TEFCA Individual Access Services (IAS) Exchange Purpose

Changes Under Consideration – February 2026

Vision and Context[1]

From the start, the Trusted Exchange Framework and Common Agreement™ (TEFCA™) Individual Access Services (IAS) Exchange Purpose (XP) has focused on giving Individuals the power to use network scale to find their health information *and* get a copy. While the IAS XP is designated as "required response," responsiveness, especially for demographics-based query, has been suboptimal due to technical variation and policy ambiguities.

The Assistant Secretary for Technology Policy/Office of the National Coordinator for Health IT (ASTP/ONC) and the Recognized Coordinating Entity® (RCE®) are working with the Qualified Health Information Network® (QHIN™) Caucus and the Participant and Subparticipant Caucus to create an approach that will address these issues and lead to a more reliable flow of data in response to IAS Queries. This work benefits from discussion by the IAS Workstream, which included both Caucus members and outside expert volunteers.

Summary of Changes Under Consideration

Topic	Summary Description of Change(s)
Credential Service Providers (CSP) Verified Demographics	Require CSPs that seek to support TEFCA IAS to increase the amount of demographics data that they must have the capability to IAL2 verify.
Valid IAS Query Requirements	Increase the required IAL2 data elements that must be included within an IAS query for it to be considered valid. An IAL2 verified phone number, or email address would need to be included in a valid IAS query.
Self-Asserted Demographics	Allow Individuals to self-assert demographics and for IAS Providers to include self-asserted demographics (e.g., nickname, maiden name, past address) in queries along with IAL2 verified data so that responders can use them to further sharpen patient matching.
Risk Mitigation	Include risk mitigations to support a Covered Entity's HIPAA Breach Notification Rule analysis of "low probability of compromise."
Matching Response Logic	Establish required response logic largely based on IAL2 verified data that would require a response to a demographics-based query when met.
Response Requirements	Clarify that two different response responsibilities exist in parallel: 1 - Responders must respond when a demographics-based match is achieved; and 2 - FHIR endpoints are also returned when available.
Technical Conformance Issues	Incorporate implementation guidance and feedback received from QHINs, IAS Providers, and network participants.

[1] This document summarizes, at a high level, changes that are currently under consideration to inform the community and provide transparency about ongoing discussions. Pending further work by the Caucuses, ASTP and the RCE will release proposed changes to the relevant SOPs following our Change Management Process. See the existing XP Implementation SOP: Individual Access Services v2.1 for current policy.

TEFCA Individual Access Services (IAS) Exchange Purpose

Changes Under Consideration – February 2026

Changes Under Consideration – Additional Details

Credential Service Provider (CSP) Responsibilities

- Increase the minimum set of data elements a CSP is required to have the capability to IAL2 verify by adding the following:
  - Middle Name/Middle Initial, Suffix, Email, Mobile Phone Number, State ID/Driver's License, and SSN (or last four digits).
- Encourage CSPs to be able to validate all other demographics that can be provided
  - For example, Verified Historical Address.

IAS Provider Responsibilities

- Queries initiated by an IAS Provider must include any self-asserted demographic information not verified by the CSP that the IAS Provider may have collected from the Individual for the purposes of matching demographics.
- When performing an IAS query, the IAS Provider must include all available IAL2 verified demographics in the query, not just the minimum set, and this MUST match the verified data provided by the CSP as part of the IAL2 Claims Token.

IAS Provider Breach Mitigation Responsibilities

- Add "Demographics Double Check"
  - An IAS Provider must perform a patient demographics match using its own algorithm with both IAL2 verified and self-asserted data held in the IAS Provider's system against the demographics returned in the message metadata from the Responding Node.
  - Checkpoint created for IAS Providers to prevent querying for clinical information when a potential false positive match has occurred and assisting Covered Entities in applying the four "low probability of compromise" factors of the HIPAA Breach Notification Rule.
- Add requirement for IAS Provider to be able to purge erroneous data following receipt of a mismatch notification from an Individual.

Demographics Double Check:

If the Demographics Double-Check does not determine a match, the IAS Provider:

- MUST reject the demographics response from the responding node, and
- MUST NOT retain the patient identifier from the Individual's request, and
- MUST NOT continue to initiate a Query from that Responding Node, and
- MAY provide the Individual with a patient portal credentials-based OAuth login for that Responding Node, if a FHIR endpoint was also provided by the Responding node, and
- MUST notify the QHIN/P/S that operates or is associated with the Responding Node that returned the mismatched demographics that IAS Provider believes a potential false positive match occurred.

TEFCA Individual Access Services (IAS) Exchange Purpose

Changes Under Consideration – February 2026

IAS and Patient Matching Response Logic

Updated Patient Matching Response Logic

While Responding Nodes still determine how to make a match on a data element by data element basis using their own computational approaches, TEFCA IAS would introduce more explicit required response logic rules:

- **Seven or Greater IAL2 Response Rule** – IF at least seven IAL2 verified demographics are matched, THEN a Response is required.
- **First Name Variation Response Rule** – IF (i) only six verified demographics are matched except for first name AND (ii) the first name variation is matched through self-asserted data (i.e., self-asserted nickname sent matches first name in Responding Node), THEN a response is required,
- **Address Variation Response Rule** – IF (i) only six verified demographics are matched except for street address AND (ii) the street address variation is matched through self-asserted data (i.e., self-asserted street address sent matches street address in Responding Node), THEN a response is required,
- **Verified and Self-Asserted Demographics Combination Response Rule** – IF only six verified demographics are matched AND at least two self-asserted data are matched, THEN a Response is required (e.g., insurance # and last four of SSN),
- If the Responding Node's matching threshold rules are less restrictive, they may continue to respond using their less restrictive thresholds.

Next Steps

We are requesting feedback from the Caucuses on the updates under consideration, and specifically on the following:

- Requirements for CSP-Verified and Self-Asserted Demographics,
- The Demographics Double Check, and
- The Patient Matching Response Logic

Feedback due February 20

Initial feedback from caucus members is due to: rce@sequoiaproject.org

Join ASTP leadership and the RCE to discuss these changes on our next monthly informational call.