CARIN Alliance Comments to Recognized Coordinating Entity on the Current Draft IAS Provider Privacy and Security Notice and Practices SOPs

To whom it may concern,

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 Draft IAS Provider Privacy and Security Notice and Practices SOPs.

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

Common Agreement Section 10.3.1.(i): "Be publicly accessible and kept current at all times, including updated versions"
We are supportive of this requirement.

Common Agreement Section 10.3.1.(ii): "Be shared with an Individual prior to the Individual's use/receipt of services from [the IAS Provider]"
We are supportive of this requirement.

Common Agreement Section 10.3.1.(iii): "Be written in plain language and in a manner calculated to inform the Individual of such privacy practices"
We are very supportive of the Sequoia Project's efforts to create standards for IAS Providers in order to ensure trust across the TEFCA network. Similar concerns about consumers needing to choose personal health apps without good, clear information about the app's policies, procedures and safeguards drove us to develop the CARIN Alliance Code of Conduct, and we appreciate that you have referenced the Code and the CARIN UX Guide in the appendix of this SOP. We have a number of comments that we hope will strengthen the SOP.

As a threshold matter, we urge the Sequoia Project to limit this SOP to objective requirements that can be adopted by IAS Providers and that ideally can be measured without application of subjective judgement. Individual Access Services is a TEFCA purpose that is too often met with a great deal of suspicion and, in some cases, hostility. We agree with setting the bar high - but the bar should also not be set in a way that provides a mechanism for the SOP criteria to be applied inconsistently, or in ways that make it unreasonably difficult for IAS Providers to connect to the TEFCA. For example, the SOP should focus primarily on the plain language standards (https://www.plainlanguage.gov/guidelines/) required by the federal government versus setting an arbitrary grade 6 reading level threshold which is subject to a subjective standard. As another example, we note the requirement to make the privacy policy available in English, Spanish, and other languages spoken by users of the app. Who decides what other languages must be offered by the app? To avoid a subjective judgement call that an IAS Provider is ineligible to connect to TEFCA due to failure to have a privacy policy in a particular language, we urge Sequoia Project to set some objective standard such as ensuring IAS providers provide culturally appropriate language accommodations based on what populations the IAS Provider may be targeting for its services. For example, Medicaid follows a rule that says if 5% of the covered population speaks a given language then member materials and the website must provide support for those languages.

We agree that the privacy policies and terms of service for IAS Providers should be required to include certain elements, and much of what is in this draft SOP mirrors the CARIN Code of Conduct. That said, we'd like to draw your attention to added SOP criteria on top of the Common Agreement's requirements, which create new areas for interpretation. For example, in connection with requiring express consent, the SOP criteria introduce the concept that consent be in writing without elaborating on the meaning of "written". Perhaps a better approach would be to specify that the consent to authorize an IAS Provider to engage in Connectivity Services on an Individual's behalf be presented unambiguously to the Individual as an opt-in choice, and not buried in a lengthy privacy policy.

Similarly, a new criteria requires a signature to meet federal e-signature requirements. The federal E-signature Act provides for a number of acceptable mechanisms for capturing an individual's agreement in e-commerce, which can range from checking a box to use of signature software such as what is present in Adobe Acrobat or DocuSign. Most individuals interact with applications and other online tools by indicating their assent digitally, without the need for something that looks like a wet signature or

requires the use of additional, out-of-band or off-platform processes. We understand this criteria to mean that any/all mechanisms appropriate under the ESIGN Act are appropriate for use in demonstrating the collection of a consent. If that is the RCE's intended interpretation, perhaps the SOP could include more detail reinforcing this interpretation. Moreover, if the intent is to generate a consent artifact for audit or verification purposes, perhaps the SOP could include examples of how that could be accomplished.

Overall, we agree that it is important that consent for sharing data not be buried in a long, general consent to use the product. We agree that the consent be, to the extent possible, knowing, informed and collected in a way (and at a time) that gives Individuals appropriate context to make a voluntary and affirmative decision (not an "opt out", for example). The Code of Conduct addresses these considerations by requiring separate, express consent for data sharing, including sharing for marketing purposes.

We also urge the RCE to focus on strengthening those aspects of the SOP that make it more likely that IAS Providers offer consumer education *in addition to* privacy policies and terms of service, so that consumers are informed about their rights under HIPAA and the Common Agreement. We appreciate the RCE's reference to the CARIN UX Guide. The CARIN app community looks forward to helping to communicate the best practices captured by the Guide, which reflects CARIN's belief that consumer-friendly education about an IAS Provider's privacy and security practices is more meaningful than a required "Privacy and Security Notice" heading and more easily achieved than writing a privacy policy at a 6th grade reading level. In the end, the criteria should be whether IAS Providers make an effort to inform and empower their consumers, by ensuring key data practices are read and understood by individuals, and that individuals are actually permitted to make choices versus being forced into default data sharing arrangements.

Along similar lines, we urge the RCE to not limit its focus on just the privacy policy document when considering how an IAS Provider can be transparent and clear to all users about its policies regarding the information it collects and the rights granted to consumers using the product. Privacy policies are often asked to serve many purposes: first, to be a tool of transparency to users and the public, and second, to be a legal document regarding the standards to which the company offering the app will be held. Because of this second purpose - that the document is legally binding on the company - privacy policies and terms of service are often written by attorneys and often must explain the company's policies on issues that are difficult to explain in plain language. A number of consumer-facing companies, recognizing that it can be difficult to serve both purposes with one document, have both a privacy policy and a separate section of their website that summarizes the key components of the policy using plain English and in easier-to-understand language. Further, apps attesting to the CARIN Code of Conduct answer a series of questions about their data practices that allow consumers to compare practices of different apps and focus on the questions and issues that are usually most important to individuals making choices about online services. We urge the RCE to allow IAS Providers to demonstrate adherence to the SOP through all consumer-facing educational resources and not just a focus on the legal documentation (privacy policy and terms of service), assuming there is no conflict between the legal documentation and the other materials.

Also, given the SOP's citation to HHS and FTC statements seeking to make privacy policy statements "clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices," we'd like to direct your attention to the standardized data practices questionnaire contained in the CARIN App Registration IG. We developed this questionnaire in response to guidance

accompanying the CMS Patient Access and Interoperability Rule, in which CMS recommended its payers to adopt an app attestation workflow. The questionnaire provides a model framework – consistent with the CARIN Code of Conduct – that the RCE could require of IAS Providers, so that they will disclose their privacy and data practices in a consistent fashion. This approach will go far in providing a more meaningful apples-for-apples comparison standard in the RCE's goal of setting a universal floor for interoperability.

Common Agreement Section 10.3.1.(iv): "Include a statement regarding whether and how the Individual's TI may be accessed, exchanged, Used, and/or Disclosed by [the IAS Provider] or by other persons or entities to whom/which [the IAS Provider] Discloses or provides access to the information, including whether the Individual's TI may be sold at any time (including the future)"
We are supportive of this requirement.

Common Agreement Section 10.3.1.(v): "Include a statement that [the IAS Provider] is required to act in conformance with the Privacy and Security Notice and must protect the security of the information it holds in accordance with Section 10 of [the] Common Agreement"
We are supportive of this requirement.

Common Agreement Section 10.3.1.(vi): "Include information regarding whom the Individual may contact within [the IAS Provider] for further information regarding the Privacy and Security Notice and/or with privacy-related complaints"
We are supportive of this requirement.

Common Agreement Section 10.3.1.(vii): "Include a requirement by [the IAS Provider] to obtain express written consent to the terms of the Privacy and Security Notice from the Individual prior to the access, exchange, Use, or Disclosure (including sale) of the Individual's TI, other than Disclosures that are required by Applicable Law"
Please review our comments in 10.3.1 (iii) regarding this topic especially the eSIGN provisions.

Common Agreement Section 10.3.1.(viii): "Include information on how the Individual may revoke consent"
We agree with this recommendation, however we believe it's important to note that we do not want users to accidentally revoke access since this is a destructive action that could result in users losing access to core functionality of the 3rd party app. In our UX guide, we state that "Revoking should trigger a confirmation dialog to ensure the user does not revoke consent by accident and provide a way back to safety."

Common Agreement Section 10.3.1.(ix): "Include an explanation of the Individual's rights, including, at a minimum, the rights set forth in Section 10.4" [of the Common Agreement]
We are supportive of this requirement.

Common Agreement Section 10.3.1.(x): "Include a disclosure of any applicable fees or costs related to IAS including the exercise of rights under Section 10.4 of [the] Common Agreement"
We are supportive of this requirement.

Common Agreement Section 10.3.1.(xi): "Include an effective date" [of the written Notice and an effective date of any subsequent material changes to such Notice]
We are supportive of this requirement.