April 29, 2026

RE: TEFCA Individual Access Services (IAS) Exchange Purpose Changes Under Consideration 2026
Submitted electronically to rce@sequoiaproject.org

To whom it may concern,

On behalf of the CARIN Alliance, we appreciate the opportunity to provide comments to the Recognized Coordinating Entity (RCE) on the proposed version 3.0 updates to the Standard Operating Procedures related to Individual Access Services among TEFCA networks and participants (the "V.3 SOP Proposal").

As you are aware, the CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers and caregivers. We are committed to providing consumers and their authorized caregivers access to health information. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain access to their health information, including their electronic health information, through modern technology protocols, the use of digital identity, and the advancement of open-source industry standards.

We appreciate the ongoing work that the RCE and ONC have undertaken to advance access by individuals to their health information through TEFCA, as a floor for network-based exchange in ways that also advance the ONC's deregulatory agenda. We remain committed to supporting the RCE and ONC as they lift the entire ecosystem. We also support CMS in work to accelerate first-movers. The CARIN Alliance remains committed to collaborating with you in advancing consumer choice, consumer privacy, and consumer access.

Again, we appreciate your consideration of our comments. Please do not hesitate to contact me if you have any further questions.

RR Ryan Howells

Ryan Howells
Leavitt Partners
On behalf of the CARIN Alliance

Identity Dynamics

The 21st Century Cures Act, the ONC Cures Act Final Rule, and the CMS Interoperability and Patient Access rule have accelerated the ability for an individual to access their personal health information via an application of their choice by leveraging HL7® FHIR® Application Programming Interfaces or APIs. Currently, the use of SMART on FHIR® allows for an individual to use their provider or payer portal username and password to authenticate themselves and retrieve their personal health information. While the CARIN Alliance strongly endorses the current implementation of SMART on FHIR® by stakeholders in the health care ecosystem to ensure individuals have immediate access to their health information, we also want to advance a future vision for how we could, as an industry, digitally authenticate individuals in a trusted way without being tied to the creation of portal accounts, and then allow an individual to use that same trusted authentication event to access their health information across multiple payers and providers.

While we appreciate that ONC and the RCE share this vision, the v.3 SOP Proposal does not go far enough to advance it, and, in many respects, takes a step backward from the progress made to this point. Our shared objective is, and should remain, the advancement of standards that reduce friction for patients and expand the range of responses they can expect. Coupled with technology vendors' reticence to accept a third-party credential, IAS on TEFCA is faced with a number of challenges to remove unreasonable barriers that prevent or delay patients' ability to access their health data, consistent with HIPAA. Our hope has been that network rules, such as the network pledge requirements from the CMS Health Technology System and the Standard Operating Procedures within TEFCA, would evolve in the same direction towards elimination of credential-based logins, while quickly iterating on consistent patient match and response standards. In the end, the ONC's deregulatory agenda depends on avoiding the need for stakeholders to implement and maintain incompatible standards, while fulfilling the RCE's broader mandate to enable individuals to successfully exercise their right of access through secure, IAL2-compliant, third-party credentials in place of credential-based logins.

For these reasons, we are concerned that the v.3 Proposed SOP does not consider some of the matching suggestions in the CMS Patient Matching and Response Proposal, which has been in development over the same period through an open, consensus-driven, industry-led process undertaken by the CMS HTE's workgroup for Identity Verification and Authentication. Participants of this workgroup include CMS, QHINs, EHRs and Covered Entities, and other pledging organizations that also participate in TEFCA.

Among other things, the CMS Patient Matching and Response Proposal addresses the predicates for successful patient matching (data handling and cleaning), which is not addressed anywhere in the v.3 Proposed SOP. It also defines an empirical testing method to determine the probability that a given combination of identity attributes will yield records on more than one patient (*i.e.*, matching rules based on probability of collision aka *p(collision)*). In contrast, the v.3 Proposed SOP doesn't set a match rate expectation, except for a single combination of three primary and choice of four different secondary attributes, which doesn't require implementation until **August 1, 2027**. This approach will not yield a consistent standard, and does not satisfactorily address known (and oftentimes underlying) issues with patient matching rates. Moreover, allowing responding nodes to use local policies over a standard for patient match and respond prevents the TEFCA community from quickly gathering empirical information with scientific rigor to inform future policies.

The CMS Patient Match and Response Proposal also establishes a conservative *p(collision)* threshold of 0.0000000002%. Combinations that match this threshold are listed in that proposal. We believe a comparable matching response threshold should be established by the RCE, to balance the flexibilities of local policies with compelled response, which should override the perceived concerns that justify ongoing use of portal credential logins. To illustrate, one QHIN with records on 340 million patients is testing the CMS Patient Matching and Response Proposal, and the preliminary results (using synthetic data) are encouraging: using the approved combinations are projected to return records on two distinct patients less than 12,000 times (out of 340 million possible records), which we feel is an acceptable risk, and a better posture than the known risks that arise from impersonation and compromise in portal credential logins.

Finally, the CMS Patient Matching and Response Proposal addresses standards for testing and validation of results that can be handled by EHR vendors and/or QHINs before responding to specific queries. That way, there is an administrative step to request additional demographics, rather than an outright failure to respond. Again, this step is being implemented in time for the CMS HTE Launch on July 4, 2027. By contrast, the v.3 Proposed SOP applies this obligation on IASPs through the Demographic Double Check proposal, with an immediate applicability date of August 1, 2026, but no such step is compelled by Responding Nodes or their QHINs.

In short, the CMS Patient Matching and Response Proposal offers a comprehensive, empirically based step to solving patient matching, not just for IAS but for all network-based exchange. QHINs and EHRs are actively working to implement its recommendations in time for the CMS HTE deadline on July 4, 2026. By contrast, the v.3 Proposed SOP is offering a step backward in consumer-mediated health data access, by making portal credential login the new default standard, applicable August 1, 2026, over the current default flow for XCPD and XCA transactions. Unfortunately, the v.3 Proposed SOP has avoided the promised opportunity to quickly test and iterate on an MVP matching standard, which was one of the goals of last fall's IAS Participant WG.

For these reasons, we propose that the RCE rescind the v.3 Proposed SOP, and work instead to develop an SOP that is compatible with the CMS Patient Matching and Response Proposal.

In addition, any new proposal should align with the following foundational principles:

1. A deadline for implementing the 3+4 matching logic in the TEFCA IAS SOP that is compatible with the CMS HTE Launch deadline. 2027 is too distant and is emblematic of perfection as the enemy of the good. While we believe the 3+4 logic is overly restrictive and will lead to unnecessary false negatives where patients will not get their data, we agree it is time to move forward and adjust the technical trust boundary over time to make data sharing to individuals both safe and universally scaled.
2. Commitment to resolve the efforts of CMS Aligned and TEFCA to incorporate best of breed solutions for patient matching including objective measurement criteria, testing and reporting as we progress and add methods, and processes to better enable patient matching.
3. An end to portal and credential-based logins by allowing for a user to create their own identity-proofed digital credential in an application of their choice and use that credential via OpenID Connect (OIDC) to authenticate into any health care portal in the country as a safe harbor for compliance.
4. An end to allowing local policies to dictate patient matching algorithms and response requirements, unless they are subject to the same *p(collision)* threshold agreed on by

participants in the CMS ID Verification and Authentication WG.

5. An end to requirements that CSPs must collect and share SSNs with IASPs, due to consumer privacy concerns and hesitancy about the overuse and sharing of these highly sensitive identifiers. However, giving CSPs the option of sharing the last 4 SSN digits should be allowed, to conform with standards agreed upon in the CMS HTE's Identity Verification and Authentication WG.
6. Eliminate the approach for consent-based exchange, because the "consent" concept is fundamentally incompatible with the right of individuals under HIPAA to exercise their right of access through their choice of IASP. The principles of data use limitation and data sharing limitations properly reside implemented downstream from network-based exchange—between the IASP and the individual, consistent with applicable federal and state health care and privacy laws.
7. The demographic double check, if it is to be included in a future SOP, should not solely be a standard requirement of IASPs. QHINs also should play a role in intercepting wrong records, and in some cases may be better positioned to do so. For IASPs that lack the resources or functional capacity to perform this process, IASPs should be able to delegate this role to their QHIN. Most QHINs are governed by their contract and in some cases legal obligations to perform a demographic double check—for example, QHINs that act as business associates to their HIPAA-covered participants and subparticipants. In the same way, non-HIPAA IASPs should be able to contract with their QHIN for performance of the demographic double check, and QHINs are already equipped to notify other QHINs when errors are detected. Independent of that, if a QHIN inadvertently transmits a wrong record to its Requesting IASP participant, it has legal obligations as the IASP's service provider to notify them. When an IASP does receive a wrong record through its QHIN, the IASP should be required to contribute information back to its QHIN to enable performance by the relevant QHIN (or data source) of the low probability of compromise analysis under the HIPAA Breach Notification Rule.

In sum, CARIN believes:

1. For IAS to work appropriately across the TEFCA community and the CMS HTE, rules need to be aligned and data holders need to be held accountable if they do not respond appropriately to patient-access requests.
2. The CMS approach to patient matching and data-holder response should be standardized and mandated in TEFCA instead of perpetuating old modalities and divergent approaches.
3. Current proposals for ongoing portal-based authorization within TEFCA are not consistent with other government initiatives and should, at least, have a near-term sunset date.
4. Timelines for implementation of new SOPs for IAS responses under Option 2 are incompatible with the ONC's deregulatory agenda and mission to advance consumer-mediated retrieval as a Mandatory purpose of exchange.

Data Retention Policies

In addition to modifications to proposals within the updated SOP, we are concerned about the apparent lack of consideration for specific data retention practices. CARIN believes that responding nodes should be precluded from retaining the demographic or identity information of individuals for whom no matches are found. The reason is that this personal information is retained without individual consent and introduces a hazard that responding nodes will use this information in top-of-funnel marketing campaigns or other ways that compete with Requesting Nodes. These practices are

contrary to fair information practice principles upon which the CARIN Code of Conduct is based and create an incentive for unfair business practices.

In addition, when personal information is stored on multiple nodes (including nodes that are not required to be HITRUST certified), its vulnerability to cyberattacks increases. For queries for which no match is found, responding nodes should be required to either immediately delete the PII used in the query, or avoid retaining the information in the first place, by requiring all QHINs to perform record location services on behalf of their participants.

Failing to address these concerns undermines the ultimate viability of TEFCA as a universal standard for trusted nationwide network-based exchange.

Similarly, CARIN believes that QHINs should be precluded from retaining the demographic or identity information of individuals for whom no matches are found, except for the narrow purpose of improving their own patient match practices, in furtherance of their QHIN duties. QHINs that keep patient matching "in-house" instead of "fanning out" patient match requests to their participants and subparticipants are inherently more privacy and security protective, due to their HITRUST certification status. These QHINs should be held to a strictly necessary standard to use this demographic or identity information for the sole purpose of delivering better match rates and latency rates over time. These are important objectives that not only serve individuals but the broader TEFCA mandate. By contrast, the QHINs that "fan out" patient record location queries create digital pathways that invite the moral hazards described above. This is a data leakage problem that goes beyond this SOP, and should be prioritized by the RCE.

As noted, we are committed to collaborating with you in advancing consumer choice, consumer privacy, and consumer access. If you have any questions about items within this comment letter, please contact David Lee (david.lee@leavittpartners.com) who leads our Policy Workgroup.