TEFCA RECOGNIZED COORDINATING ENTITY

Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS)

Version 3.0

Effective Date:

Applicability:

4.1 - 4.6: IAS Providers

4.7, 4.8: QHINs, Participants, Subparticipants

1 Common Agreement References

The requirements set forth in this Standard Operating Procedure (SOP) are for implementation, in addition to the terms and conditions found in the Framework Agreements, the Qualified Health Information Network® (QHIN™) Technical Framework (QTF), and applicable SOPs. The Trusted Exchange Framework and Common Agreement™ (TEFCA™) Cross Reference Resource identifies which SOPs provide additional detail on specific references from the Common Agreement.

All documents cited in this SOP can be found on the Recognized Coordinating Entity® (RCE®) website.

2 SOP Definitions

Select terms used throughout this SOP are defined in this Section for ease of reference. All capitalized terms used in this SOP have the respective meanings assigned to such term in the TEFCA Glossary.

Individual Access Services (IAS): the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant, or Subparticipant, as applicable, agrees to satisfy that Individual's ability to use TEFCA Exchange to access, inspect, obtain, or transmit a copy of that Individual's Required Information.

Individual Access Services Provider (IAS Provider): each QHIN, Participant, and Subparticipant that offers Individual Access Services (IAS).

3 Purpose

This SOP identifies specific requirements that IAS Providers are required to follow for Individual identity verification when sending an IAS Query. This SOP also identifies when a QHIN, Participant, or Subparticipant is required to Respond to an IAS Query.[1] This SOP includes context-specific privacy and security transaction requirements for IAS Providers. General privacy and security requirements for IAS Providers are included in the IAS Provider Requirements SOP, along with the Common Agreement.

[1] Nothing in this SOP alters a Covered Entity's obligations under applicable law.

4 INDIVIDUAL ACCESS SERVICES (T-IAS)

4.1. Exchange Purpose Code (XP Code)

a) All TEFCA Exchange under IAS MUST use the XP Code T-IAS.

4.2. QHIN Technical Framework (QTF)

a) All TEFCA Exchange under IAS MUST follow technical requirements as specified in the QTF and the Facilitated FHIR Implementation SOP.

4.3. Compliance Dates

SOP Section Number	Compliance Requirement	Applicability	Compliance Date
4.6	Demographics Double Check	IAS Providers	August 1, 2026
4.8	Responding Nodes that are not Responding in accordance with Approach 1 MUST Respond in accordance with Approach 2.	Q/P/S	August 1, 2026
4.8	Responding Nodes MUST Respond in accordance with Approach 2. Responding Nodes with a FHIR Endpoint MUST also continue to Respond in accordance with Approach 1.	Q/P/S	August 1, 2027

4.4. IAS Provider Use of Approved Credential Service Providers (CSPs)

IAS Providers are only permitted to use CSPs that have been approved by an RCE-selected CSP approval organization. IAS Providers must ensure the CSP(s) it partners with do the following:

a) Conduct identity proofing to at least Identity Assurance Level 2 (NIST IAL2) as defined by the then latest version of NIST SP800-63A.

b) Be able to verify the following demographic information[2]:

1) First Name
2) Middle Name/Middle Initial
3) Last Name
4) Suffix
5) Date of Birth
6) Street Address
7) City
8) State
9) Zip Code
10) Email
11) Mobile Phone #
12) State ID/Drivers License #
13) SSN or SSN Last Four

c) After verifying an Individual's identity, deliver to the IAS Provider a signed (with the CSP's private key) IAL2 Claims Token in the OpenID Connect format (as detailed in Appendix 1) with all of the Individual's demographics that were verified by the CSP.[3]

d) Provide a publicly accessible endpoint (without authentication) to share a JSON Web Key Set (JWKS), which Initiating Nodes and Responding Nodes are able to use to validate an identity token issued by that CSP. The private key used to create the signed token has a corresponding public key found in the JWKS document mentioned above, whose URL is found in the jwks_uri metadata value provided by the CSP.[4]

e) Supply configuration information per *OpenID Connect Discovery 1.0 incorporating errata set 2:Obtaining OpenID Provider Configuration Information*. Configuration values are known as OpenID Provider Metadata. From the OpenID specification: OpenID Providers supporting Discovery MUST make a JSON document available at the path formed by concatenating the string /.well-known/openid-configuration to the Issuer.

4.5. IAS Provider Responsibilities

a) IAS Providers MUST have an agreement with a CSP that has been approved by an RCE-selected CSP approval organization.[5]

[2] IAS Providers are encouraged to look for CSPs that can verify historical addresses, additional email addresses, additional mobile phone numbers, and provide a CSP Issued Identifier (if issued as a customer digital identifier).
[3] In the OpenID Connect Protocol, the CSP implements the requirements of the OpenID Provider.
[4] CSP are encouraged to rotate encryption keys as described in OpenID Connect Core. See Final: OpenID Connect Core 1.0 incorporating errata set 2 for details.
[5] The RCE-selected CSP approval organizations are published and maintained on the RCE website.

b) IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2[6] (AAL2) requirements.

c) IAS Providers MUST ensure the identities of Individuals that elect to use their IAS offering are verified to at least NIST IAL2 via a CSP when any of the following occurs:

    i. Prior to the Individual's first use of TEFCA Exchange,

    ii. When verified demographics change, or

    iii. After credentials expire.

d) An IAS Provider MUST include the following IAL2-verified demographics in an IAS Query for the query to be valid and usable for TEFCA Exchange:

    i. First Name
    ii. Last Name
    iii. Date of Birth
    iv. Street Address
    v. City
    vi. State
    vii. Zip Code, and
    viii. *Either* email address *or* mobile phone

e) IAS Providers MUST include all the IAL2-verified demographics provided by its CSP in the IAS Query even when more than the minimum needed for a valid IAS Query have been verified.

f) IAS Queries initiated by an IAS Provider MUST contain the IAL2 Claims Token.

g) IAS Queries initiated by an IAS Provider MUST also include all 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.

4.6. IAS Provider Breach Mitigation Responsibilities

The following applies to an IAS Provider in the context of assisting HIPAA Covered Entities apply the four "low probability of compromise" factors established in paragraph (2) of the "breach" definition adopted at 45 CFR 164.402 of the HIPAA Breach Notification Rule. All other Applicable Laws continue to apply. IAS Provider breach reporting and notification responsibilities are set forth in the IAS Provider Requirements SOP.

[6] See https://pages.nist.gov/800-63-3-Implementation-Resources/63B/AAL/ for full information on the levels.

a) When an IAS Provider receives a successful patient discovery response from a Responding Node, the IAS Provider **MUST** perform a patient demographics match comparison using its own algorithm with both IAL2 verified and self-asserted data in the IAS Provider's system against the demographics returned in the patient discovery response from the Responding Node ("Demographics Double-Check").

   i. If the Demographics Double-Check does not determine a match between the IAL2 verified and self-asserted data in the IAS Provider's system and the demographics data returned by a Responding Node, the IAS Provider:

      1) **MUST** reject the demographics response from the Responding Node, and

      2) **MUST NOT** retain the patient identifier from the Individual's request, and

      3) **MUST NOT** continue to initiate an IAS Query to that Responding Node and,

      4) **MAY** provide the Individual with the Responding Node's credential-based approach using FHIR OAuth for that Responding Node, if provided by the Responding Node, as defined in the Facilitated FHIR Implementation SOP.

   ii. When a Demographics Double-Check does not determine a match, the IAS Provider **MUST** notify the QHIN, Participant, or Subparticipant that operates or is associated with the Responding Node that returned the demographics. This can be done directly, or via the QHIN of the Responding Node.

b) If after viewing the TEFCA Information returned via an IAS Query by an IAS Provider, an Individual notifies the IAS Provider that they believe another Individual's data has been attributed to them, the IAS Provider MUST:

   i. Notify the QHIN, Participant, or Subparticipant associated with the Responding Node that its customer has affirmatively indicated that they have received the wrong person's data. In this scenario, unless the QHIN, Participant, or Subparticipant identifies other breach mitigation factors, it would likely need to follow the HIPAA Breach Notification Rule's requirements for a one-person breach; and

   ii. Have a process in place to purge the erroneous data.

4.7. Required Information

a) Required Information is specified in the Exchange Purposes (XPs) SOP.

4.8. Response Requirement Approaches

a) From August 1, 2026 to July 31, 2027, Response Approach 2a or Respond Approach 2b below is optional for Responding Nodes with FHIR Endpoints published in the RCE Directory Service. As of August 1, 2027, all Responding Nodes MUST Respond in accordance with Response Approach 2a or Response Approach 2b. Responding Nodes with a FHIR Endpoint MUST also continue to Respond in accordance with Approach 1.

b) Responding Nodes MUST indicate which Response Approach it supports in the RCE Directory Service (*per identifiers in the directory*).

c) **Response Approach 1**: Any Responding Node that 1) receives a valid IAS Query, 2) has a FHIR Endpoint that supports the credential-based log-in flow and is listed in the RCE Directory Service, per the Facilitated FHIR Implementation SOP, and 3) matches the following demographics: verified Given (first) Name or self-asserted first name; verified Family (last) Name; verified Date of Birth, MUST return its FHIR Endpoint that supports credential-based log-in.

d) **Response Approach 2a**: Any Responding Node that receives a valid T-IAS Query MUST Respond when the following conditions are satisfied:

   i. The IAS Provider has provided the express documented and informed consent(s) ("TEFCA IAS Consent") that validates and verifies that the individual has consented to use the Individual Access Service; and

   ii. A match is determined per the Rules in Section 4.8.2;

e) **Response Approach 2b:** Any Responding Node that receives a valid T-IAS Query MUST Respond when the Responding Node has determined a match consistent with its response policy, which may include:

   i. Determining a Response is acceptable based on a match with fewer demographics than the Matching Rules for Responding Nodes in Section 4.8.2; and/or

   ii. Determining a Response is acceptable without requesting the TEFCA IAS Consent.

f) For the avoidance of doubt, an IAS Provider's response policy cannot require a match on more demographics than required by the Response logic rule specified in Section 4.8.2.

Note: The Approach 2a and 2b transaction flow is intended to support demographics-based matching for both document-based IAS Queries and FHIR-based IAS Queries, separate from the FHIR credential-based log-in flow leveraged by Approach 1.

4.8.1. TEFCA IAS Consent Policy

a) For a document-based transaction, the TEFCA IAS Consent MUST make it explicit that the IAS Query is a Query for, at least, all of the Individual's Required Information that is maintained by Responding Nodes in the RCE Directory.

b) IAS Providers MUST make it clear in the TEFCA IAS Consent that the TEFCA IAS Consent is in effect until it is revoked by the Individual, per Section 8 of the IAS Provider Requirements SOP.

c) IAS Providers SHOULD include an assertion in the IAS Query that they have the TEFCA IAS Consent. If an IAS Provider includes the TEFCA IAS Consent assertion, it MUST assert the TEFCA IAS Consent using the flow described in QTF Patient Discovery *Alternate Flow 2: Initiating Node asserts an Instance Access Consent Policy or Access Consent Policy*.

d) If the Responding Node indicates in the RCE Directory Service that it requires a TEFCA IAS Consent per Approach 2a, then the Responding Node MUST retrieve and store the asserted TEFCA IAS Consent Policy using the flow described in QTF Patient Discovery *Alternate Flow 2: Initiating Node asserts an Instance Access Consent Policy or Access Consent Policy*.

4.8.2. Matching Rules for Responding Nodes

Each Responding Node leverages its own matching algorithm to determine when an individual demographic element is considered a match. When a Responding Node has determined that a data element is matched, the following response rules apply:

a) Rule 1: Seven or Greater IAL2 Response Rule:

If all three "primary attributes" along with any four "secondary attributes" are matched then a Response is required.

- Primary Attributes (must match **all** 3): Given (first) Name; Family (last) Name; Date of Birth.
- Secondary Attributes (match **any** 4 other verified demographics). Other verified demographics may include: Middle Name/Middle Initial; Suffix; City; State; Zip; Mobile phone number; E-mail; Street Address with house number; Social Security (SSN); SSN4: last four of the SSN; State ID/Driver's License Number.

b) Rule 2: First Name Variation Response Rule:

If Rule 1 is met, except that Given (first) Name is matched through self-asserted data (i.e., the self-asserted nickname sent in the Query matches the first name in the Responding Node's system), then a Response is required.

c) Rule 3: Address Variation Response Rule:

If Rule 1 is met, except that Street address with house number is matched through self-asserted data (i.e., the self-asserted street address sent in the Query matches the street address in the Responding Node's system), then a Response is required.

4.9. Identity Token Requirements

a) The OpenID Connect Core[7] specification describes the OpenID Connect ID Token required for IAS exchange. The following additional requirements apply:

i. Public Keys Published as Bare JWKS: The CSP MUST publish public keys as bare JWKS, which MAY also be accompanied by X.509 representations of those keys.

ii. Signed ID Token: The CSP MUST support Signing ID Tokens with RSA SHA-256.

iii. Claims: The CSP MUST include the claims in Tables 1, 2 and 3, in addition to all other required OIDC Core claims.

Table 1: OpenID Connect (OIDC) JWT Header Claims

OIDC JWT Header	**Description**
alg	Hardcoded to "RS256".
kid	Identifies which key to use from the JWKS.
typ	Hardcoded to "JWT".

[7] See http://openid.net/specs/openid-connect-core-1_0.html for details

Table 2: OpenID Connect (OIDC) JWT Body Claims

OIDC JWT Body	**Description**
aud	HCID of the IAS Provider as a URI. For example, urn:oid:<oid> (per RFC 3001) must be used and must be the unique HCID per directory entry[8].
iat	When the CSP issued the token.
iss	The Issuer Identifier for the CSP. An HTTPS URL used as the base for OIDC Discovery. Validators retrieve JWKS key material via the `jwks_uri` value in `<iss>/.well-known/openid-configuration`
jti	Unique identifier for the JWT.
Demographics that MUST be included or use "Unknown" in your Query	
given_name	Blank
family_name	Blank
birthdate	Blank
address	Current verified address. A single JSON object per OIDC Core §5.1.1. MUST NOT be an array.
email phone_number	Either verified email *or* verified phone number is required. Both can be included, but at least one of these must be present.
Demographics that MUST be included if known	
middle_name	Blank
middle initial	Extension
suffix	Extension
email phone_number	A verified email *or* verified phone number that was not already included above.
ssn	Extension
ssn_last_four_digits	Extension
zip+4	Extension
gender	Blank
historical_address	Extension. Verified historical address. See list and definition of address elements, below. Array of previously verified address objects, ordered most-recent to least-recent. Each element conforms to OIDC Core §5.1.1 address schema.
csp_issued_identifier	Extension

[8] In standard OIDC, the `aud` claim contains the `client_id` assigned to the Relying Party by the OpenID Provider at the time of OAuth client registration. In TEFCA, the IAS Provider's HCID OID URI serves as the functional equivalent of the `client_id` for purposes of audience binding. CSPs MUST populate `aud` with the IAS Provider's HCID expressed as `urn:oid:<oid>` per RFC 3061, obtained from the TEFCA directory. IAS Providers MUST validate that the `aud` value in any received IAL2 Claims Token matches their own HCID OID URI. This substitution is a TEFCA-specific constraint on the OIDC `aud` claim and does not alter any other requirement of OIDC Core §2 or §3.1.3.7.

Table 3: OpenID Connect (OIDC) JWT Body Address Objects

OIDC JWT Body Address Object	Note	Optionality
formatted	Blank	OPTIONAL
street_address	Blank	REQUIRED
locality	City of residence	REQUIRED
regionality	State of residence	REQUIRED
postal_code	ZIP Code	REQUIRED
country	Blank	REQUIRED

b) If known and verified, all additional claims (such as Historical Name) **MUST** be included by adding the claim labelled as:

`http://rce.sequoiaproject.org/OIDC/claim/[claim]`

Examples of the OIDC JWT are online at the RCE resources site here: <include URL>

c) The OpenID Connect token MUST be included in all IAS Queries, including all Patient Discovery, Document Query, Document Retrieval, and FHIR Authentication.

d) An IAS Provider using Facilitated FHIR MUST follow the requirements as set out in the Facilitated FHIR Implementation SOP.

e) An IAS Provider using QHIN Query MUST relay the CSP-provided OpenID Connect token[9] within its Query using an additional Security Assertion Markup Language (SAML) attribute with Name `urn:ietf:params:oauth:token-type:id_token` and NameFormat `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` containing the OpenID Connect token in a QHIN Query or as an additional element ("id_token") within the TEFCA_IAS extension in the FHIR Query.

f) Examples are online at the RCE resources site here: <include URL>

[9] See https://openid.net/specs/openid-connect-core-1_0.html#IDToken for details on base token requirements.

5 VERSION HISTORY

Version	Revision Date	Section #(s) of Update
1.0	September 16, 2022	First Release
2.0	August 6, 2024	All Sections
2.1	April 11, 2025	All Sections – Language aligned with Exchange Purposes (XPs) SOP Version 4.0
3.0		All Sections