CARIN Alliance Comments to Recognized Coordinating Entity on the Current Draft IAS Exchange Purpose Implementation SOP

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. We are pleased 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 Exchange Purpose Implementation SOP.

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 ryan.howells@leavittpartners.com.

Thank you for considering our comments and recommendations.

Ryan Howells
Leavitt Partners
On behalf of the CARIN Alliance

Credential Service Provider

IAS Providers are required to have an agreement with a credential service provider (CSP) who has been approved by an RCE-selected CSP approval organization. The CSP approval organization must maintain a published list of CSPs who conduct identity proofing to Identity Assurance Level (IAL) 2 as defined by the then latest version of NIST SP800-63A. The CSP approval organization must require approved CSPs to be assessed for conformance to the minimum appropriate identity proofing and credential management standards, and to publish and maintain the standards to which the CSPs are assessed.

CARIN agrees with an 'RCE-selected CSP approval organization.' We would strongly recommend the RCE initially leverage existing trust framework certification organizations who have done this for many years. We would also recommend the RCE define what an 'RCE-selected approval organization' or trust framework is. Our definition is an organization that curates, independently assesses and enforces a collection of policies, technical specifications, and interoperability criteria that are accepted by a diverse set of stakeholder participants to satisfy a particular need. In the case of digital identity in online transactions, a Trust Framework provides policy and technical interoperability for the issuers of digital identity credentials, the individuals asserting their identities through the use of the credentials, and the organizations relying on the identity assertions linked to the digital credentials. Trust Frameworks accredit or certify organizations against the criteria, developed through consensus, in an effort to build trust among participants. These organizations also require the use of independent assessors, provide well-exercised processes, employ a valid appeals process, and provide timely approvals. Long-established trust framework organizations include Kantara International and the DirectTrust project. Just as there will be a marketplace of CSPs who use different technologies (API and PKI), we believe the RCE should recognize more than one trust framework organization to serve as a CSP approval organization. This would imply the eventual adoption by the RCE of a common digital identity trust framework agreement for IAL-2 digital identity certification that would be incorporated into the Common Agreement. We believe the work the CARIN Alliance has done and will be releasing later this year for public comment and consumption could help the RCE in that effort.

The CARIN Alliance has worked on a weekly basis for more than a year to develop an interoperable open digital federated trust agreement so the industry can leverage multiple CSPs using multiple different technologies. This agreement will allow for multiple technologies (e.g., API (NIST 800-63) and PKI (RFC 3647 and NIST 800-53)) to work together seamlessly because it will establish policy equivalency across multiple trust frameworks or RCE-selected CSP approval organizations. Without this agreement, RCE-selected CSP approval organizations or trust frameworks will not be interoperable with each other and the RCE will need to select a single technology standard and likely a single trust framework organization to implement the TEFCA.

As an example of where policy equivalency across trust framework organizations is needed, a digital credential has differing timeframes for when the credential needs to be reissued based on which technology (API or PKI) or which trust framework is used. We have come to consensus

on these types of topics regardless of which technology or trust framework is used whether it's based on NIST 800-63, NIST 800-53, or RFC 3647. You can read more about how we have organized our work in the whitepaper we wrote in 2020 (https://www.carinalliance.com/wp-content/uploads/2020/12/LPCA_CARIN-Alliance-Federated-Trust-Agreement_FINAL-12.3.2020.pdf).

We look forward to publishing an initial draft of our work later this year for the community to comment on and use as they see fit. We have spoken to the Federal PKI team and NIST who have both expressed interest in leveraging our work for their purposes and to help scale FALs. We would welcome the opportunity to further discuss our work with the ONC and RCE at your convenience. -

We have supported setting the standard for credentialing at IAL2, per the latest version of NIST 800-63, since 2017. However, it is important that the RCE knows that NIST plans to release a draft of NIST 800-63 v4 in the Fall for public comment and workshops. Based on conversations with NIST, we have been told v4 will be updating IAL1 to fall somewhere between the current IAL1 – IAL2 identity assurance. The CARIN alliance will be closely watching what NIST updated guidance in the Fall that will describe the new IAL1. We want to make sure the level of identity proofing provided in the marketplace doesn't pose an undue barrier to those who want to access their own health care information. We also want to make sure we strengthen the ability for users to authenticate into health care systems using modern technologies. We believe we can do both. In sum, we believe that for the initial rollout of the TEFCA and individual access services, the industry can support the NIST 800-63 v3 of IAL2 with the support of trust framework organizations who support that same version. Once NIST releases v4, we will be examining the new IAL1 and any additional changes they plan to make and then discussing whether the new IAL1 makes sense to use for IAS. It's important to note the CSPs, industry, applications, and certification organizations fully support IAL2 today and are actively implementing tools that support it.

Identity Verification Requirement

Identity Verification Requirement. IAS Providers are required to verify the identities of Individuals via a CSP prior to the Individual's first use of Connectivity Services, and then again after credentials expire. a. Verification must include, at a minimum, the following demographics: First Name, Last Name, Date of Birth, Current Address, City, State, ZIP, Sex. b. Verification should also include, but does not require, Middle Name, Middle Initial, Suffix, Email Address, Mobile Phone Number, SSN, SSN last 4 digits, ZIP+4, Medical Record Number, and other identifiers.

Overall, we would recommend separating attributes for ID verification (IAL2) that can be validated from additional patient matching components. The industry (both EHRs and CSPs) support attributes for ID validation today but the additional matching components cannot be validated. We would also recommend the RCE use the NIST definitions of validation and verification. There is a difference between those two terms.

According to NIST 800-63A, Section 5.2, validation means:
The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: collecting the appropriate identity evidence, confirming the evidence is genuine and authentic, and confirming the data contained on the identity evidence is valid, current, and related to a real-life subject.

It's currently not possible to validate attributes that are not part of a government issued ID. We support the use of validated demographics for Individual Access. Specifically, we support First Name, Last Name, Date of Birth, Current Address, City, State, and Zip. Each of those attributes are able to be validated and referenced within NIST 800-63-3. There is not currently NIST 800-63 guidance on validating 'Sex' and 'Medical Record Number' and those attributes are not required to meet IAL2. We recommend the RCE only require for identity purposes the minimum number of attributes that can be validated and are required by the NIST 800-63 guidance.

Additionally, for the list of demographics that are not required but should be included for ID proofing, we recommend removing Medical Record Number and SSN. CSPs cannot validate this information, so inclusion in the list of demographics for ID proofing doesn't make sense. Those data elements may make sense to use for better patient matching but not for ID proofing.

Evidence of Individual Identity Proofing

IAS Providers are required to demonstrate that all Individuals that elect to use their IAS offering have proven their identities consistent with achieving NIST IAL2.
a. The user proof of identity verification will be included in the QHIN Query or QHIN Message Delivery request SAML via a tag set which includes:
i. comprising the Business Name or URL of the CSP and,
ii. with a comma or space separated list of the user demographics and identifiers that have been verified by the CSP.
b. The following is an example SAML information block identifying the CSP organization and the list of verified attributes: http://www.example-csp.com
lname,fname,address,city,state,email,ssn,sex
c. The codes for the verified attributes are as follows:
A second historical demographic may have a numeric designation appended (e.g., hfname2). Numbering of additional historical codes begins at 2 and should not skip numbers. e. No IAS Request without the above SAML tags is to be processed. If an IAS Request lacks the above required SAML tags, an appropriate error must be returned.

We are not aware of any CSP that validates a prior name or any of the additional attributes listed above. Again, we would strongly recommend only requiring the attributes for identity that are listed in the NIST 800-63 guidance and can be validated via government issued sources. The additional data elements will be helpful for patient matching but not ID proofing.

Use of Proven Demographics

IAS Providers are required to submit queries to the QHIN that include as primary demographics only the demographics as provided to the CSP and verified to NIST IAL2. a. Historical name and/or address information may also be included if and only if verified by the CSP for identity proofing for that individual. b. Historical information must be marked as historical.

We agree with the position that IAS Providers should be the ones to submit the queries to the QHIN, and that those queries should include, for identity proofing processes, only the demographics as provided to the CSP and verified to NIST IAL2 (the IAS Providers have the relationship with the patient and have been requested by the patient to make queries for their health records, and receive those records in return). We are not aware of any CSP that validates a historical name or address or any of the additional attributes listed above. Again, we would strongly recommend only requiring the attributes for identity that are listed in the NIST 800-63 guidance and can be validated via government issued sources. The additional data elements will be helpful for patient matching but not ID proofing.

Response

QHINs, Participants, and Subparticipants that receive a QHIN Query for an IAS Exchange Purpose that provides the information specified in (3) and (4) and provides an acceptable match, based on responder policy, are required to Respond with the Required Information per the Common Agreement, the QHIN Technical Framework, and the Exchange Purposes SOP.

We strongly support this provision. We believe that it is imperative for all QHINs, Participants, and Subparticipants who receive a QHIN Query for an IAS Exchange Purpose be required to respond with the required information per the Common Agreement and SOPs. We believe this is critical to ensuring wide availability of IAS services across the TEFCA environment. If the RCE and TEFCA do not require a response, we have not meaningfully advanced IAS in the US. Individuals have a right to access all of their health information and we believe TEFCA can help make that easier and more efficient than what is happening today.

Certified Changes Only

An IAS Provider is required to ensure that all updates to demographic information transmitted via Connectivity Services for the IAS Exchange Purpose have the demographics verified to NIST IAL2 by the CSP prior to their use.

1. What are the policy, legal, and/or regulatory challenges that may impact the ability of TEFCA QHINs, Participants, or Subparticipants to respond to IAS Requests based on demographics-based patient-matching, as proposed in the draft IAS Exchange Purpose Implementation SOP?

We would invite the RCE to read our joint letter from the CARIN Alliance, DirectTrust, eHealth Exchange, Commonwell Health Alliance, and Civitas Networks for Health dated July 20th, 2022 to Acting Office of Civil Rights (OCR) Director Melanie Fontes Rainer about what's needed from

an OCR policy perspective related to IAS-related data breaches for us to meaningfully advance IAS via TEFCA.

We have included a link to the letter and the letter's text below. https://www.carinalliance.com/wp-content/uploads/2022/07/CARIN_Final-Letter-to-OCR-re-Breach-Notification_07202022.pdf

We write to ask for your help in clarifying how the breach notification regulations under the Health Insurance Portability and Accountability Act (HIPAA) will apply when health care providers share protected health information (PHI) with individuals, and use applications for such purposes, including through health information networks and exchanges as defined in the information blocking regulations established by the Office of the National Coordinator for Health IT (ONC). We describe below how certain interpretations of the breach notification rules are causing obstacles to interoperability and the adoption of electronic PHI (ePHI) with individuals, and we request a meeting with you and relevant staff to discuss this issue in more detail, and to consider ways to address it. We want to strongly emphasize that without OCR providing formal guidance or enforcement discretion on this topic, there will be significant adverse consequences to achieving nationwide interoperability and patient access. The CARIN alliance is a multi-sector collaborative working to advance consumer-directed exchange of health information that was convened in early 2016 and now has more than 70 organizations as members. CARIN's vision is to rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals. In this letter, we join with fellow collaborative organizations who we are working with to advance health care interoperability across the country. Today, individuals (or personal representatives acting on their behalf) are increasingly accessing ePHI by connecting a chosen personal health application to their ePHI through open, standard application programming interfaces (APIs) available through certified electronic medical record systems used by their health care providers. In addition, the information blocking regulations and the Trusted Exchange Framework and Common Agreement (TEFCA) are expanding possibilities for individuals to be able to access their electronic health information (EHI) directly from health information exchanges/networks (HIEs). Although participation in TEFCA is voluntary, entities participating in TEFCA will be required to respond to requests for EHI for treatment and for access by individuals (referred to as "individual access services"). These 21st Century Cures Act initiatives should enable individuals to quickly access key health information across multiple providers through a single query, which we believe will be a game-changer for patients. As HIEs and large national HIE networks begin to prepare for individual access, they are raising questions about how to assure, to the extent possible, they are accurately matching individuals to their EHI and to understand their potential liability under the HIPAA regulations for sending an inaccurate match. Recent draft guidance by the recognized coordinating entity (RCE) solidified recommendations made by the CARIN Alliance in 20171 and 20202 , that individual access service providers should ensure that consumer-facing applications follow a reasonable standard that matches the NIST 800-63-3 3 guidelines of IAL2. Our fellow collaborative organizations have already shown how this could work and the CARIN Alliance is currently working with stakeholders from across the industry, including the Department of

Health and Human Services, on how a digital identity federation proof of concept could work in a networked environment.

Today, HIEs predominantly disclose or facilitate disclosure of information for treatment purposes. Most HIE treatment disclosures are done in response to queries, and matching information to the correct patient occurs by attempting to match demographic variables such as full name, address, full date of birth, phone number, and in some cases the last four digits of a social security number, using a variety of deterministic and probabilistic matching algorithms. In conversations with large national HIE networks, we have learned that these networks typically return only one patient's records in response to a treatment query, or if there is insufficient data in the query to yield a unique match, no records will be returned. TEFCA standards similarly mandate that only unique matches be returned. Notwithstanding efforts to assure return of only the correct patient's records in response to a given query, the possibility exists that the wrong patient's records will be sent. In such a case, HIEs and participants in existing large networks rely upon the following exception to the HIPAA breach definition: "Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in future use or disclosure in a manner not permitted [by the Privacy Rule]." 45 C.F.R. 164.402. The exception was an important element in the regulatory framework because it addressed potential liability for Covered Entities and their Business Associates related to circumstances beyond their control for benign disclosures of PHI, and as such, helped lead to the adoption of national exchange networks for treatment purposes. Like the treatment use case, we believe the exception is as important to the future success and adoption of individual access services. It reflects a reality about the difficulty in achieving 100% matching accuracy, despite ongoing efforts by ONC and industry to improve matching accuracy. However, it is not as clear that the HIPAA breach notification rules are as supportive of the responsible exchange of digital health information through HIEs when patients choose apps or services that are not covered by HIPAA. When a non-HIPAA app offering individual access services queries an HIE or national network for individual access using some of the same demographic data fields, the return of records is not subject to a clear exemption from breach liability. As a result, and based on discussions with national networks, we have been told that the networks are seeking to establish an even higher threshold for matching a query to a unique patient in terms of number of demographic data fields and the source of those data fields - a threshold for which is there is no standard definition and that may be difficult to operationalize. The threat of potential penalties in the event of a breach - and having to inform individuals and HHS (on an annual basis) - is an obstacle to facilitating individual access through HIEs and the TEFCA using the same infrastructure used today to support treatment queries. Given the 21st Century Cures Act initiatives supporting expanded data access for patients through their chosen application, we believe further guidance from your office would be welcomed to address this matching issue. In developing this guidance, we think an important consideration that can be borrowed from current practice is that data recipients (providers of individual access service) be held to a similar, common standard of responsible behavior (reviewing and returning or securely destroying non-matching records). While HIPAA does not apply to non-HIPAA participants

offering individual access services, existing HIPAA breach regulations could be interpreted to exclude from breach any inadvertent disclosure of an inaccurately matched patients to providers of individual access services that agree through participation agreements to maintain similar standards of behavior in reviewing and returning/destroying mismatched records before they are populated in the wrong patient's record. To illustrate, we suggest consideration of the following options (and of course are open to exploring others) to help address the matching issue:

1) Extend applicability of the exception set forth in 45 CFR §164.402(1)(iii) to participants involved in the delivery of individual access services: in the instance of a disclosure where the discloser has a good faith belief that the recipient would not reasonably have been able to retain the PHI.

For example, the preamble to the Breach Interim Final Rule provides a case study where an explanation of benefits is mis-addressed and returned by the Post Office to the sender, unopened. In this circumstance, the Post Office was aware that an individual was a member of a health plan, but that was not considered to be a breach because the contents were not accessed. If a provider of individual access services (such as an app vendor) reviews demographic information and returns or securely destroys non-matches without accessing the underlying records or sending them to the wrong patient, we believe there is a similar result.

2) Issuing guidance and/or enforcement discretion for situations where an app vendor reviews or securely destroys non-matches prior to populating them in the wrong patient's record under the "low probability of compromise" analysis, set forth in 45 CFR §164.402(2).

In such a case an exception to the definition of breach provides the highest level of certainty to Covered Entities and Business Associates, but failure to meet an exception does not mean a disclosure of PHI is a breach. Covered Entities and Business Associates must consider whether there is a low probability that the PHI has been compromised, based on the following factors: The nature and extent of the information involved, including the types of identifiers and likelihood of reidentification; The unauthorized person who used the information or to whom the disclosure was made; Whether the PHI was actually acquired or viewed; and The extent to which the risk to the information has been mitigated. In circumstance where a potential match is sent in good faith by a Covered Entity or Business Associate (whether directly or via an HIE or national network), but the recipient app vendor evaluates the demographic data from those matches and determines that the information was sent on the wrong patient and securely returns or destroys the incorrect record, it is conceivable that under current regulations, a Covered Entity or Business Associate could conclude there was a low probability that sensitive medical record information was compromised. However, entities will likely fear penalties for being wrong in this assessment. But if OCR were to signal that implementation of such policies for dealing with incorrect matches would or should meet the low probability of compromise, that might remove this potential obstacle to nationwide interoperability for individual access services through HIEs and the TEFCA. TEFCA policies and agreements (such as through flow

down provisions) could reinforce or require such practices on the part of app vendor recipients. We appreciate your consideration of these issues and look forward to further discussing them in more detail with you.

1.a. What approaches could the federal government consider to help organizations address these challenges?

Please reference the letter our 5 organizations sent to OCR here. (https://www.carinalliance.com/wp-content/uploads/2022/07/DRAFT-IAS-Provider-Privacy-and-Security-SOP-Final-Comments.pdf)>

2. What are some considerations for solving the challenges presented by demographics-based patient matching at a national network scale?

The use of CSPs who are IAL2 certified as being the 'source of truth' for individual's demographic data will help.

2.a. Please identify educational or collaboration resources, as well as potential policy and technical approaches, that can be implemented across organizations to help identify a common baseline for how to improve confidence in patient matching and increase the response rate to IAS Requests.

We believe the CARIN Alliance Digital Identity Federation PoC with the Department of HHS, ONC, and CMS along with multiple private sector partners will significantly advance the industry's understanding of how an IAL2 certified digital credential can be used across a networked environment. We are actively engaged in the PoC right now as the developers are building the technology infrastructure to support a federated CSP environment. You can read more about our work here: https://www.carinalliance.com/wp-content/uploads/2022/03/Proof-of-Concept_Outline_01252022.pdf. We would also welcome the opportunity to further discuss it with you in person.

3. How do organizations determine they have achieved an acceptable match for IAS? How much variation exists across the market in policies for determining an acceptable match?

IAS providers should be required to partner with a credentialing service provider (CSP) who verifies a user's identity to at least an IAL2 level or higher. Demographics verified by the CSP will be passed within the query. Responders with a 100% match (based on their own definition) will be required to respond where applicable law allows. Based on past conclusions, any change to a verifiable demographic would require a patient to go through identity proofing again. Once the patient has been verified, they may continue to assert that credential as long as it remains valid through their CSP.

3.a. Would the use of IAL2 verified identifiers increase match confidence? If so, how?

Absolutely. Our membership includes all of the national CSPs and representatives of the major national data exchange networks. It has been their experience as part of pilot programs they have run that IAL2 verified identifiers significantly increase match confidence. The CSPs have also had experience in seeing increased match rates with validated attributes.

3.b. What additional steps might be taken at a TEFCA-wide level to improve match confidence?

We believe the use of the USPS Address Verification API would help with matching but it would not help with ID proofing since the CSPs currently use government issued ID-based demographic information. Implementing an IAL2 certified digital identity credential across all systems will also help.

4. In the FHIR roadmap, QHINs, Participants, and Sub-Participants will be required to respond to an IAS Request based on responder-issued credentials presented through an OAuth flow. How could TEFCA use responder-issued credentials as a means of definitively authenticating IAS Requests in a non-FHIR environment?

Contractual commitments binding an IAS provider to ID proof in accordance with the required NIST 800-63-3 standards is consistent with how HIE exchange occurs in other B2B contexts. We believe requiring those contractual commitments of participants will follow a similar successful model that has been in place for more than a decade. It's also important that the data transmitted by the CSP shall not be classified as a QHIN or Resource Holder data.

4.a. What are the challenges?

Ensuring that TEFCA allows for a marketplace of solutions and approaches that will provide multiple different IAS providers the ability to access individual health care data for the myriad of different consumer-centric use cases that are emerging.

4.b. Given that TEFCA will support FHIR and non-FHIR exchange, how important is it to have an authentication process using responder-issued credentials in non-FHIR transactions brokered through QHINs?

OAuth does not work on a SOAP based transaction. We support validated attributes being sent via an IHE demographic query. We believe that validated attributes (that have been ID-proofed) via a demographic query will be the main way IAS will be provided for the next few years. There is no need to have an authentication process for a non-FHIR based query.