American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

April 24, 2026

Mariann Yeager
RCE Program Lead
Sequoia Project
TEFCA Recognized Coordinating Entity
8300 Boone Blvd.
Suite 500
Vienna, VA 22182

Submitted Electronically

RE: Trusted Exchange Framework and Common Agreement Individual Access Services Exchange Purpose Standard Operating Procedures 3.0

Dear Ms. Yeager,

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to provide comment on the Trusted Exchange Framework and Common Agreement (TEFCA) Individual Access Services (IAS) Exchange Purpose (XP) Standard Operating Procedures (SOP) version 3.0. [1]

Our members recognize the important role that data interoperability — that is, the ability to securely access, exchange and integrate data across multiple information systems and entities — plays in advancing the broader goals of the health care ecosystem. Many of our members participate in TEFCA and other interoperability networks to support better continuity of care, improve patient safety and ultimately deliver better patient outcomes. Voluntary participation in interoperability networks continues to grow rapidly. Almost 500 million records have been exchanged in TEFCA across 71,000 participants since December 2023, with approximately 490 million records exchanged in

[1] Standard Operating Procedure (SOP): Individual Access Services (IAS) Exchange Purpose Implementation

2025.[2] Our members recognize that IAS, in particular, can support patients to make more informed decisions, promote increased engagement and foster patient choice.

At the same time, the protection of patient data is foundational to patient trust in the health care system and, as such, the government has codified, through statute and regulation, actions certain entities must take to ensure such protection. Thus, any efforts to foster data exchange must be balanced with the existing statutory obligations to protect patient data. Indeed, as covered entities, hospitals and health systems are legally bound to take verification and other protective steps as mandated by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) and subsequent regulations. These statutes and rules were established to prevent unauthorized use, access or disclosure of personal health information (PHI) while also supporting patients in accessing their own medical data.

While we support efforts to advance interoperability, the AHA believes that the proposals included in the IAS XP SOP do not contend with the statutory and regulatory obligations of hospitals and health systems to protect patient data, creating serious compliance and liability risks associated with disclosure of PHI. **We therefore recommend that the SOP implementation be delayed until these concerns can be addressed through statutory or regulatory means.** For example, we support developing a safe harbor for providers who utilize this SOP for an IAS request or, alternatively, developing regulations that would reconcile these proposed processes with HIPAA privacy, security and breach notification rules.

Additional details are below.

BACKGROUND

Interoperability networks have been developed as flexible frameworks to enable adjustment for technology changes. These networks are generally predicated on private-public partnerships, with oversight functions performed by a variety of agencies and private sector partners with different roles. At the agency level, the Office for Civil Rights (OCR) provides enforcement for HIPAA privacy, security and breach notification rules, while the Office of the National Coordinator (ONC) provides overarching policy for TEFCA and establishes data standards to support. The Sequoia Project functions as the recognized coordinating entity (RCE), providing oversight for Qualified Health Information Networks through the common agreement, terms of participation and SOPs.

SOPs provide guidelines for specific exchange purpose use cases, or the reasons that entities request to send or receive data. The current exchange purpose use cases under TEFCA include public health, payment, government benefits determination,

---

[2] TEFCA™, America's National Interoperability Network, Reaches Nearly 500 Million Health Records Exchanged as HHS Leverages Technology and AI to Lower Costs and Reduce Burden | HHS.gov

health care operations and IAS. IAS supports patients in accessing their own medical records by creating workflows to direct the data to third-party apps. IAS workflows entail identity verification (checking that the patient is who they claim to be), patient matching (linking patient records across different systems using demographic data) and patient consent (patient directs the disclosure of their own health data to parties of their determination).

PROPOSED RESPONSE NODE REQUIREMENTS

The proposed IAS XP SOP version 3.0 outlines three proposed approaches for responding nodes to respond to IAS requests.[3] The proposals touch on all three aspects of the IAS workflow.

- Response Approach 1: Would require responding nodes to respond to IAS requests using a Fast Healthcare Interoperability Resources (or FHIR) credential-based log-in flow using certain demographic fields for patient matching.
- Response Approach 2a: Would require responding nodes to respond to IAS requests using a new "TEFCA IAS Consent" (TIC) flow, which would prevent responding node verification, and a revised proposed patient matching process that has not been validated. The TEFCA RCE would require responding nodes to implement this by Aug.1, 2027.
- Response Approach 2b: Would require responding nodes to respond to IAS requests using the same approach as approach 2a, but with fewer patient matching data fields or without the TIC. The TEFCA RCE would require responding nodes to implement this by Aug. 1, 2027.

The AHA appreciates that these approaches intend to support patient choice and reduce patient burden. However, we are concerned that the proposed SOPs rely on untested consent and patient matching components, presenting significant compliance risks for responding nodes that are covered entities. The proposed implementation date also does not provide adequate time to build functionality, test reliability and integrate workflows, much less address some of the legal and regulatory compliance risks. **As outlined further below, we recommend a delay of the proposed SOP until statutory and regulatory compliance concerns are addressed.**

Proposed TIC Process Has Not Been Developed and Inappropriately Bypasses Response Node Verification Processes. Approaches 2a and 2b reference a new proposed TIC process, whereby the third-party app would validate and verify that the individual has consented to use the IAS. TIC workflows do not currently exist and have not been tested. Most significantly, the proposed process has not been reconciled with

[3] 5 C.F.R. § 172.102 defines responding node as "A Node through which the QHIN, Participant, or Subparticipant Responds to a received transaction for TEFCA Exchange."

the legal and regulatory obligations for responding nodes that are covered entities to verify requests for access and use of data.

As covered entities, providers are governed by HIPAA privacy, security and breach notification rules. The HIPAA privacy rule specifies that covered entities must have "appropriate administrative, technical and physical safeguards to protect the privacy of protected health information" and also outlines verification requirements for covered entities to confirm the identity and authority of entities requesting PHI.[4,5] The TIC proposals and approaches risk preventing providers from properly verifying the identity and authority of third-party entities requesting data, potentially impeding covered entities from fulfilling their legal obligations to validate the request before disclosing data. The TIC proposals similarly do not address the state and local privacy and consent requirements, which may expose providers to additional compliance risk.

Failure to comply with these rules not only generates substantial financial and reputational risk and legal liability for hospitals and health systems, but it can harm patient care by delaying delivery of care, impacting access to critical information for treating providers, and ultimately eroding patient trust in providers and the security of their most sensitive data. Should the Sequoia Project move forward with proposals without addressing these risks, we are concerned that providers will be disincentivized from participating in TEFCA, given these significant legal, compliance and patient care concerns.

Proposed Patient Matching Methodology Has Not Been Validated. Patient matching processes are foundational for patient safety, ensuring that the right patient receives the right care. Patient misidentification increases the risk for adverse events. Misidentification also raises privacy concerns, where data may be sent to the wrong patient, resulting in unauthorized disclosures. In other instances, it can result in billing delays, duplicative testing and claims denials.

To adequately protect patient safety and privacy, patient matching methodologies must work reliably. However, the proposed IAS SOP workflow and patient matching methodologies entail potential end-user manual entry of demographic data fields. The experience of health care providers has shown that such approaches are more prone to data entry errors or data theft. For these reasons, we urge rigorous testing to ensure that the revised patient matching methodologies work consistently as intended.

SUMMARY OF RECOMMENDATIONS

We urge the Sequoia Project to delay implementation of these proposals and encourage them to coordinate with ONC and OCR to pursue statutory and regulatory relief for providers because many of these questions exceed the capacity for sub-

[4] 45 C.F.R. § 164.530(c)
[5] 45 C.F.R. § 164.514(h)(1)

regulatory guidance, such as the SOPs, to address. For example, the creation of a statutory safe harbor protecting providers from liability for disclosures fulfilled via these IAS processes could mitigate risks for providers in the event of a breach. When a third party misrepresents consent for disclosure, providers should not be held liable or obligated to undertake breach notification steps if they were complying with the IAS process. Alternatively, OCR could issue regulations clarifying that providers who comply with this IAS process have fulfilled their legal obligations to verify patient consent, as well as the identity and authority of the entity requesting health information, prior to disclosing records.

The current asymmetry in privacy and security requirements, whereby third parties requesting data are not covered entities or business associates, forces providers and covered entities to bear the full risk for activities outside their control. Entities without the same level of downside risk — such as the third parties making or facilitating these data requests — are not similarly incentivized to undertake the same levels of data protection and verification. We have consistently urged that third parties be held to the same privacy and security requirements as covered entities and business associates.[6,7] We would encourage the Seqouia Project to work with ONC and OCR to issue agency-level requests for information, proposed rules and clarifying guidance. Such regulations should address topics such as providers' duty to verify third parties, responsibilities for breach notification and liability in the event of third-party breaches resulting from IAS workflows.

We look forward to working with the Sequoia Project, OCR and ONC to address these concerns. Our members and we are committed to finding solutions that can promote interoperability and patient choice while protecting patient data, and believe that the delay of the proposed IAS XP SOP provides additional time for stakeholder input to support the long-term viability of TEFCA.

Please contact me if you have questions, or feel free to have a member of your team contact Jennifer Holloman, AHA director of health IT policy, at jholloman@aha.org.

Sincerely,

/s/

Ashley Thompson
Senior Vice President
Public Policy Analysis and Development

---

[6] https://www.aha.org/lettercomment/2026-02-23-aha-response-hhs-rfi-ai-health-care
[7] https://www.aha.org/testimony/2025-07-09-aha-statement-senate-help-committee-cybersecurity