2200 River Plaza Drive
Sacramento, CA 95833

Sutter Health

January 13, 2023

General Feedback and Considerations

Sutter Health thanks the RCE for the opportunity to share our feedback about this policy proposal.

Sutter Health is an internationally respected non-profit, integrated health delivery system that encompasses more than 23 hospitals, 33 ambulatory surgery centers, and over 30 other health care centers and facilities serving northern California. The Sutter Health community includes more than 53,000 dedicated team members and 12,000 physicians providing services in support of the organization's mission-driven vision. Sutter Health's mission includes the important work to enhance the well-being of people in the communities we serve through a not-for-profit commitment to compassion and excellence in healthcare services.

Section 3: Definitions

N/A

Section 4: Standard

N/A

Section 5: Procedure

** Authentication – Workforce Members**

Sutter Health is responsible for managing the security of our patients protected health information and the hardware and software in which it is contained. We are concerned about the proposal for a requirement for broad AAL2 multi-factor authentication (MFA) to control access to exchanged data or general PHI and the impact that would have on our operations with limited evidence of need.

HIPAA requires Covered Entities to implement appropriate, risk-based technical, administrative, and physical safeguards. Our organization is subject to HIPAA, and we have experience implementing MFA in targeted, high-risk workflows, such as the ordering of controlled substances. Expanding MFA to encompass all workforce staff with access to TI or PHI (which is virtually all staff, including providers, nurses, schedulers, billers, registrars, and more) will slow care by adding an additional login task to their routine act of logging in to our eHR platform.

According to Epic, our eHR vendor, a typical provider logs into the electronic health record 30 times per day, with a quarter of users logging in 55+ times per day. Experience has shown a strong inverse correlation between system access burden and provider satisfaction. Requiring MFA to be used every time workforce members access TI or PHI is an unacceptable disruption.

In addition to the workflow disruption, expanding AAL2 MFA to all workforce staff will require additional IT infrastructure, expanding the cost of healthcare. For example, physical authenticators or licenses for device applications will be necessitated for all workforce staff.

Because of the incurred cost and burden we believe that requiring AAL2 MFA for all workforce members with access to TI or PHI is unnecessary and unwise. RCE has not provided any evidence that would justify the proposed requirement, nor an analysis of the cost of implementation. We, at Sutter, would have to seriously consider whether voluntarily participating in TEFCA would make sense for our organization if this requirement is finalized.

If RCE believes that existing HIPAA requirements are insufficient to protect TI and PHI, it should work to address it through national policy rulemaking rather than via TEFCA SOP.

Traditionally health IT security is regulated by HIPAA and we would suggest that we continue with that arrangement to not have overlapping and conflicting security requirements.

RCE should compile a cost/benefit analysis that includes real-world estimates of financial and workflow burden.

The analysis should include the specific risks that RCE believes are being mitigated by AAL2 MFA with specific evidence supporting that thesis. It should also include justification for why RCE is pursuing these changes via SOP rather than formal rulemaking. An amended SOP should be released for public comment after that analysis is available.
If RCE believes they must add security regulations to their TEFCA regulations then we would recommend further considerations:
RCE should amend this SOP in the next draft to indicate that AAL2 will be conditionally required using rules-based logic.
Some examples of rules RCE should consider include:

1. When using an on-premises workstation, AAL2 is not required. Access to workstations on-premises is restricted via physical controls.
2. AAL2 is only required once every 24 hours. Requiring workforce staff to perform AAL2 repeatedly throughout the day is an unacceptable disruption.
3. Workforce staff are permitted to use a "remember my device for 30 days" feature. When selected, AAL2 will not be required again until the 30 days expire.

** Authentication – Individuals **
Adding AAL2 MFA as an additional step for Individuals (and their proxies) to access their health information may introduce an additional barrier to patients accessing their own data and actively participating in their healthcare.
RCE should compile a cost/benefit analysis of how AAL2 MFA will burden Individuals' access to their own health information. The analysis should include the risks that RCE believes are being mitigated by AAL2 with specific evidence supporting that thesis. An amended SOP should be released for public comment after that analysis is available.
RCE should amend this SOP in the next draft to indicate that AAL2 will be conditionally required for Individuals using rules-based logic. Some examples of rules that RCE should consider include:

1. When using a provider-controlled network, AAL2 is not required. It is common for Individuals to access their data while in a healthcare facility. For example, MyChart Bedside is a patient-engagement platform that includes an admitted patient as an active part of their healthcare delivery. Patients can message staff, review lab & imaging results, and plan their daily schedules. Requiring AAL2 many times throughout the day while the patient is on-premises is disruptive and unnecessary.
2. Individuals may choose to opt-out of AAL2 if they prefer not to participate.

** Audit Trail **
Federal and state regulations already place obligations on Covered Entities and Business Associates to audit system access and retain records. RCE should align with HIPAA rather than requiring a different auditing standard. Such an approach is better for "future proofing" TEFCA policy because RCE will not risk the scenario where HIPAA is updated in a manner that is incompatible with ASTM E2147-18.
If RCE's concern is specific to Non-HIPAA Entities (NHEs) who are not subject to federal and state regulations, then RCE should target additional auditing obligations to them without affecting Covered Entities and Business Associates perhaps by referring to already well-developed HIPAA rules.

On behalf of Sutter Health, thank you for the opportunity to provide our feedback on this proposed rule. I can be reached at 415-668-8900 or adam.davis@sutterhealth.org with any questions.

Adam Davis, M.D.
Physician Informaticist, Sutter Health
Pediatrician, SF Bay Pediatrics