ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

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

Publication Date: September 16, 2022

Applicability:
3.1, 3.2, 3.3, 3.4, and 3.6: IAS Providers Leveraging Demographics-Based Patient Matching for Requests

3.5: QHINs, Participants, Subparticipants (for purposes of IAS Responses)

1 Common Agreement References

The specifications set forth in this SOP are required for implementation in addition to the terms and conditions found in **CA Section 10: Individual Access Services**.

Capitalized terms used below without definitions shall have the respective meanings assigned to such terms in the Common Agreement and the QHIN Technical Framework.

2 Purpose

This SOP identifies specific requirements that IAS Providers are required to follow for Individual identity verification. This SOP also identifies when a QHIN, Participant, or Subparticipant is required to Respond to an IAS Request.[1]

3 Procedure

1. **Credential Service Provider.** IAS Providers are required to have an agreement with a credential service provider (CSP) who has been approved by an RCE-selected CSP approval organization.[2] The CSP approval organization must maintain a published list of CSPs who conduct identity proofing to Identity Assurance Level (IAL) 2 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.

2. **Identity Verification Requirement**. IAS Providers are required to verify the identities of Individuals via a CSP prior to the Individual's first use of Connectivity Services, and then again after credentials expire.
    a. Verification must include, at a minimum, the following demographics: First Name, Last Name, Date of Birth, Address, City, State, ZIP.
    b. Verification should also include, but does not require, Sex, Middle Name, Middle Initial, Suffix, Email Address, Mobile Phone Number, SSN, SSN last 4 digits, ZIP+4, Medical Record Number, and other identifiers.

3. **Evidence of Individual Identity Proofing**. IAS Providers are required to demonstrate that all Individuals that elect to use their IAS offering have proven their identities consistent with achieving NIST IAL2.

[1] Nothing in this SOP alters a Covered Entity's obligations under the HIPAA Rules.
[2] The RCE-selected CSP approval organizations will be published and maintained on the RCE website.

a. The user proof of identity verification will be included in the QHIN Query or QHIN Message Delivery request SAML via a <saml:AttributeStatement> tag set which includes:
    i. <saml:Attribute name="csp" NameFormat=""> comprising the Business Name or URL of the CSP and,
    ii. <saml:Attribute name="validated_attributes" NameFormat=""> with a comma or space separated list of the user demographics and identifiers that have been verified by the CSP.

b. The following is an example SAML information block identifying the CSP organization and the list of validated attributes:

```
<saml:AttributeStatement>
 <…>
<saml:Attribute Name="csp" NameFormat="">
 <saml:AttributeValue>http://www.example-csp.com</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="validated_attributes" NameFormat="">
 <saml:AttributeValue>lname,fname,address,city,state,email,ssn,sex
 </saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

c. The codes for the validated attributes are as follows:

Demographic	Code
First Name	fname
Last Name	lname
Middle Name	mname
Middle Initial	minitial
Suffix	suffix
Date of Birth	dob
Sex	sex
Address	address
City	city
State	state
ZIP/ZIP+4	zip
Phone Number	phone
Email Address	email
Social Security Number	ssn
SSN last 4 digits	ssn4
Medical Record Number	mrn
Identifier	identifier

d. Historical demographic codes are above with an h prefix (e.g., historical first name is hfname). A second historical demographic may have a numeric designation appended (e.g., hfname2). Numbering of additional historical codes begins at 2 and should not skip numbers.
e. No IAS Request without the above SAML tags is to be processed. If an IAS Request lacks the above required SAML tags, the following SAML fault status code must be returned: urn:oasis:names:tc:SAML:2.0:status:AuthnFailed
f. An IAS Provider may include in its QHIN Query or QHIN Message Delivery a token provided by the CSP asserting IAL2 verification of the Individual has been completed.

4. **Use of Proven Demographics.** IAS Providers are required to submit queries to the QHIN that include only the demographics as provided to the CSP and as part of the patient's identity verified to NIST IAL2.
    a. Historical name and/or address information may also be included if and only if validated by the CSP for identity proofing for that Individual.
    b. Historical information must be marked as historical.

5. **Response**. QHINs, Participants, and Subparticipants that receive a QHIN Query for an IAS Exchange Purpose that provides the information specified in (3) and (4) and provides an acceptable match based on responder policy are required to Respond with the Required Information per the Common Agreement, the QHIN Technical Framework, and the Exchange Purposes SOP.[3] A responder's determination of a patient match shall not require more than the demographics in (2a) and (2b) above, unless required by applicable law.

6. **Certified Changes Only**. An IAS Provider is required to ensure that all updates to demographic information transmitted via Connectivity Services for the IAS Exchange Purpose have the demographics validated to NIST IAL2 by the CSP prior to their use.

[3] The IAS Exchange Purpose is required six (6) months following the publication date of this SOP.