October 26, 2021

Ms. Mariann Yeager
Chief Executive Officer
The Sequoia Project
8300 Boone Blvd.
Suite 500
Vienna, Virginia 22182

RE: Elements of the Common Agreement Request for Stakeholder Feedback

Dear Ms. Yeager:

The Confidentiality Coalition appreciates the opportunity to provide comments on the "Elements of the Common Agreement" (ECA) released by The Sequoia Project as the Trusted Exchange Framework and Common Agreement (TEFCA) Recognized Coordinating Entity (RCE).

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective patient privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

General Comments

The Confidentiality Coalition strongly supports the TEFCA goals to establish a floor of universal interoperability and connectivity to allow greater access to and sharing of health data. This will improve care and allow patients to become more involved in decisions about their care. For the last 21 years, the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules have engendered consumer trust through a rigorous, but flexible, framework for the safeguarding of "protected health information" (PHI) held by health plans, covered health care providers and health care clearinghouses. The Coalition believes that Framework Agreements, including the Common Agreement and standard operating procedures (SOPs), should align with HIPAA to the maximum extent possible, including the implied consent for the exchange of PHI for treatment and payment and health care operations. We applaud the RCE for incorporating HIPAA concepts and definitions in the ECA, and for striving to ensure harmonization with HIPAA requirements.

We also strongly support the ECA's requirement for privacy and security protections for non-HIPAA personal health information. We request more clarity on how these protections will be

enforced for non-HIPAA covered entities. Since the passage of HIPAA in 1996, and in the past few years, there has been an exponential increase in health data use and exchange that falls outside the HIPAA regulatory framework.[1] The proliferation of consumer-facing health apps that generate and/or collect health data, coupled with big technology's data gathering and analytic capabilities, means that an increasing share of personal health data needs the robust privacy and security protections afforded to PHI. Considering this, we believe that it is of paramount importance for the Common Agreement to require strong privacy and security protections for non-HIPAA health data similar to the standards provided by HIPAA for PHI. It is equally important that there be enforcement of these requirements through meaningful penalties in the event of non-compliance. This will not only engender consumer trust in the TEFCA framework; but will lead to greater participation by individuals and their caregivers, a key goal of the 21st Century Cures Act and TEFCA.

Specific Comments

1. Definitions

The Common Agreement would define certain key terms, including "TEFCA Information" and "Required Information." TEFCA Information is defined very broadly to include any information that is exchanged between Qualified Health Information Networks (QHINs) for one or more of the exchange purposes. The ECA explains that TEFCA Information also includes HIPAA de-identified information, although the HIPAA Privacy Rule protections would not apply to de-identified information. "Required Information" is electronic protected health information (ePHI) that is a subset of TEFCA Information that must be provided in response to a request for an exchange purpose unless an exception applies. The ECA defines ePHI using the language laid out in HIPAA.

The Confidentiality Coalition appreciates the ECA providing key definitions and explaining their application. We also strongly support aligning the Common Agreement definitions with their HIPAA counterparts and commend the RCE for hewing as closely as possible to the HIPAA definitions. This will not only allow harmonization with HIPAA, but also allow the Common Agreement to thereby incorporate the well-understood parameters of these definitions and concepts that have been established through HIPAA guidance over many years.

We are concerned, however, that having several definitions for the term "data" subject to different elements of the Common Agreement will cause some confusion, as well as potential gaps. We recommend that the ECA clarify the rationale for including HIPAA de-identified data as part of TEFCA Information, since this is not Required Information, nor is it subject to HIPAA Privacy Rule protections. The ECA also does not address other de-identified information (i.e., de-identified data, however de-identified, that is generated from personal health information that is not PHI, such as de-identified data created by consumer-facing applications and other non-HIPAA entities). It is also not clear whether the only difference between TEFCA Information and Required Information is that the former includes de-identified data. The definition of ePHI is also confusing, since it is defined as a subset of PHI, but then the ECA states that Required Information includes ePHI of non-HIPAA entities, even though these entities do not hold ePHI. We request that further clarification be provided about the extent to which the intention is to define ePHI in the same way as defined in HIPAA, regardless of whether the data is exchanged by a HIPAA covered entity or business associate.

[1] Antonio Reynolds, *With Health Apps on the Rise, Consumer Privacy Remains a Central Priority*, JD Supra (February 19, 2021), https://www.jdsupra.com/legalnews/with-health-apps-on-the-rise-consumer-8744752/.

Finally, we ask that the RCE consider including definitions for all key terms, such as “Signatory,” “Request,” and “Response,” to name a few that are not included in the ECA Definitions.

2. Exchange Purposes

The ECA lists six initial exchange purposes for which information may be requested and shared for QHIN-to-QHIN exchanges. These include treatment, payment, and health care operations, as these terms are defined by HIPAA, as well as public health, benefits determination, and individual access services (IAS). The ECA states that the RCE plans to work with stakeholders to identify additional exchange purposes over time and gives as an example biomedical research.

The Confidentiality Coalition supports the inclusion of the six listed exchange purposes, and the alignment of the definitions of treatment, payment, and health care operations with the HIPAA definitions of these terms. We support the incremental approach of starting with the six core exchange purposes identified in the ECA, since this will allow the RCE to prioritize these key functions and focus on ensuring that the Framework is operating as intended before expanding its scope. Once the Framework is fully operational and the RCE has had an opportunity to evaluate its operations and functioning, we recommend that it then work with stakeholders to consider including other appropriate exchange purposes and to share a proposed timeline and process for doing so. We caution that as additional use cases are added, considerations will be needed to ensure applicability and appropriateness of existing components (including definitions) of the ECA. We believe that biomedical research would be an appropriate exchange purpose and that protections should be included for this data if it falls outside of HIPAA.

We note that the ECA would include as an exchange purpose the health care operations of non-HIPAA covered health care providers, but not those of other non-HIPAA entities, such as social service agencies. As Footnote 1 of the ECA makes clear, this would mean that a social service agency that is not a health care provider could request health information as an IAS provider or contractor to a health care provider, but not for its own care coordination purposes. Given that covered health care providers and health plans may disclose PHI to social service agencies for care coordination purposes under HIPAA (and the 2020 proposed HIPAA Privacy Rule would add regulatory text to make this clear), it may be appropriate to allow such entities to request health information for their care coordination purposes in addition to doing so on behalf of an individual as an IAS, provided patient information continues to receive robust privacy and security protections.

We also note that the information exchange described in the ECA draft currently is for Request-Response only between stakeholders. Inclusion of additional approaches, such as the Publish-Subscribe model, would allow real-time dynamic information updates across all authorized participants without the need for pushing the Requests and pulling the Responses each time information is needed.

3. Participants and Sub-participants

The ECA envisions a network of QHINs to share health information on behalf of contracting participants, and for participants, in turn, to share information on behalf of contracting sub-participants. The ECA states that stakeholders would connect at the point that is most appropriate for them. However, the ECA appears to contemplate that a “health information exchange, health IT software developer, health care system, payer, or federal agency” would connect as participants, whereas a physician practice, hospital, pharmacy, or public health agency would connect as a sub-participant.

The Confidentiality Coalition appreciates the flexibility of the proposed structure but requests the RCE provide guidance on the distinction between participants and sub-participants, particularly as it relates to their different obligations and responsibilities and the circumstances under which a health care organization would be required to become a sub-participant to utilize the QHIN network. For example, if a health system that is a participant owns several hospitals, those individual hospitals should not have to sign sub-participation agreements. Similarly, if an entity owns a chain of pharmacies, only one data exchange agreement should be necessary, although it is not clear based on current information whether it would be more appropriate for that agreement to be at the participant or sub-participant level. It would also be helpful for the RCE to further clarify to what extent the RCE envisions other non-HIPAA covered entities, such as researchers, pharmaceutical manufacturers and their hubs, social service agencies and community organizations, healthcare clearinghouses and other stakeholders to participate, and why. Additional conversations are needed across stakeholders if additional non-HIPAA covered entities are able to participate and request information.

4. Individual Access Services (IAS)

The ECA states that the Common Agreement anticipates that individuals could use an account with a connected consumer-facing application or platform to request their health information from participating entities. IAS are defined broadly as the services provided by any QHIN, participant or sub-participant, to an individual to satisfy that individual's request to access, inspect, or obtain a copy of that individual's TEFCA Information. IAS providers would be required to adhere to additional privacy and security requirements, including a written privacy notice with specified elements, obtaining express consent from individuals regarding the way their information will be used or disclosed, and providing individuals with certain data rights, such as the right to delete and to obtain an export of their data in computable format.

The Confidentiality Coalition believes that it is important to recognize the need for robust privacy and security requirements for consumer-facing apps that have access to consumer health data, and for specifying these requirements in the Common Agreement. We have long advocated for a national consumer privacy law to protect health data that falls outside of HIPAA and have called for such legislation to harmonize with HIPAA so as to allow the seamless flow of health data across the health ecosystem without any degradation to its privacy or security. Until such time as Congress acts to pass such a law, it is imperative that the TEFCA Framework, which will form the backbone for universal interoperability, ensure that such improved data exchange does not come at the expense of consumer data privacy and security, and overall consumer trust.

Given the breadth of the definition of IAS, however, the activities of many HIPAA covered entities and their business associates could potentially fall under this exchange purpose, potentially categorizing them as IAS providers. For example, consistent with a patient's rights under HIPAA, a patient might ask their current health care provider to obtain their electronic health record from a previous health care provider. In this situation it is not clear whether the ECA would view this as an IAS purpose or a treatment purpose of the health care provider, and on what basis it would make this distinction. To the extent a HIPAA covered entity, or its business associate performs activities that could fall under IAS, and so make it an IAS provider, we recommend that the Common Agreement make clear that such entities' privacy and security obligations are governed by HIPAA, and that such entities would not be subject to the additional privacy and security requirements applicable to consumer-facing applications and other non-HIPAA IAS providers.

We recommend a layered approach to implementing individual access services. First, it should focus on consent and revocation of data being shared as an initial layer. As the authentication

and consent model is more fully developed, then additional data access should be added. This would ensure that privacy and security concerns have been fully analyzed and addressed.

5. QHIN Designation and Eligible Criteria

We note that the 12-month provisional QHIN status may inhibit new exchange solutions and reduce innovation and competition. We recommend reduction of the provisional period as a means to balance opportunities between new and existing health information exchanges. The Coalition also encourages the Common Agreement to support new technologies to ensure information sharing is supported by up-to-date solutions addressing privacy and security. Integrating these platforms will better enable stakeholders to take advantage of innovative solutions to improve data sharing in a responsible manner.

6. Privacy and Security

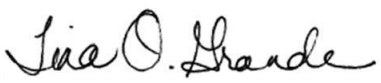
The ECA states that the Common Agreement would require non-HIPAA entities to protect TEFCA Information that is individually identifiable in substantially the same manner as HIPAA covered entities protect PHI, including having to comply with the HIPAA Security Rule and most provisions of the HIPAA Privacy Rule. It adds that QHINs would be expected to meet and maintain third-party certification to an industry-recognized cybersecurity framework and undergo annual security assessments, and that the Common Agreement would specify expectations for security incident notifications that would flow down to participants and sub-participants. These provisions would be designed to avoid conflict with applicable law and duplicative notification requirements.

The Confidentiality Coalition commends the RCE for it focus on strong privacy and security protections that align with HIPAA. We agree that this alignment will promote trust, and that this trust will, in turn, encourage participation. We also appreciate the RCE's effort to avoid conflicts with existing laws and duplicative requirements. In that regard, we would like to confirm that HIPAA covered entities and their business associates will not be subject to the additional third-party certifications, annual security assessments or security incident notifications referred to in the ECA, given that these entities are already subject to the HIPAA Security Rule, as well as the HIPAA breach notification Rule, upon which the ECA's definition of a TEFCA Security Incident is based.

Summary

The Confidentiality Coalition looks forward to working with you as you implement the components of the TEFCA Framework that will usher in an era of universal interoperability leading to improved patient care and engagement. Please contact me at tgrande@hlc.org or 202-306-3538 with any questions.

Sincerely,



Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council