EHRA
HIMSS ELECTRONIC HEALTH RECORD ASSOCIATION

350 North Orleans Street, Suite S10000
Chicago, IL 60654

@EHRAssociation | ehra.org

January 13, 2023

EHR Association Feedback to the ONC TEFCA RCE on the Draft QHIN, Participant, and Subparticipant Additional Security Requirements SOP

General Feedback and Considerations

As a national trade organization of electronic health record (EHR) developers, the HIMSS Electronic Health Record Association and our 30 member companies appreciate the opportunity to provide feedback on the QHIN, Participant, and Subparticipant Additional Requirements SOP.

While we generally agree with the goal of providing secure access to data by authorized users, we suggest that the proposed approach does not consider existing controls, the prerogative of providers as Covered Entities to be responsible for making the determination of what authentication methods are appropriate for their workforce under HIPAA based on their own understanding of their risk, nor the substantial end-user workflow changes that would be required. Further, the benefits of investments necessary to support the changes in processes and infrastructure to achieve the proposed approach are unclear. As such, the EHR Association suggests narrowing the scope for workforce authentication requirements and auditing standards. We recommend workforce authentication requirements be applied only to the QHIN workforce, with specific consideration given to participants and sub-participants who are not HIPAA Covered Entities. Auditing standards should align with those in place under the ONC Certification Program.

Section 3: Definitions

The general definition of "Workforce" seems broad, while the Procedure section narrowly applies it to specific actors involved with the Trusted Exchange Framework. The EHR Association recommends that the more narrow definition of Workforce be used in this SOP to avoid confusion.

The EHR Association further suggests that the definition of "Individual" be stated here as well for completeness, as we understand this to be a patient, consumer, or proxy exercising their individual right of access.

AdvancedMD
Allscripts
Altera Digital Health
Athenahealth
BestNotes
CPSI
CureMD
eClinicalWorks
eMDs – CompuGroup Medical
Endosoft
Epic
Experity
Flatiron Health
Foothold Technology
Greenway Health
Harris Healthcare Group
MatrixCare
MEDHOST
MEDITECH, Inc.
Medsphere
Modernizing Medicine
Netsmart
Nextech
NextGen Healthcare
Office Practicum
Oracle Cerner
Sevocity
STI Computer Services
TenEleven Group
Varian – A Siemens Healthineers Company

Section 4: Standard

While the general definition of the standards is reasonable, we suggest that adjustments may be necessary to focus on QHIN and non-covered entities more specifically, given our recommended revisions to the section above.

Section 5: Procedure

The EHR Association is concerned that the AAL2, multi- or two single-factor authentication requirement for the entire workforce across QHINs, Participants, and Subparticipants is too broad to be feasible in the current exchange environment.

Currently, the recommended authentication approaches are typically implemented only for targeted use cases, such as e-prescribing in which such authentication is necessary to comply with controlled substance prescribing regulations. Organizations are otherwise not required to deploy the proposed approaches, and there is no reason to consider TI any different from other information that a covered entity currently manages and provides access to users with current controls. Introducing additional authentication requirements for all use cases in which a user is accessing TI or PHI effectively requires that users interacting with PHI must always be subject to these requirements, as isolating the scenarios where they truly are requesting and interacting with TI would interrupt workflow. Additionally, many of the interactions involving TI would be orchestrated by the system on behalf of the provider organization, not necessarily under the authentication of any specific user.

Further, the imposition of this requirement on providers as Covered Entities proposed by this draft SOP encroaches on the prerogative of those Covered Entities to determine their own compliance posture based on their risk assessment, as is required by the HIPAA Security Rule, and the technical security measures appropriate to mitigate identified risks and threat vulnerabilities. We note that extensive network-based interoperability already takes place, and Covered Entities would have assessed the risk under HIPAA and determined that AAL2 is not a control that appreciably mitigates risks associated with network interoperability. The EHR Association strongly urges that the RCE not dictate required technical security measures that would contradict or constrain the use of those that such Covered Entities already have determined for themselves for user authentication not otherwise required by law.

We also recognize authentication requirements may be a consideration for non-covered entities, as TEF intends to manage Participants and Subparticipants consistently, as seen in the Common Agreement which extends specific HIPAA clauses to non-covered entities. Consequently, we believe that given those contractual obligations in this context where all Participants and Subparticipants already need to manage PHI to the same level of privacy and security, the SOP should align with existing requirements to manage PHI where TEF is not part of the fabric, thus focus on the QHIN specifically, and if necessary, non-covered entities and non-business associates which are already subject to HIPAA.

We recognize, however, the special role of the QHIN workforce, for whom we agree that these requirements are appropriate where that workforce may require access to PHI.

We note that Carequality does not have such authentication requirements, nor has identified the need to do so. If there is a need to require this additional level of authentication for covered entities, we suggest that it be done consistently through regulatory processes to ensure PHI meets the same standards and procedures wherever it flows, within an organization, within a network, or outside a network.

We suggest aligning the requirement to adhere to ASTM E2147-18 with ONC's Certification Criterion § 170.314(d)(2), which references § 170.210(e)(1), which in turn references § 170.210(h) - ASTM E2147-18 (incorporated by reference in § 170.299). We note that § 170.210(e)(1) specifically identifies specific sections in ASTM E2147-18. The rationale for differing from ONC certification requirements is unclear. The EHR Association recommends that, for at least Participants and Subparticipants, there is no need for additional requirements.

Established in 2004, the Electronic Health Record (EHR) Association is comprised of 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.