TEFCA RECOGNIZED COORDINATING ENTITY

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

Version 3.0

Effective Date: August 3, 2026

Applicability:

4.1 - 4.4, 4.6, 4.8 – 4.9: IAS Providers

4.3 Credential Service Providers via the IAS Providers

4.5, 4.8 – 4.9: 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 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).

TEFCA IAS FHIR Endpoint: The Fast Healthcare Interoperability Resources® (FHIR®) Endpoint that is listed in the RCE Directory Service and Responds to IAS Queries.

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. Additional 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.

b) If QHINs, Participants or Subparticipants are using Facilitated FHIR-based flows in support of their IAS, the TEFCA Exchange MUST also follow the technical requirements as specified in the Facilitated FHIR Implementation SOP. However, Sections 4.6(a)(1.2) and 4.6(b)(2.3) supersede the Facilitated FHIR Implementation SOP deadlines.

4.3. 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 is capable of doing the following:

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

b) Verify the following demographic information[2]:

i. First Name
ii. Middle Name/Middle Initial
iii. Last Name
iv. Suffix
v. Date of Birth
vi. Street Address
vii. City
viii. State
ix. Zip Code
x. Email
xi. Mobile Phone Number
xii. State ID/Driver's License Number

[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).

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 Section 4.9) with 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) Use distinct issuer URLs for production and non-production IAS TEFCA Exchange.

f) 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.

4.4. IAS Provider Responsibilities

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

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. When the verified demographics expire or are otherwise invalidated by the CSP.

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

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

vii. Zip Code, and
viii. *Either* email address *or* mobile phone

e) An IAS Provider MUST include all the IAL2-verified demographics provided by its CSP in the IAS Patient Discovery request body in accordance with QTF.

f) The IAL2 Claims Token MUST be provided in all IAS Patient Discovery, Document Query, and Document Retrieval requests, and applicable FHIR authentication requests.

4.5. Required Information

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

4.6. Response Requirement Approaches

Upon receipt of a valid IAS Query, Responding Nodes MUST support at least one of the following modes for Individuals to access their Required Information[7]. *Note:* The number attributed to each response mode is strictly for ease of reference. It does not imply implementation priority or order. On a go-forward basis, the TEFCA network intends to focus its IAS efforts on improving "verified identity-based" responses with the goal of requiring Response Mode 2 as soon as practicable in a subsequent SOP update.

a) **Response Mode 1 – Individual Authentication-based**

1.1. When a Responding Node with a TEFCA IAS FHIR Endpoint achieves a possible match[8], it MUST Respond with the applicable directory identifier for the TEFCA IAS FHIR Endpoint for the Individual to access their Required Information via Responder-supported authentication mechanisms (e.g., password, passkey).[9]

1.2. On and after July 1, 2027, all TEFCA IAS FHIR Endpoints deployed for Response Mode 1 MUST support the requirements in the Health Level Seven® (HL7®) Security for Scalable

[7] All QHINs, Participants, and Subparticipants that have a Node that is required in Federal regulation to support individual access Application Programming Interfaces (APIs) are recommended to list the TEFCA IAS FHIR Endpoint for such Node in the RCE Directory Service to support Response Mode 1. This includes health care providers that have adopted Certified EHR Technology and deployed certified API technology (e.g., technology certified to 45 CFR 170.315(g)(10)), and health plans required by Centers for Medicare and Medicaid (CMS) rules.

[8] Because this mode is focused on returning Individual authentication-based TEFCA IAS FHIR Endpoints, which will require subsequent action by an Individual, the possibility of a match based on limited demographics (e.g., first name, last name, date of birth) should take priority to give Individuals the best chance of accessing their Required Information from all locations on TEFCA.

[9] To the extent that the Responding Node is leveraging Office of the National Coordinator for Health Information Technology-certified (ONC-certified) API technology, it is expected that the same refresh token approach outlined in 45 CFR 170.315(g)(10) will be followed. We encourage non-certified technology to follow the same approach.

Registration, Authentication, and Authorization (SSRAA) FHIR Implementation Guide (IG)[10] as outlined in the Facilitated FHIR Implementation SOP.

b) **Response Mode 2 – Verified Identity-based**

2.1. When a Responding Node achieves an acceptable, uniquely attributable demographics-based match for an Individual according to its matching policy[11], it MUST Respond to the Patient Discovery Query and MUST provide at least one of the following without requiring the Individual to separately log-in using their portal credentials to the Responding Node:

2.1.1) an identifier, which can be used to initiate a Document Query to request an Individual's documents with their Required Information, or

2.1.2) a directory identifier for the TEFCA IAS FHIR Endpoint, which can be used by an Individual to grant an IAS Provider's application access to their Required Information.

2.2. IAS Providers MUST perform the Demographics Double-Check requirements as outlined in Section 4.7 before initiating an IAS Query to a Responding Node that supports Response Mode 2. If, following the IAS Provider's Demographics Double-Check, the Responding Node receives an IAS Query, the Responding Node MUST Respond with the Required Information per the Framework Agreements and Applicable Law.

2.3 On and after July 1, 2027, all TEFCA IAS FHIR Endpoints deployed for Response Mode 2 MUST support the requirements in HL7 SSRAA FHIR IG as outlined in the Facilitated FHIR Implementation SOP.

4.7. 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.

a) When an IAS Provider receives a successful Patient Discovery Response from a Responding Node, via Response Mode 2 in Section 4.6, the IAS Provider MUST perform an Individual demographics match comparison using an algorithm with both IAL2 verified

[10] The HL7 Security for Scalable Registration, Authentication, and Authorization FHIR Implementation Guide supports dynamic client registration.

[11] Responding Nodes should base their response policy on industry standard methods, accommodate high friction points like nickname resolution and address variation, and consider consensus-based approaches for patient matching such as those emerging from the CMS Health Tech Ecosystem.

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, except via Response Mode 1, if available, and

4) MAY provide the Individual with a supported FHIR Authorization Code flow approach, 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, preventing the use of Mode 2, 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. Timely 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 notification requirements per Applicable Law, and

ii. All erroneous data MUST be purged from the IAS Provider's system in a timely manner.

4.8. Compliance Dates

Review the applicable Exchange Purpose Implementation SOP: Individual Access Services (IAS) version 3.0 Section Numbers for more information regarding the requirements for these compliance dates. If not noted below, all other requirements outlined will be applicable on the Effective Date of this SOP.

SOP Section Number	Compliance Requirement	Applicability	Compliance Date
4.3	Have the capability to use distinct issuer URLs for production and non-production TEFCA IAS exchange.	CSPs via the IAS Providers	October 1, 2026
4.6	Indicate the Response Mode leveraged by the Responding Node in the RCE Directory Service	QHINs, Participants, Subparticipants	60 days following implementation of supported RCE Directory fields
4.6	Modes 1.2 and 2.3: All TEFCA IAS FHIR Endpoints MUST support the requirements in HL7 SSRAA FHIR IG as outlined in the Facilitated FHIR Implementation SOP.	QHINs, Participants, Subparticipants	July 1, 2027
4.7	Demographics Double-Check	IAS Providers	January 1, 2027
4.9	All IAL2 Claims Tokens meet requirements and SAML claim updates.	QHINs, Participants, Subparticipants	October 1, 2026

4.9. Identity Token Requirements (v3.0)

a) The OpenID Connect (OIDC) Core[12] specification describes the OpenID Connect ID Token required for IAS TEFCA Exchange. ID Tokens SHALL conform to the OpenID Connect Core specification with the following additional requirements:

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 sign ID Tokens with RSA SHA-256.

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

iii. Claims: The CSP MUST include the claims in Tables 1, 2 and 3, in addition to all other required OIDC Core claims. The CSP MUST NOT include unverified demographic claims in the token.

iv. The claims SHOULD include the tefca_ial2claims_version as an extension to indicate the policy under which the token is issued. When used, this MUST have a string value indicating the version used. If omitted, it defaults to a value of "1.0".

v. The claims MAY include the csp_issued_identifier. This identifier differs from the OIDC 'sub' with the additional constraint to remain not only unique, but also stable over time for the same patient (e.g., not change if the same patient creates a new account). If used, this identifier SHOULD be unique across all the clients of a single CSP OIDC provider even if the OIDC uses the pairwise mode for its 'sub' claims.

b) Initiating and Responding Nodes are encouraged to validate the IAL2 Claims token received in a request by reviewing the validating issuer, audience, validity window, and signature verification, as well as a comparison of the proofed identity to the patient a request identifies.

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".

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 3061) MUST be used and MUST be the unique HCID of the IAS Provider's Directory Entry[13].
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`.
exp	Expiration time for the token, appropriately set based on the system requirements for a short-lived token.
jti	Unique identifier for the JWT.
Demographics that MUST be included in your Query	
given_name	If the given name consists of multiple parts, they SHALL be delimited according to OIDC specifications.
family_name	If the family name consists of multiple parts, they SHALL be delimited according to OIDC specifications.
birthdate	Represented in YYYY-MM-DD format according to ISO 8601-1. All three elements (year, month, and day) MUST be present; partial dates (with missing year, month, or day) SHALL NOT be used.
address	Current verified address. A single JSON object per OIDC Core §5.1.1 and the additional requirements in Table 3.
email	*Either* verified email address *or* verified phone number is required. Both can be included, but at least one of these MUST be present.
phone_number	
Demographics that MUST be included if verified	
historical_address	Verified historical address using the same format as for "address".
middle_name	
middle initial	
suffix	
gender	

[13] 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 RCE 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 Object Additional Requirements

The following additional requirements apply to the address object defined in OIDC Core §5.1.1:

OIDC JWT Body Address Object	Note	Optionality
formatted	This field MAY contain multiple lines, separated by ("\r\n") or ("\n").	OPTIONAL
street_address		REQUIRED
locality	City of residence	REQUIRED
regionality	State of residence using the 2-letter codes defined in ISO 3166-2 for US states and territories.	REQUIRED
postal_code	ZIP Code	REQUIRED
country	Country code based on the 2-letter codes defined in ISO 3166	REQUIRED

c) All additional verified claims (such as Historical Name) MUST be labelled as:
`http://rce.sequoiaproject.org/OIDC/claim/[claim]`

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

e) An IAS Provider using QHIN Query MUST relay the CSP-provided OpenID Connect ID token[14] 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 ID token in a QHIN Query or as an additional element ("id_token") within the TEFCA_IAS extension in the FHIR Query, and include ID tokens for applicable FHIR workflows.

f) Examples will be made available online at the RCE resources site.

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

5 VERSION HISTORY

Version	Publication 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
3.0	July 1, 2026	All Sections