OCHIN

A driving force for health equity

Submitted via rce@sequoiaproject.org

January 13, 2023

Mariann Yeager CEO
The Sequoia Project
8300 Boone Blvd. Suite 500
Vienna, Virginia 22182

Re: Recommendations on Standard Operating Procedure QHIN, Participant, and Sub participant Additional Security Requirements.

Dear Ms. Yeager,

On behalf of OCHIN, I appreciate the opportunity to submit the following recommendations to the Sequoia Project in relation to *Standard Operating Procedures; QHIN, Participant, and Sub participant Additional Security Requirements*. OCHIN is a national nonprofit health IT innovation and research network with over two decades of experience transforming health care delivery among underserved communities. OCHIN provides leading-edge technology, data analytics, research, health IT workforce training and development, technical assistance, and additional support services to more than 1,000 locally controlled community health care sites, reaching more than 6 million patients in 45 states and supporting more than 21,000 providers. We have serious concerns that two of the proposals will preclude the participation of providers in underserved communities from participating in TEFCA. This would create structural inequities that impact patient care.

OCHIN is committed to driving the widespread development, testing, and adoption of national standards that support interoperability and the suitability of health data for a full range of uses in health care. National data standards are the foundation needed to improve the quality of care, bend the cost curve, and empower patients, while paving the way for payment and delivery transformations, particularly for community-based providers that do not have the resources to comply with varied local, regional, state, and national standards. Further, widely adopted national standards are essential to address structural inequality in health care as well as to mount timely, data-driven responses to public health emergencies. Reducing complexity and duplication not only decreases costs and resource needs but can facilitate solutions that address clinician cognitive fatigue and can contribute to streamlined clinical practice that are critical to address workforce challenges.

FEEDBACK

If the standard operation procedure and policy relating to multi-factor authentication moves forward as written, the outcome will be hesitation by healthcare providers to participate in TEFCA, hindering the national goal of improving interoperability. This policy will weigh heavily on the guidance and considerations we share with our network members who are considering TEFCA participation.

Section 5: Procedure

Authentication – Workforce Members

OCHIN has responsibility to manage security of the collaboratives network, including proposing modifications to the rules that govern network participation. In our many years of running the largest EHR-based Health Center Controlled Network in the country, neither the OCHIN nor its network membership have raised the need for broad AAL2 multi-factor authentication (MFA) to control access to exchanged data or general patient health information (PHI).

HIPAA requires Covered Entities and their Business Associates to implement appropriate, risk-based technical, administrative, and physical safeguards. All of our network members are subject to HIPAA, and all have experience implementing MFA in targeted, high-risk workflows, such as 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 disrupting workflows.

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 that disparately impacts providers in underserved communities who have fewer resources and funding. For example, physical authenticators must be provisioned for all workforce staff. This policy risks pricing smaller providers and critical access hospitals out of participation in TEFCA.

Because of the cost and burden incurred, and the lack of feedback from our network membership regarding the need for broad MFA of all workforce staff, we believe that requiring AAL2 MFA for all workforce members with access to TI or PHI is unnecessary. RCE has not provided any evidence that would justify the proposed requirement, nor an analysis of the cost of implementation.

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.
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.

RCE should amend this SOP in the next draft to indicate that AAL2 will be conditionally required using rules-based logic. We note that rules-based application of AAL2 is typical in industry. For example, in Microsoft products this is referred to as Conditional Access Policy and allows organizations to tailor access policies to match multiple risk level scenarios.
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 and will likely disenfranchise patients in underserved communities that have limited access to smartphones.

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.

Thank you for the opportunity to offer comment and input on the critically important work the Sequoia Project is undertaking. Advancing data standards is a key piece of building true health care equity and access. Please contact me at stollj@ochin.org if we can assist or provide any additional information.

Sincerely,

Jennifer Stoll
Executive Vice President
External Affairs