eHealth Exchange Feedback Regarding

Standard Operating Procedure (SOP):

QHIN, Participant, and Subparticipant Additional Security Requirements

Published: Not specified in document

URL: https://rce.sequoiaproject.org/wp-content/uploads/2022/11/SOP-QHIN-Participant-and-Subparticipant-Additional-Security-Requirements-for-public-feedback_FINAL.pdf

Feedback from the eHealth Exchange

Prepared by Eric Heflin, Consultant

Introduction

We appreciate the opportunity to provide feedback on this new SOP.

After careful review, we respectfully offer the following suggestions for improvement which we sincerely hope assists the RCE in its efforts.

Any errors are the responsibility of the author, not the eHealth Exchange.

Overall Comments

This new SOP may be overly ambitious at this time due to the burden of implementing MFA and additional audit logging requirements. This may prevent or delay some organizations from joining the TEF. The eHealth Exchange agrees with the direction of this new SOP but recommends a phase-in period of 6 to 24 months (as noted below). In addition, we feel there are potentially other ways to increase security more effectively and with much less burden such as requiring firewall "pinholes" between TEF organizations, which, for a relatively small amount of time and staff expense, can reduce the attack surface area of a healthcare organization by many orders of magnitude.

The following comments are presented in approximate priority-based order, from the eHealth Exchange's perspective.

- [Section 5: Authentication]
    - **eHealth Exchange Comments**: MFA is likely to be a high burden for many organizations. The eHealth Exchange recommends that the RCE not mandate MFA at this time.
- [Section 5: Audit] Requiring ASTM E2147-18
    - **eHealth Exchange Comments**: We agree with this change, but suggest a phase-in period of 12 to 18 months to allow time for vendor upgrades to be developed, procured and placed into production.
- [Section 4] Flowing down the HIPAA Security Rule.
    - **eHealth Exchange Comments:** Flowing down the HIPAA Security Rule to Participant and Subparticipant organizations may force Participants and Subparticipants to re-contract

with all of their internal connections and their workforce. See the next comment for more thoughts on flow-downs.

- [Section 4] "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."
    - **eHealth Exchange Comments**: It is very costly for Participants and Subparticipants to flow down provisions. Each time the flow down terms are changed, many Participants will have to re-contract with all their Subparticipants. The quoted text may have the unintended consequence of delaying Participants and Subparticipants agreeing to participate in the TEF until **all** flow down provisions are published. We respectfully suggest the RCE prioritize publishing all flow-down provisions ASAP to avoid multiple rounds of flow-down provision updates.
- [Section 5: Secure Channel] Requiring TLS 1.2 with BCP-195 or greater versions of TLS
    - **eHealth Exchange Comments**: We agree with this change, but suggest a phase-in period of 6 to 12 months to allow time for vendor upgrades to be developed, procured and placed into production.
- [Throughout] A minor editorial issue: The document has a copyright of 2020 in the footer, and no publication date on the first page.

(end of comments)