Exchange QHIN Participant must:
        i. Immediately notify the QHIN Governance Committee eHealth Exchange QHIN by sending an email to the Alert email: securityevent@ehealthexchange.org.
            1. This email address is monitored by the eHealth Exchange QHIN support staff, including the CISO.
        ii. Send a notification of the TEFCA Security Incident to all of the Participant's Subparticipants. Participant must also notify any/all other eHealth Exchange QHIN Participants that are likely impacted by the TEFCA Security Incident. Notification sent to other eHealth Exchange QHIN Participants must be sent to the contact(s) identified in the TEFCA Security Incident Notification contact list.
    b. eHealth Exchange QHIN Participants are to send TEFCA Security Incident notifications through a secure means, when appropriate, and labeled as "Confidential Information." The notification must include sufficient information for the QHIN Governance Committee, in coordination with the eHealth Exchange QHIN CISO, the QHIN Governance Committee Participant's Subparticipants, and any other likely impacted Participants to understand the nature of the TEFCA Security Incident. For instance, such notification could include, to the extent available at the time of the notification, the following information:
        i. One or two sentences describing the TEFCA Security Incident
        ii. Description of the roles of the people involved in the TEFCA Security Incident (e.g., employees, Participant/Subparticipant Users, service providers, unauthorized persons, etc.)
        iii. The type of information involved in the TEFCA Security Incident
        iv. eHealth Exchange QHIN Participants/Subparticipants likely impacted by the TEFCA Security Incident
        v. Number of individuals or records impacted/estimated to be impacted by the TEFCA Security Incident
        vi. Actions taken by the eHealth Exchange QHIN Participant/Subparticipant to mitigate the TEFCA Security Incident
        vii. Current status of the TEFCA Security Incident (under investigation or resolved)
        viii. Corrective action taken and steps planned to be taken to prevent a similar TEFCA Security Incident

Commented [PR1]: From Cait:
Regarding the highlighted portion of the above comment: The feds are **not** entitled to anything different related to TEFCA Security Incidents. The notice requirement under the Common Agreement and Required Flow-Downs is within 5 days – period.

A QHIN can certainly *shorten* that time period. It simply cannot allow more than 5 days in which to provide notice of a TSI.

Given the notice timeframe required under TEFCA, the only reason I can think of for carrying the 1-hour Federal Participant notification over to the eHx QHIN requirements would be if it gave eHx a competitive advantage in enlisting Federal QHIN Participants.

Commented [PR2]: Jay: Should we create an email address that gets routed to this email address? (TEFCAsecurityincident@ehealthexchange.org)

Commented [tbd3R2]: This would be good to make it even more clear this is a TEFCA security notification. Good idea.

Commented [PR4R2]: Great: I will request Erik to create this email address and have it routed to securityevent@ehealthexchange.org

Commented [CLR5R2]: I believe we actually noted in the QHIN Application responses that this e-mail address would be the same as what is used for Adverse Security Events. The rationale of a having a single point of intake for security incidents is that Participants likely will not know whether something is a TEFCA Security Incident or an Adverse Security Event and will need the eHealth Exchange's assistance in determining which it is.

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

The notification must NOT include any Protected Health Information (PHI). eHealth Exchange QHIN Participants are strongly urged to label the notification (e.g., subject line or posting, etc.) as Confidential eHealth Exchange QHIN Participant/Subparticipant Information.

c. The eHealth Exchange QHIN Participant shall have the duty to supplement the information contained in the notification as it becomes available. Supplemental information should be directed to the same addresses used for the original notification. eHealth Exchange QHIN Participants and Subparticipants are strongly urged to label (e.g., subject line or posting, etc.) the supplemental information as Confidential eHealth Exchange QHIN Participant/Subparticipant Information.

d. If, on the basis of the information that the eHealth Exchange QHIN Participant has, the eHealth Exchange QHIN Participant believes that it should temporarily cease exchanging TEFCA Information through the eHealth Exchange QHIN, it may undergo a voluntary suspension from the eHealth Exchange QHIN.

6. **One-Hour Notification** of TEFCA Security Incidents involving eHealth Exchange QHIN Federal Participants:

   a. Within one (1) hour of Discovering information that leads the eHealth Exchange QHIN Participant to reasonably believe that a TEFCA Security Incident may have occurred, and that such incident may involve an eHealth Exchange QHIN Federal Participant, the eHealth Exchange QHIN Participant shall:

      i. Immediately alert the eHealth Exchange QHIN Federal Participant in accordance with the procedures and contacts provided by such eHealth Exchange QHIN Federal Participant.

      ii. Within twenty-four (24) hours after determining that a TEFCA Security Incident may have occurred and is likely to have an adverse impact on the eHealth Exchange QHIN Federal Participant(s), the eHealth Exchange QHIN Participant shall provide notification to the QHIN Governance Committee of the potential TEFCA Security Incident by sending an email to the dedicated email address: securityevent@ehealthexchange.org (hereinafter "Alert Email").

      iii. Within twenty-four (24) hours after determining that a TEFCA Security Incident has occurred and is likely to have a adverse impact on an eHealth Exchange QHIN Federal Participant(s), the eHealth Exchange QHIN Participant shall provide a notification to all such eHealth Exchange QHIN Federal Participants that may have had a TEFCA Security Incident or otherwise are likely affected by the TEFCA Security Incident in accordance with the procedures and contacts provided by such Federal Participant.

   b. Communication procedure as outlined in 5.b. and 5.c. should be followed.

   c. If, on the basis of the information that the eHealth Exchange QHIN Federal Participant has, the eHealth Exchange QHIN Federal Participant believes that it should temporarily cease exchanging through the eHealth Exchange QHIN, it may undergo a voluntary suspension from the eHealth Exchange QHIN.

Commented [CLR6]: See comment above about this shorter federal notice requirement being *permitted* but not required under TEFCA

Commented [CLR7]: We should consider what the implications are if any of the federal partners are Subparticipants versus Participants. Since federal agencies do not have the benefit of a different notice timeframe under the Common Agreement or Required Flow-Downs, I have honestly not analyzed this from a downstream perspective yet.

Commented [CLR8]: Same comment as above

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

7. The eHealth Exchange CISO is responsible for reporting to and advising the QHIN Governance Committee regarding any reported and potential TEFCA Security Incident(s) and seeking the necessary approvals from the QHIN Governance Committee for responding to the TEFCA Security Incident, including the final determination from the QHIN Governance Committee regarding dissemination of any notification(s) by the eHealth Exchange QHIN in accordance with the Common Agreement.
    a. The eHealth Exchange CISO is responsible for reporting the confirmed or suspected TEFCA Security Incident(s), any updates and/or supplemental information, and the resolution to the QHIN Governing Committee.
8. QHIN Governance Committee Disposition of TEFCA Security Incident Alerts and Notifications
    a. At the earliest possible time following receipt of the TEFCA Security Incident Alert Email, the QHIN Governance Committee Chair shall schedule a meeting of the QHIN Governance Committee, to include the CISO, for the purpose of reviewing the notification and determining the following:
        i. The impact of the TEFCA Security Incident or potential TEFCA Security Incident on the privacy, security, and integrity of TEFCA Information exchanged through the eHealth Exchange QHIN;
        ii. Whether the QHIN Governance Committee needs to take any action to suspend the eHealth Exchange QHIN Participant(s) involved in the TEFCA Security Incident or potential TEFCA Security Incident in accordance with the TEFCA Terms & Conditions.
        iii. Whether other eHealth Exchange QHIN Participants and their Subparticipants that have not been notified of the TEFCA Security Incident or potential TEFCA Security Incident would benefit from a summary of the notification or alert; or whether a summary of the notification or alert to the other eHealth Exchange Participants would enhance the security of the eHealth Exchange QHIN; and:
            1. If the QHIN Governance Committee and the eHealth Exchange CISO determine that a summary should be distributed to the eHealth Exchange QHIN Participants, the eHealth Exchange CISO will obtain the required approval from the QHIN Governance Committee and distribute such summary in a timely manner.
            2. This summary shall not identify any of the eHealth Exchange QHIN Participants or individuals involved in the TEFCA Security Incident.
        iv. Whether the QHIN Governance Committee should take any other measures in response to the notification or alert.
    b. If an eHealth Exchange QHIN Participant reports a potential TEFCA Security Incident and later determines that a TEFCA Security Incident did not, in fact, occur, the QHIN Governance Committee has final discretion regarding whether a meeting is necessary to discuss the disposition of the incident.
    c. The QHIN Governing Committee and/or the CISO QHIN Governance Committee are permitted to request additional information from the eHealth Exchange QHIN

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

Participant(s) involved in the TEFCA Security Incident or potential TEFCA Security Incident to fulfill their responsibilities. However, with respect to potential TEFCA Security Incident alerts, the QHIN Governance Committee is encouraged to hold inquiries and requests for additional information to allow the eHealth Exchange QHIN Participant time to determine whether a TEFCA Security Incident actually occurred.

d. If it is determined a TEFCA Security Incident occurred, and once sufficient information about the TEFCA Security Incident becomes available, the eHealth Exchange CISO and QHIN Governance Committee will meet at the earliest possible time to determine whether the actions taken by the eHealth Exchange QHIN Participant(s) involved in the TEFCA Security Incident are adequate to mitigate the TEFCA Security Incident and prevent a similar TEFCA Security Incident from occurring in the future. Once the eHealth Exchange CISO and QHIN Governance Committee are satisfied that the eHealth Exchange QHIN Participant(s) have taken all appropriate measures, the eHealth Exchange CISO and QHIN Governance Committee will deem the TEFCA Security Incident resolved. QHIN Governance Committee
    i. This resolution will be communicated to all eHealth Exchange QHIN Participant(s) that received notification of the applicable TEFCA Security Incident and any eHealth Exchange QHIN Participant(s) that ceased exchanging with the eHealth Exchange QHIN Participant(s) involved in the TEFCA Security Incident.

Definitions

All capitalized terms, if not defined herein, shall have the same meaning as set forth in the TEFCA Terms & Conditions or the TEFCA Protocols.

References

"TEFCA Terms and Conditions"

- Section 11.1.6, from 45 CFR 164.514, Other Requirements Relating to Uses and Disclosures
- Section 12.3, TEFCA Security Incident Notification
- Section 16.1.4, Survival, Vertical Reporting of TEFCA Security Incident(s)

Related Protocols

eHealth Exchange™

Effective Date: XX/XX/XXXX
Last Revision Date: NA
QHIN Governance Committee Approval Date: xx/xx/xxxx

8300 Boone Blvd., Suite 500, Vienna, Virginia, 22182

EHEALTH EXCHANGE TEFCA SECURITY INCIDENT PROTOCOL

ID	Date	Author	Comments
		Pat Russell	Initial Protocol