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

Version 2.0

August 6, 2024

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

Terms defined in this Section are introduced here and can be found in the TEFCA Glossary. Capitalized terms used in this SOP have the respective meanings assigned to such term in the TEFCA Glossary.

No new definitions are introduced in this SOP.

The following defined terms from the Common Agreement and other SOPs are repeated here for reference.

> **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] Privacy and security

[1] Nothing in this SOP alters a Covered Entity's obligations under the HIPAA Rules.

requirements for IAS Providers are out of scope for this SOP and are in the IAS Provider Requirements SOP, along with the Common Agreement.

4 LEVEL 1: 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. Definition

a) TEFCA Exchange under the XP Code T-IAS means 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.

4.4. Credential Service Provider

a. IAS Providers MUST have an agreement with a credential service provider (CSP) that has been approved by an RCE-selected CSP approval organization.[2]

b. The CSP approval organization must maintain a published list of CSPs who conduct identity proofing to at least Identity Assurance Level 2 (NIST IAL2) as defined by the then latest version of NIST SP800-63A. The CSP approval organization MUST require approved CSPs to be assessed for conformance to the minimum appropriate identity proofing and credential management standards, and to publish and maintain the standards to which the CSPs are assessed.

c. After verifying an Individual's identity on behalf of the IAS Provider, the CSP MUST make available to that IAS Provider a signed OpenID Connect token. Each CSP will provide an endpoint to share a JSON Web Key Set (JWKS), which a Responding Node MAY use to validate an identity token issued by that CSP.

[2] The RCE-selected CSP approval organizations are published and maintained on the RCE website.

d. The CSP signs the token with a private key and publishes the corresponding public key at <iss>/.well-known/openid-configuration per OpenID Connect Discovery[3]. For example, if the ID token's iss element is https://csp.example.com, the CSP's JWKS document would be available at: https://csp.example.com/.well-known/openid-configuration. The CSP MUST provide the JWKS publicly without requiring authentication. CSP are encouraged to rotate encryption keys as described in OpenID Connect Core[4]

e. Initiating Nodes and Responding nodes MAY use the public key to verify the CSP's signature on demographics included in the JSON Web Token (JWT.)

4.5. IAS Provider Individual Verification

a. IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2[5] (AAL2) requirements.

b. IAS Providers MUST verify the identities of Individuals to at least NIST IAL2 via a CSP prior to the Individual's first use of TEFCA Exchange, when verified demographics change, and after credentials expire. An IAS Provider MUST ensure that all updates to demographic information used for TEFCA Exchange for IAS are validated to NIST IAL2 by the CSP prior to their use.

c. IAS Providers MUST demonstrate that all Individuals that elect to use their IAS offering have proven their identities consistent with achieving NIST IAL2. This evidence MUST be included within the Query as an IAL2 Claims Token using the OpenID Connect token format as detailed in Section 4.6.

d. Queries initiated by an IAS Provider MUST include only the demographics as provided to the CSP and as part of the Individual's identity verified to NIST IAL2.

4.5.1. Verification Demographics

Verification of an Individual to at least NIST IAL2 MUST meet the following requirements:

a. Verification MUST include, at a minimum, the following demographics: First Name, Last Name, Date of Birth, Address, City, State, and Zip Code.

b. Verification SHOULD also include, but does not require the following demographics: Sex, Middle Name OR Middle Initial, Suffix, Email Address, Mobile Phone Number, Social Security Number (SSN) OR last four (4) digits of SSN, Zip Code+4, and other verifiable identifiers (e.g., Medical Record Number, Passport Number, Driver's License, or other Government Issued Identification).

[3] See Final: OpenID Connect Discovery 1.0 incorporating errata set 2 for details.
[4] Final: OpenID Connect Core 1.0 incorporating errata set 2 for details.
[5] See https://pages.nist.gov/800-63-3-Implementation-Resources/63B/AAL/ for full information on the levels

c. Historical name and/or address information MAY be included only if validated by the CSP for identity proofing for that Individual.

4.6. Identity Token

a. The OpenID Connect Core[6] specification describes the OpenID Connect ID Token required for T-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 below claims.

Table 1: OpenID Connect (OIDC) JWT Header Claims

OIDC JWT Header	
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 3001).
iat	When the CSP issued the token.
iss	The base URL of the CSP at which the JWKS is accessible.
jti	Unique identifier for the JWT.
Demographics that MUST be included or use "Unknown" in your Query	
given_name	
family_name	
nickname	
birthdate	
address	See list and definition of address elements below. Allow multiple addresses (array) if supported by the CSP.
Demographics that MUST be included if known	
historical_address	See list and definition of address elements, below. Allow multiple addresses (array) if supported by the CSP.
middle_name	
middle initial	

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

OIDC JWT Body	Description
suffix	
email	
phone_number	
SSN	
SSN_Last_four_digits	
ZIP+4	
Gender	

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

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

iv. Additional Claims MAY be included as follows: Mother's Maiden Name, Birth Place Address, Birth Place Name, Principle Care Provider ID (i.e., NPI) by adding the claim labelled as http://rce.sequoiaproject.org/OIDC/claim/ [Claim] as indicated in the below example.

Example OIDC JWT

{
"alg":"RS256",
"kid":"toW9jMUSN/5/L3iwaQGdTmNDuhvp/JcAZVH/RGF2aWQgUHlrZQ==",
"typ":"JWT"
}
{
"aud":"hci1",
"iat":1666280632,
"iss":"https://csp.example.com",
"sub":"f7bdf590-2fc4-4718-8f33-043c8f96b66d",
"jti":"bcb9533e-1cc1-48bd-848b-b4200ea504b9",
"given_name":"John",
"family_name":"Schmidt",
"middle_name":"Jacob Jingleheimer",
"nickname":"Ed",
"email":"jjjs@example.com",

“email_verified”:true,
“phone_number”:”555-555-5555”,
“gender”:”M”,
“birthdate”:”Unknown”,
“address”:{
“formatted”:”1060 West Addison Street, Chicago, IL 60613 USA”,
“street_address”:”1060 West Addison Street”,
“locality”:”Chicago”,
“region”:”Illinois”,
“postal_code”:”60613”,
“country”:”USA”
},
“http://rce.sequoiaproject.org/OIDC/claim/mothers_maiden_name”:”Vedder”,
“http://rce.sequoiaproject.org/OIDC/claim/principle_care_provider_id”:”2938457234”,
“http://rce.sequoiaproject.org/OIDC/claim/birth_place_address”: {
“formatted”:”1060 West Addison Street, Chicago, Illinois 60613 USA”,
“street_address”:”1060 West Addison Street”,
“locality”:”Chicago”,
“region”:”Illinois”,
“postal_code”:”60613”,
“country”:”USA”
}
“historical_address”:{
“formatted”:”31 Spooner Street, Quahog, Rhode Island 02907”,
“street_address”:”31 Spooner Street”,
“locality”:”Quahog”,
“region”:”Rhode Island”,
“postal_code”:”02907”,
“country”:”USA”
},
“http://rce.sequoiaproject.org/OIDC/claim/birth_place_name”:”Peaceful Valley Hospital”
}

b. The OpenID Connect token MUST be included in the Security Assertion Markup Language (SAML)for all IAS Queries, including all Patient Discovery, Document Query, Document Retrieval, and FHIR Authentication.

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

d. An IAS Provider using QHIN Query MUST relay the CSP-provided OpenID Connect token[7] within its Query using an additional SAML attribute statements (“id_token") and

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

NameFormat containing oasis:names:tc:SAML:2.0:cm:bearer, 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. For example:

```
<saml2:Attribute Name="id_token">
<saml2:Attribute NameFormat="oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:AttributeValue>{Base64 encoded token}</saml2:AttributeValue>
</saml2:Attribute>
```

4.7. Required Information

a. For TEFCA Exchange under the XP Code T-IAS, beginning December 31, 2024, Required Information is, at least, the USCDI v1 data classes and data elements[8] that the Responding Node maintains.

b. If the Responding Node is controlled by a Health Plan, the Responding Node MUST also share individual claims and encounter data (without provider remittances and enrollee cost-sharing information) that it maintains.

c. Additional details on implementation specifications for Required Information are provided in the QTF and applicable XP Implementation SOP(s). For the avoidance of doubt, prior to January 1, 2026, the QTF does not require USCDI data to conform to USCDI vocabulary standards.

4.8. Response Requirement

a. Any Responding Node that receives an IAS Query from an IAS Provider that includes the appropriate IAL2 Claims Token, as specified in 4.3(c), and that achieves an acceptable demographics-based match based on responder policy OR where responder issued credentials are presented MUST Respond with the Required Information per the Framework Agreements and Applicable Law.

[8] See https://www.healthit.gov/isp/united-states-core-data-interoperability-uscdi for details.

5 VERSION HISTORY

Version	Revision Date	Section #(s) of Update
1.0	September 16, 2022	First Release
2.0	August 6, 2024	All Sections