CARIN Alliance Comments to Recognized Coordinating Entity on the Proposed Elements of the Common Agreement

To the Sequoia Project (Recognized Coordinating Entity) and the Office of National Coordinator,

We appreciate the work that has been done to advance the Trusted Exchange Framework and Common Agreement. As you may know, the CARIN Alliance is a multi-sector group of stakeholders representing consumers, patients, health systems, insurers, technology organizations, personal health record developers, and others. We are universally committed to enabling consumers and their authorized caregivers easy access to their personal health information. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via open APIs. We are grateful that the proposed Common Agreement anticipates the use of consumer-facing applications.

The CARIN Alliance fully supports many components and elements of the proposed Common Agreement. We are especially thankful to the RCE for including Individual Access Services (IAS) as one of the exchange purposes subject to a required response with Required Information, with narrow exceptions. As part of this access, we encourage you to consider the additional needs for consumers seeking to access their information through the Trusted Exchange Framework (TEF):

1. **Advancing the Use of Fast Healthcare Interoperability Resources (FHIR) and other standardization.** As noted above, we are grateful that the RCE recognizes the value of consumer-facing applications and the utility of standards-based application programming interfaces (APIs), including the FHIR standard. We support the eventual transition to the use of standards-based APIs, specifically FHIR resources. We appreciate that this transition is on the technical roadmap for the RCE. We believe this transition is important for the ultimate success of the Individual Access Services element as the use of FHIR APIs and the standardization occurring at FHIR patient access API endpoints is already advancing consumer-directed exchange. We believe FHIR patient access APIs through the TEF will advance consumer-directed exchange by eliminating the need for consumers to create portal credentials at each of their providers and payers before accessing their data. Eliminating this step will not only remove friction from the consumer experience but contribute to building consumer trust in consumer-facing applications that agree to the Common Agreement's privacy, security and IAL-2 digital identity proofing standards for IAS providers.

2. Optionality of Offering Individual Access Services:
    a. We agree that Individual Access Services should be a required exchange purpose for QHINs, Participants, and Sub-participants. We endorse the use of flow down provisions to enforce this requirement in the QHIN CA to Participants and Sub-participants.
    b. We believe the concept of Individual Access Services should be clarified, to make clear that the act of responding to an Individual Access Services request is not Individual Access Services.
    c. We endorse that privacy and security standards should be imposed on any provider of Individual Access Services as a condition of participation in the Common Agreement (but see further comment below).

d. While we agree that Non-HIPAA Entities offering Individual Access Services should not be required to respond to Exchange Purposes, we also believe this carve out should apply equally to HIPAA Covered Entities and Business Associates that provide Individual Access Services. We'd like to draw the RCE's attention to the fact that information created, received, or shared as part of Individual Access Services must be managed, shared, and controlled by individuals, consistent with the HITECH definition of a "personal health record". CARIN Alliance can point to examples of HIPAA covered entities and business associates that offer PHR functionality for patients and plan members.
e. Moreover, the data maintained by HIPAA covered entities or their business associates to support PHR functionality should not be considered "designated record sets" that require interoperability in response to requests for required exchange purposes. When considering this comment, we draw your attention to the fact that not all business associates providing PHR functionality are covered actors under the Information Blocking Rule. Moreover, HIPAA covered entities participating in the TEF may choose to respond to required requests through one or more designated business associates, rather than by each business associates that also participates in the TEF as a QHIN, Participant or Sub-Participant.
f. We support the proposal that a QHIN, Participant, or Sub-participant can voluntarily offer individual access services to persons with whom they have a direct relationship. As QHINs, Participants, and Sub-participants become more sophisticated and experienced in providing Individual Access Services, these direct relationships will allow for greater information sharing with consumers, including sharing through standards-based APIs.

3. As QHINs, Participants, and Sub-participants share information for Individual Access Services, it is critical to maintain clarity around who can query for individual services and how applications can facilitate that activity. Additionally, it is critical to ensure that Individual Access Service providers should offer protections like those outlined in the CARIN Alliance Code of Conduct. However, we also believe that IAS provider privacy and security requirements should only apply when providing those IAS services (as opposed to other use cases that the provider may support).

4. As the RCE moves forward in implementing both the Trust Exchange Framework and the Common Agreement, it is critical that the Agreement not set ID proofing or matching requirements in a way that discriminates against Individual Access Services providers. Similarly, the TEF should not require IAS providers to do more for ID proofing than other network participants. We would recommend the RCE move to adopt the NIST 800-63-3 IAL2 standard for all participants and adopt the digital identity federation framework being developed, implemented, and piloted by the CARIN Alliance and the Department of Health and Human Services (HHS) which can be found on our website called 'Digital Identity and Federation in Health Care'.

5. Regarding the requirement of all entities, including non-HIPAA covered Individual Access Services providers, to abide by most of the HIPAA Privacy Rule and the HIPAA Security Rule, we disagree with the framing that "most of the Privacy Rule" provisions should apply to consumer-facing apps. Individuals using apps should have stronger rights to control their data (vs. having that data subject only to HIPAA's permissions like TPO). Additionally, security incident notifications should

be consistent with existing breach notification obligations (whether HIPAA or HITECH) and should focus on threats to the network (existing definition of security incident aligns more with the HIPAA breach notification definition than those for personal health records under HITECH). As noted above, however, we do support privacy and security requirements for IAS services. We encourage the RCE to consider the CARIN Code of Conduct as the model for IAS providers to provide privacy and security, including by requiring proactive individual consent for additional data sharing activity.

6. We recommend that the elements of Common Agreement make clear that a patient consent can be collected via an E-SIGN Act compliant means. As currently written, the Common Agreement requires that consent should follow HIPAA, but HIPAA doesn't require the acceptance of a digital signature.

7. We strongly support a broad description of required information that must be exchanged by TEF participants for the Exchange Purposes. For IAS, the information required to be shared in response to a query should be any electronic protected health information that meets the definition of "designated record set" under the HIPAA Privacy Rule.

8. Representatives of patients and Individual Access Services providers should be included in the various governing bodies. At present, most representation and input from patients and IAS providers has been accomplished through listening sessions and public comment opportunities. We believe that it is critical for the patient, caregiver, and consumer voice to be present in all RCE considerations and the ongoing development of the TEF and iteration of the CA. Additionally, as flow-down provisions for IAS providers exist, it is critical that their perspective is also represented.

Additional Considerations and Recommendations to HHS:

1. It is critically important that the provisions of the Common Agreement align with HIPAA and other regulatory requirements. Therefore, it will be critical to the success of TEFCA for ONC and OCR to clarify the role of Business Associates (BAs) who are "actors" under the information blocking rule regarding information sharing (i.e., the BAA should not be used to limit information sharing otherwise permitted or required by HIPAA).

2. ONC should also move quickly to enhance the value of participating in TEFCA by tying robust participation to the information blocking rules (i.e., presumption is that an actor is appropriately sharing EHI if participating in the TEFCA).

3. ONC should provide more details on what scenarios fit into the bucket of exchange of non-health information given the health "orientation" of the required purposes.

Again, we appreciate your work here and your consideration of our comments. If you have any questions or additional follow-up, please contact me at david.lee@leavittpartners.com.

Thank you for considering our comments and recommendations.

David Lee
Leavitt Partners
On behalf of the CARIN Alliance