ONC TEFCA RECOGNIZED COORDINATING ENTITY

Standard Operating Procedure (SOP): Facilitated FHIR Implementation

Version 1.0

July 1, 2024

Applicability: QHINs, Participants, Subparticipants that engage in TEFCA Exchange leveraging Facilitated FHIR

TABLE OF CONTENTS

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 without definition here MUST have the respective meanings assigned to such term in the TEFCA Glossary.

FHIR Adopters: Any QHIN, Participant, or Subparticipant that wishes to engage in TEFCA Exchange leveraging Facilitated FHIR, as described in this SOP.

3 Purpose

This SOP identifies specific requirements for Facilitated FHIR implementation activities. Any FHIR Adopter may participate in any of the FHIR activities specified in this SOP.

The goal of this SOP is to encourage consistent adoption of a scalable, network approach to Facilitated FHIR across TEFCA. This SOP provides a roadmap that allows for a transition period to ease adoption of an eventual network-wide approach. Many of the conformance requirements in this SOP are optional to allow for maximum flexibility during the transition period. This will likely lead to the need for direct coordination between FHIR Adopters and could result in acceptable inconsistencies in the scope of data exchanged, the Exchange Purposes selected for Facilitated FHIR implementation activities, and the initial partners with whom each FHIR Adopter exchanges. The FHIR Implementation Advisory Group[1] is established to collect and document learnings and progress towards this goal, including assessing adoption and implementation of the HL7 Security for Scalable Registration, Authentication, and Authorization (HL7 SSRAA) FHIR Implementation Guide (IG). The FHIR Advisory Group will provide regular updates to the TEFCA Transitional Council or the Governing Council (as applicable) on progress, and informed by that progress, will have the authority to recommend changes to the dates in the FHIR Security

[1] See Advisory Groups SOP: https://rce.sequoiaproject.org/tefca-and-rce-resources/

Roadmap detailed in Section 6.2 of this SOP and/or conformance statements throughout this SOP for approval by ONC and the RCE.

4 FACILITATED FHIR QUERY SCENARIO

In this scenario, a health care provider treats a patient in an emergency department and seeks to retrieve information regarding the patient's care from the patient's primary care provider(s) through Facilitated FHIR TEFCA Exchange.

The basic pattern of the flow follows the Patient Discovery and Document Query flows and then diverges to use FHIR queries to identify the specific patient and query for specific FHIR resources.

Once the Initiating Node has the appropriate endpoints it begins a HL7 *FAST* UDAP Security for Scalable Registration, Authentication, and Authorization (SSRAA) Trusted Client Registration to assert its identity to the authorization server using a TEFCA certificate. Once identified and issued a client_id, the Initiating Node authenticates, authorizes access, and receives an access token.

Once authorization has been granted, the Initiating Node queries the FHIR server for the appropriate Patient Resource including the demographics known to the Initiating Node and begins to Query for that patient's health care data.

Note: This flow assumes SSRAA IG use; alternate flows may use manual registration and/or SMART on FHIR.

Specified standards for a Facilitated FHIR Query are included in **TABLE 1. SPECIFIED STANDARDS FOR FACILITATED FHIR QUERY**.

TABLE 1. SPECIFIED STANDARDS FOR FACILITATED FHIR QUERY

Query Functions	Specified Standard(s) / Profile(S)
Secure Channel	• IETF TLS 1.2 w/ BCP-195[2] or • IETF TLS 1.3 w/ BCP-195
Node Registration	• OAuth V2.0 • HL7 *FAST UDAP* Security for Scalable Registration, Authentication, and Authorization V1.0.0
User Authentication	• OAuth V2.0 • HL7 *FAST UDAP* Security for Scalable Registration, Authentication, and Authorization V1.0.0 • SMART Application Launch Framework Implementation Guide Release 1.0.0 • SMART Backend Services: Authorization Guide

[2] *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* (IETF BCP 195) available at https://tools.ietf.org/html/bcp195.

Query Functions	Specified Standard(s) / Profile(S)
Authorization & Exchange Purpose	• OAuth V2.0 • HL7 *FAST UDAP* Security for Scalable Registration, Authentication, and Authorization V1.0.0 • SMART Application Launch Framework Implementation Guide Release 1.0.0 • SMART Backend Services: Authorization Guide
Query for Patients	• IHE XCPD • FHIR R4 V4.0.1 • HL7 FHIR US Core Implementation Guide V3.1.1 or higher
Information Query and Retrieve	• FHIR R4 V4.0.1 • HL7 FHIR US Core Implementation Guide V3.1.1 or higher • FHIR Implementation Guides as required by the Exchange Purposes (XP) SOP and XP Implementation SOPs, as applicable
Auditing	• IHE ATNA (QHINs; Content only) • ASTM E2147-18 (Participant/Subparticipant; Content only)

4.1. Actors

The following lists the Actors and services included as part of the workflow. Cardinality represents the number of that Actor/service expected and which QTF "system" Actor is expected to have that service or Actor role. The Initiating Node uses a FHIR $match operation with the Patient Discovery demographics to validate the Response from the QHIN and to gain patient context.

Actors/Services	Cardinality	System Actor
Initiating Node	1..1	Any Initiating Node
Initiating Gateway	1..1	Initiating QHIN
QHIN Directory	1..1	Initiating QHIN
QHIN Directory	1..*	Responding QHIN(s)
Responding Gateway	1..*	Responding QHIN(s)
Responding Node(s)	1..*	Any Responding Node

4.2. Assumptions

1. All Initiating and Responding Nodes agree on transport level details (specified for transactions between QHINs elsewhere in this document) that allow for the following:
   a. System authentication and encrypted communications over a secure channel;
   b. The ability to provide information in each transaction that identifies security and permission details about the Query such as: who is sending, what their role is, and what their Exchange Purpose is; and
   c. The ability of Actors to choose if/how to allow a transaction to proceed based on privacy policies, security details, and the requirements of the Common Agreement.

2. The Initiating Node may not know the patient identifier(s) and/or Responding Node(s) for a Query.

3. The RCE Directory has up-to-date listings of all FHIR-capable Participants' and Subparticipants' FHIR Endpoints.

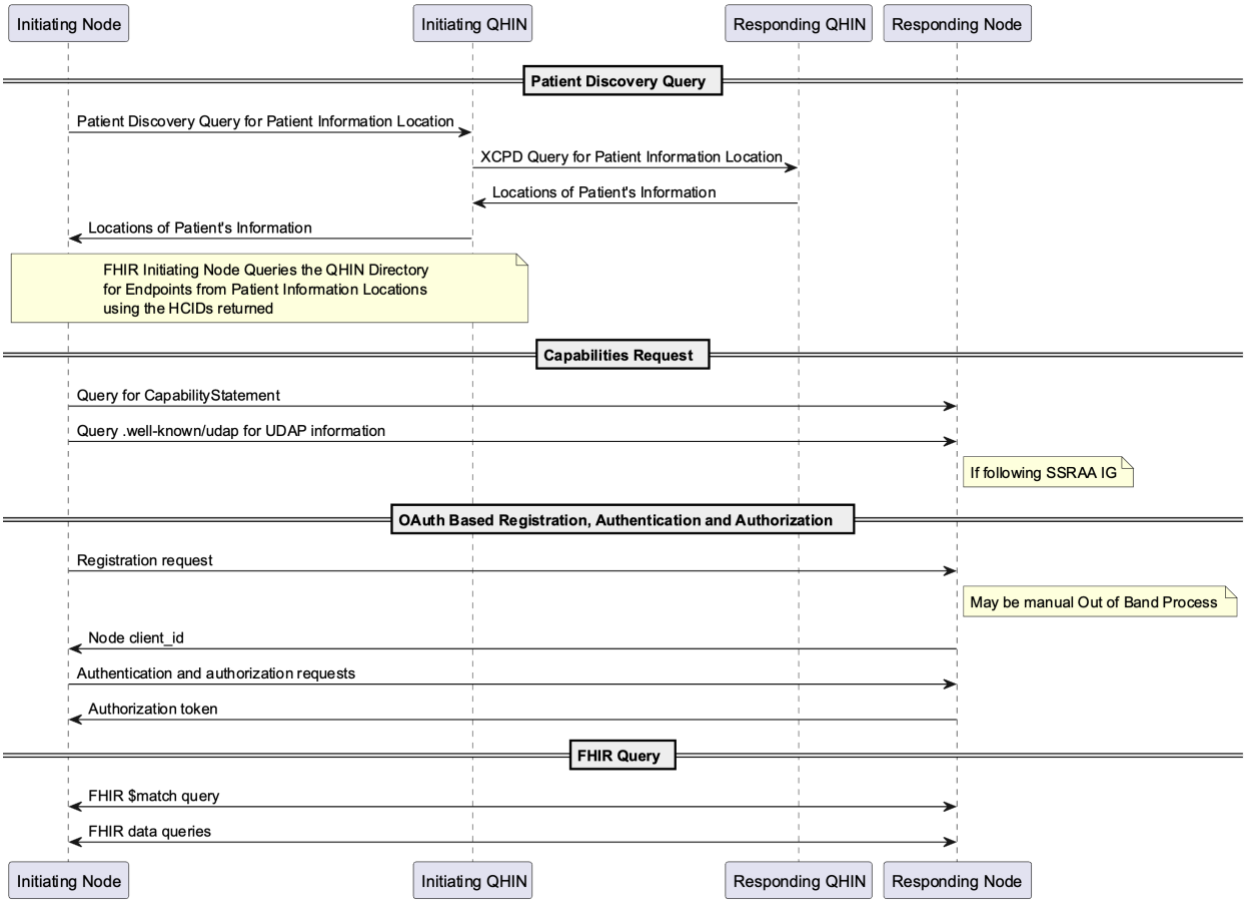
4.3. Pre-conditions

This workflow assumes the following conditions:

1. The Initiating Node knows sufficient patient demographics for a successful match as determined by the Responding Node.
2. Each Actor has the appropriate service endpoint(s) and other connectivity information for any other Actors above or below it in the hierarchy with which it connects directly.
3. The RCE Directory includes the organization facility name(s) for all current Participants and Subparticipants.
4. Each QHIN maintains an up-to-date copy of the RCE Directory.
5. Each QHIN has either a Record Locator Service (RLS) or Enterprise Master Patient Index (eMPI) or uses other techniques to perform patient lookup within the Service Level Requirements timeout limitation as specified in the QHIN Service Level Requirements Policy.

5 USE CASE STEPS

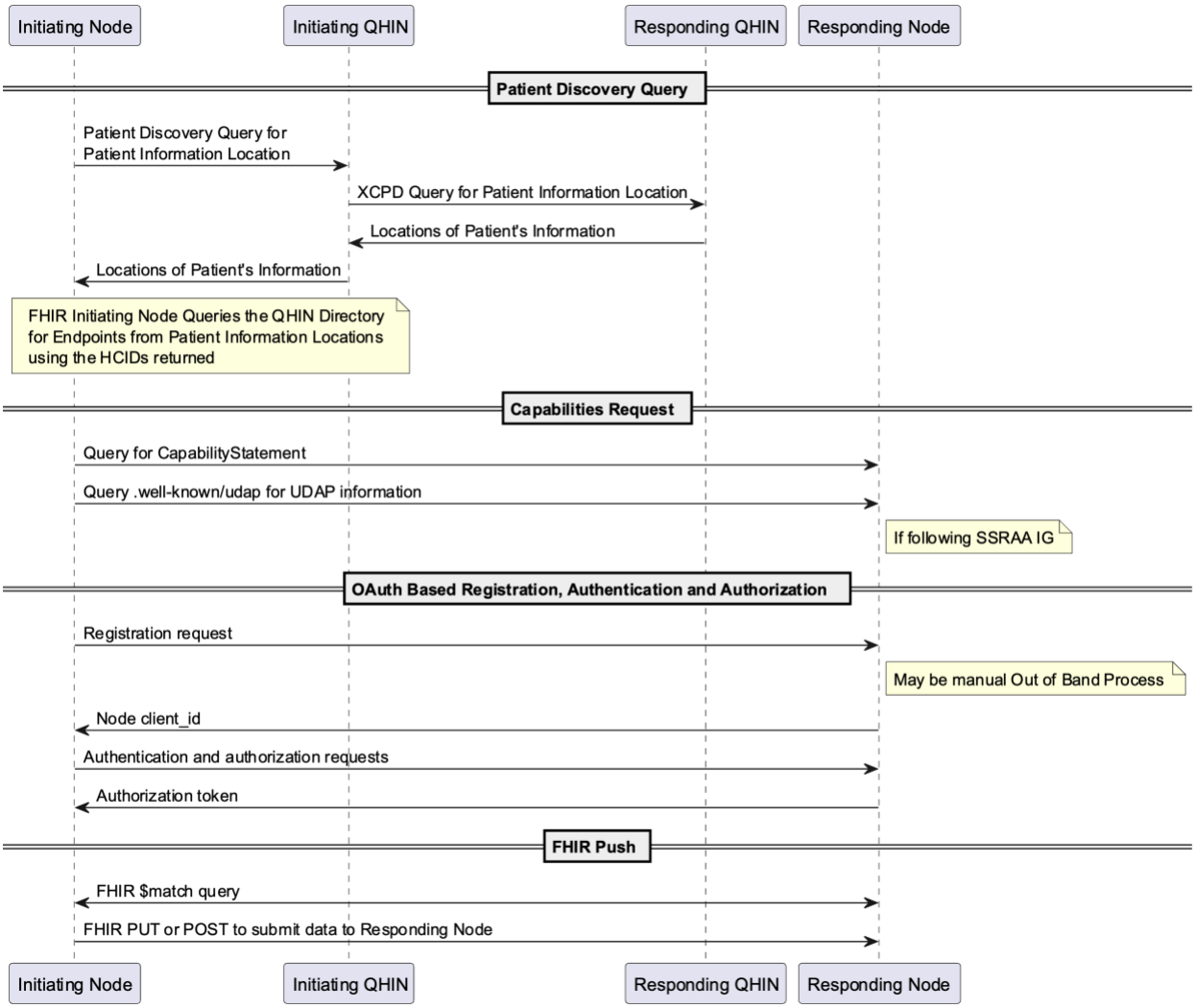
Nominal Flow



1. The Initiating Node sends a Patient Discovery Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to Query for patient information as per the QTF.
   a. The Patient Discovery returns a list of HCIDs with relevant patient information.
2. Initiating node queries the QHIN Directory for FHIR Endpoints using the HCIDs returned.
3. Initiating Node selects which FHIR Endpoint(s) they will be querying for data.
4. The Initiating Node queries for the Responding Node's CapabilityStatement and reviews all capabilities for matches with the Initiating Node requirements.
5. The Initiating Node queries the .well-known/udap endpoint to get all needed information for UDAP registration including the address of the authorization server and supported scopes.

   a. If not following the SSRAA FHIR IG, registration is completed out of band, the flow continues at Step 6.
   b. The Initiating Node sends a UDAP Dynamic Client Registration Request to the Responding Node's authorization server with all relevant information and a list of needed scopes.
   c. The Responding Node's authorization server returns a client_id unique to that Initiating Node.
6. The Initiating Node uses the returned client_id, relevant scopes and user information contained in the relevant extensions to Request authentication and authorization to query patient data.
   a. The authorization server grants the Initiating Node a token allowing for querying of data from the Responding Node.
7. The Initiating Node uses the token in the query flow to identify itself to the Responding Node and uses the $match operation with a US Core Patient Resource to gain a list of patients matching the demographics.
8. The Initiating Node selects the appropriate patient from the list provided and begins Querying for associated data.
   a. The Initiating Node and Responding Node create an audit log of all transactions.

Alternate Flow 1: FHIR Push



1. Flow begins at step 8 of the Nominal Flow above.
2. The Initiating Node selects the appropriate patient from the list provided and executes a PUT or POST to submit data to the Responding Node.

6 PROCEDURE

6.1. Overarching Requirements

1. All TEFCA Exchange leveraging Facilitated FHIR, including transactions that use out-of-band arrangements, as described in Section 6.1(4)(iii) of this SOP, MUST abide by the Common Agreement, QHIN Technical Framework, and Standard Operating Procedures (SOPs), except as stated herein.

2. All FHIR Adopters MUST follow the requirements as specified in the QHIN Technical Framework (QTF) Constraints Specific to Facilitated FHIR Exchange when initiating or Responding to a FHIR Query.
3. All use of certificates for HL7 SSRAA or other authentication must be consistent with the use of TEFCA certificate requirements as set out in the Technical Trust Requirements document.
4. All FHIR Adopters MUST indicate in their Directory Entry the supported registration and authentication/authorization standards used as follows:
    a. The FHIR Endpoint to be used for TEFCA FHIR exchange.
    b. Indicate support for the HL7 SSRAA FHIR IG 1.0.0 STU 1 – US Dynamic Registration (True/False)
    c. Indicate support for one or more of:
        i. HL7 SSRAA FHIR IG 1.0.0 – STU 1 US, Sections 4 and 5;
        ii. SMART Backend Services or Application Launch Framework Implementation Guide Release (SMART) 1.0.0; and
        iii. Some other authentication and authorization framework that adheres to the requirements of the QTF, based on out-of-band agreements between exchange partners.

6.2. FHIR Security Roadmap

1. Requirements surrounding the registration, authentication, and authorization of a FHIR client to a Responding Node MUST follow these requirements:
    a. Prior to January 1, 2026:
        i. All FHIR Adopters MAY follow the requirements of HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Section 3 Registration.
            1. Manual registration requests for client_id MUST be resolved within 5 business days where sufficient information has been provided. Information requirements MUST NOT exceed those in Section 3 of HL7 SSRAA FHIR IG and this SOP.
        ii. All FHIR adopters MUST use one of the following:
            1. HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Sections 4 and 5;
            2. SMART Release 1.0.0; or
            3. Some other authentication and authorization framework that adheres to the requirements of the QTF, based on out-of-band agreements between exchange partners.

b. Beginning January 1, 2026, all FHIR Adopters MUST follow the requirements in HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Sections 2, 3, 4, and 5.

6.3. Exchange Partners

Prior to January 1, 2026, FHIR Adopters MAY determine their own exchange partners. FHIR Adopters will be responsible for coordinating directly with each other to identify which FHIR Adopters have (1) a compatible registration approach and (2) a compatible approach to patient discovery.

This may result in FHIR Adopters not using FHIR Exchange with all other FHIR Adopters, which will not be considered to be a violation of the Framework Agreements, any applicable SOP, or the QTF.

6.4. Exchange Purposes

1. All transactions MUST use the Exchange Purpose code system OID: 2.16.840.1.113883.3.7204.1.5.2.1, as defined in the Exchange Purposes (XPs) SOP or an applicable Exchange Purpose (XP) Implementation SOP.
2. Notwithstanding the foregoing, if a QHIN has a TEFCA FHIR testing environment, they MUST test FHIR capabilities with any QHIN or Candidate QHIN who request non-production partner testing of such capabilities.

6.5. General Requirements

1. FHIR Adopters MUST make available all US Core V3.1.1 or higher Resources where such data exists.
2. The following FHIR Implementation Guides SHOULD be supported:
    a. Bulk Data Access IG V1.0.1,
    b. Mobile access to Health Documents (MHD) V4.2.1,
        i. ITI-67 and ITI-68 transactions SHOULD be supported, all other transactions MAY be supported.
    c. HL7 Da Vinci Clinical Data Exchange FHIR Implementation Guide Version 2.0.0,[3]
    d. HL7 Da Vinci Payer Data Exchange FHIR Implementation Guide Version 1.0.0,[4] and
    e. Any other FHIR IG included in an XP Implementation SOP.

6.6. FHIR Endpoints & Endpoint Discovery

A required endpoint listing will be executed through a query to the QHIN's Directory following a Patient Discovery Query. These Queries will return FHIR Endpoints for locations where patient

[3] Implementation Guide available at https://hl7.org/fhir/us/davinci-cdex/
[4] Implementation Guide available at https://hl7.org/fhir/us/davinci-pdex/index.html.

data exists. FHIR Endpoints returned in these Queries will not be limited to patient context and a patient search will be necessary to identify the specific patient.

1. All discovery of endpoints by Participants and Subparticipants MUST be executed by a Query to the QHIN Directory using the HCID returned from a Patient Discovery Query which will have the FHIR Endpoint(s) for Responding Nodes.
2. All Responding Nodes with FHIR Capabilities listed in the RCE Directory Service MUST provide access to the Patient Resource and at least one additional patient compartment[5] FHIR Resource.
3. All Responding Nodes MUST provide a CapabilityStatement resource.
4. Responding Nodes MUST use the FHIR CapabilityStatement resource to define FHIR server capabilities.
5. All FHIR-capable Responding Nodes MUST provide at least one publicly discoverable CapabilityStatement where CapabilityStatement.kind=”instance”.
6. All Responding Nodes with FHIR Capabilities listed in the RCE Directory Service MUST provide a CapabilityStatement for each endpoint associated with a FHIR server, defining the capabilities available at that endpoint.
7. Capabilities listed within the CapabilityStatement MUST include all FHIR Implementation Guide operations supported by the Responding Node.
8. Capabilities listed within the CapabilityStatement SHOULD include all FHIR Implementation Guides supported by the Responding Node.

6.7. Patient Matching

Patient matching for the purpose of gaining or confirming the needed patient identifier for further data retrieval will conform to the FHIR Core Patient operation $match but use a US Core Patient Resource to allow for the additional demographics, including race and ethnicity.

1. All Nodes with FHIR Capabilities listed in the RCE Directory Service MUST support the FHIR $match operation using a US Core Patient Resource
2. $match operations MUST be executed using the demographics matching those used in the Patient Discovery Query as payload to allow for full Responses to Patient Queries from Initiating Nodes.
3. Responding Nodes SHOULD have the capability to return more than one potential patient match when a patient search yields more than one match.
4. Responding Nodes MUST NOT return more than one potential match when such action could be a violation of HIPAA or other Applicable Law.

[5] See https://www.hl7.org/fhir/r4/compartmentdefinition-patient.html for a complete definition

5. When the Initiating Node specifies "onlyCertainMatches"=true within a $match Query Responding Nodes MUST honor that request by returning one and only one match, if a unique match can be found.
6. Responding Nodes MUST NOT return more than 100 potential matches when onlyCertainMatches is set to false.
7. All Initiating Nodes MUST include all available US Core Patient Resource demographics, including current and historical addresses, which can be sent and are not constrained by applicable law, within a $match Query for patient discovery with the exception of a Social Security Number, which MAY be included.
8. The Responding Node MAY fall back to requesting user specified credentials whenever authenticating with patient demographics per the Individual Access Services (IAS) XP Implementation SOP: Demographic Matched fails or is not feasible.
9. Initiating Nodes MUST populate all Query elements in accordance with the adopted FHIR US Core's vocabulary bindings.
10. Initiating Nodes MUST normalize addresses to the Project US@[6] Technical Specification. However, if the field does not contain a street address but contains other geographical details, it is recommended that whatever information the patient provided not be abbreviated.
11. Demographics used in all Queries and Query Responses MUST follow all elements in the US Core Patient Resource, where available.
12. Responding Nodes MUST NOT require more than all US Core Patient Resource demographics before returning a patient list Response.

6.8. Provenance Use

The Provenance Resource will be used to track transformation of data to and from FHIR resources. This will allow for accurate understanding of when a patient record is converted so that appropriate follow-ups can be made, where necessary. Use of Provenance only applies where data has been transformed.

1. A FHIR US Core Provenance Resource MUST be available for Query for any data that has been transformed from another interoperability standard.
2. Responding Nodes MUST use the FHIR US Core Provenance Resource to define the source of the data and as a record of any transformations to convert the data to or from FHIR resources as per FHIR Core section 6.3.4.5 Use of Provenance to record Import and Transform.

[6] *Project US@ Technical Specification.* – available at https://oncprojectracking.healthit.gov/wiki/pages/viewpage.action?pageId=180486153

3. Provenance.target MUST be references to all FHIR resources extracted from the document referenced by the Provenance.entity element.
4. Provenance.policy MUST contain the static URI "urn:oid:2.16.840.1.113883.3.7204.1.5.1.2".
5. Provenance.agent MUST contain at least one entry [1..*] describing the system that extracted the elements from the document.
6. Provenance.agent.type MUST contain code "assembler" from the code system http://hl7.org/fhir/ValueSet/provenance-agent-type.
7. Provenance.agent.who SHOULD be a Device Resource identifying the system that extracted the data. If no Device resource exists, the Organization Resource who conducted the extraction MUST be used.
8. Provenance.entity MUST contain one element [1..1] describing the source document from which the information was extracted.
9. Provenance.entity.role MUST be the code "source" from the http://hl7.org/fhir/provenance-entity-role code system.
10. Provenance.entity.what MUST be a reference to the DocumentReference Resource pointing to the original document.

6.9. Error Responses

All error messages returned in Response to a FHIR Query will need to have sufficient information to allow for troubleshooting. This will follow the FHIR OperationOutcome Resource requirements and specification in FHIR Core R4.

1. Errors resulting from FHIR transactions SHOULD use the OperationOutcome Resource to return both human readable and machine processable information with sufficient detail to allow the client to determine if the error can be corrected at the client side.
2. QHINs, Participants, and Subparticipants MAY choose to obscure some of OperationOutcome details for security reasons. Any such choices SHOULD be linked to articulable security concerns.

6.10. Security

The following requirements are additional constraints on OAuth 2.0 [7] to further enable interoperability without reducing the security of transactions.

1. Registration, Authorization and Authentication for FHIR exchange SHOULD follow the requirements specified in sections 0 and 4.
2. Authorization Servers SHOULD issue access tokens with a lifetime no longer than 60 minutes.

[7] https://oauth.net/2/

3. An Authorization Server MAY issue a refresh token to an application using the Authorization Code Grant type if the Authorization Server issues a refresh token to an application that has requested and has been authorized to use the “offline_access”.
4. All implementations MUST support RS256, and SHOULD support ES256, ES384 and RS384.

6.11. Requirements for Use of HL7 SSRAA

Registration

1. If the Authorization Server returns a different client_id in the registration modification Response, the client application MUST use only the new client_id in all subsequent transactions with the Authorization Server.
2. The udap_certifications_supported metadata returned MUST include https://rce.sequoiaproject.org/udap/profiles/basic-app-certification.
3. The udap_certifications_required metadata returned MUST include https://rce.sequoiaproject.org/udap/profiles/basic-app-certification.
4. An Authorization Server MAY issue a refresh token to an application using the Authorization Code Grant type if the Authorization Server issues a refresh token to an application that has requested and has been authorized to use the “offline_access”.
5. The software statement MUST contain a certification_name element of “TEFCA Basic App Certification".
6. The software statement MUST contain a certification_uris element which MUST be a fixed array with single string element of https://rce.sequoiaproject.org/udap/profiles/basic-app-certification
7. If a new client_id has been issued for a registration modification, the responding Authorization Server MUST disable the old client_id so that it cannot be used for subsequent Queries.
8. Any retired client_ids MUST be preserved by the Authorization Server so that it can be associated with log entries and the Initiating Node.
9. If the client attempts to register for either a Client Credentials Grant or an Authentication Code Grant with a User scope but does not specify a user during registration, the server must respond with an “invalid scope” and not attempt to correct the scope to a System scope.

Business to Business (B2B) Client Credentials Grant

1. The software statement extensions element MUST be present and contain a JSON Object containing the key “hl7-b2b” with a value equal to a B2B Authorization Extension Object.
2. Use of the hl7-b2b extension MUST conform to the requirements in Table 2 TEFCA Specific hl7-b2b Extension Requirements.

TABLE 2. TEFCA SPECIFIC HL7-B2B EXTENSION REQUIREMENTS

organization_id	required	String containing the URL of Initiating Node's Organization resource in the RCE Directory service
organization_name	required	String containing the Initiating Node's human readable organization name
subject_id	conditional	String containing a unique identifier for the requestor responsible for originating the Query. MUST be present when applicable
purpose_of_use	required	An array of strings containing the purpose for which the data is Queried, from the code set of authorized Exchange Purposes found in the Exchange Purposes SOP

3. When the B2B Authorization Extension object is included in a token request and the data holder determines that the authorization metadata submitted is insufficient for the data holder to grant access because the requestor has omitted the ACP parameter or has asserted a policy that is not acceptable to the data holder, then the Authorization Server MUST return an invalid_grant error Response to the token request, and this error Response SHOULD include the TEFCA-specific error extension as specified in Table 3 TEFCA Authorization Extension Error Object in the 'extensions' object of the error Response.

TABLE 1. TEFCA AUTHORIZATION EXTENSION ERROR OBJECT

Extension Name: "hl7-b2b"		
Element	**Optionality**	**Requirement**
consent_required	required	The list of acceptable Access Consent Policy Identifier(s) corresponding to the asserted Access Policy required for authorization, an array of string values from the list of valid policy OIDs in Appendix A of this IG, each expressed as a URI.
consent_form	optional	A URL as a string where the required consent form may be downloaded, if applicable.

4. Responders supporting use cases that require transmission of consent information MUST support the consent_policy and consent_reference claims and MUST be able to resolve a DocumentReference[8] or Consent[9] Resource included in the consent_reference array.

Individual Access Services (IAS) Queries

1. Responders MUST support the Authorization Code Grant type for IAS Queries.
2. The Initiating Node MUST provide the tefca_ias extension during the Authorization flow.

[8] See https://hl7.org/fhir/R4/documentreference.html
[9] See https://hl7.org/fhir/R4/consent.html

3. The responder MUST support the TEFCA IAS Authorization Extension Object identified by the extension key "tefca_ias" as defined in Table 4 TEFCA IAS Authorization Extension Object.

TABLE 4. TEFCA IAS AUTHORIZATION EXTENSION OBJECT

Extension Name: "tefca_ias"		
Element	**Optionality**	**Requirement**
version	Required	Fixed string value: "1"
purpose_of_use	Required	Fixed Value "T-IAS".
user_information	Required	FHIR RelatedPerson Resource with all known demographics. Where the user is the patient, the value of the relationship element MUST be "ONESELF"
patient_information	Required	FHIR US Core Patient Resource with all known and validated demographics
Ial_vetted	Conditional	OIDC token provided by Identity Verifier when the Identity Verifier is not the Responding Node. Responding server MAY respond with invalid_grant if missing.
consent_policy	Required	The Access Consent Policy Identifier corresponding to the asserted Access Policy that represents the identity proofing level of assurance of the user, array of string values from the subset of valid policy OIDs in that represent identity proofing levels of assurance, each expressed as a URI, e.g. ["urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.2.1"]
consent_reference	Optional	An array of FHIR Document Reference or Consent Resources where the supporting access consent documentation can be retrieved, each expressed as an absolute URL, e.g. ["https://tefca.example.com/fhir/R4/DocumentReference /consent-6461766570"]
Id_token	Optional	Additional token as per relevant SOP

4. A client application requesting a token for patient requests MUST include the TEFCA IAS Authorization Extension Object in its token request in addition to the hl7-b2b Authorization Extension object during the authorization flow.
5. The user metadata submitted by the requesting application in the patient_information element of the TEFCA IAS Authorization Extension Object MUST correspond to the verified identity attributes of the permitted user who is making the Query.
6. If the submitted user information does not sufficiently match a person known to the responder, or if the responder does not support this workflow for IAS Queries, it MUST return an invalid_grant error in Response to the token request.

6.12. Requirements for Use of SMART Backend Services or App Launch Implementation Guide

1. The SMART capabilities MUST include “launch-standalone”, “client-public”, “context-standalone-patient”, “permission-patient”, and “permission-user”.
2. The SMART grant_types_supported MUST include “authorization_code”.
3. Each QHIN, Participant, or Subparticipant MUST establish a process by which its FHIR Initiating Node(s) completes client registration. As part of that process, at least the information in the following table MUST be collected.

TABLE 2. TEFCA CLIENT REGISTRATION INFORMATION

Element	Optionality	Description
client_name	Required	Human Readable Name of the client application
redirect_uris	Required	An array of one or more redirection URIs used by the client application.
logo_uri	Optional	A URL string referencing an image associated with the client application, i.e., a logo. The URL MUST use the https scheme and reference a PNG, JPG, or GIF image file, e.g., `"https://myorg.example.com/MyOrg.png"`
jwks_url	Required	A URL string referencing the location of a JSON Web Key Set (JWK) which is constructed per RFC 7517. The URL MUST use the https scheme.
scope	Required	String containing a space delimited list of scopes requested by the client application for use in subsequent requests. The list of scopes MUST be limited to only those that the client application intends to access. The Authorization Server MAY consider this list when deciding the scopes that it will allow the application to subsequently request. Listed scopes MUST be derived from scopes specified by the SMART App Launch IG. For IAS requests, patient scopes MUST be requested. For other requests, user scopes MUST be requested.
purpose_of_use	Required	One of the codes corresponding to the Exchange Purpose code system OID: 2.16.840.1.113883.3.7204.1.5.2.1, as defined in the Exchange Purposes SOP or an applicable Exchange Purpose Implementation SOP.

4. Authorization Servers MUST assign a unique client_id to each registered client.
5. Responders MUST support the Authorization Code Grant type for requests.
6. The Initiating Node MUST provide the tefca_smart extension when requesting the authorization code.

7. The responder MUST support the TEFCA User Authorization Extension object identified by the key "tefca_smart " as defined in TABLE 3. TEFCA SMART AUTHORIZATION EXTENSION OBJECT.

TABLE 3. TEFCA SMART AUTHORIZATION EXTENSION OBJECT

Extension Name: "tefca_smart"		
Element	**Optionality**	**Requirement**
version	Required	Fixed string value: "1"
purpose_of_use	Required	One of the codes corresponding to the Exchange Purpose code system OID: 2.16.840.1.113883.3.7204.1.5.2.1, as defined in the Exchange Purposes SOP or an applicable Exchange Purpose Implementation SOP.
consent_policy	Optional	The Access Consent Policy Identifier corresponding to the asserted Access Policy that represents the identity proofing level of assurance of the user, array of string values from the subset of valid policy OIDs in QTF-108 that represent identity proofing levels of assurance, each expressed as a URI, e.g. ["urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.2.1"]
consent_reference	Optional	An array of FHIR Document Reference or Consent resources where the supporting access consent documentation can be retrieved, each expressed as an absolute URL, e.g. ["https://tefca.example.com/fhir/R4/DocumentReference/consent-6461766570"]
id_token	Optional	Additional token as per the IAS Implementation SOP or other relevant SOP

1. A client application requesting a token for patient requests MUST include the TEFCA SMART Authorization Extension Object in its authorization code Request.
2. If the submitted id_token does not sufficiently match a person known to the responder or is invalid, or if the responder does not support Demographic Matched IAS for patient requests, then when it cannot authenticate the user using issued login credentials, it MUST return an invalid_grant error in Response to the token request.
3. When issuing an access token as a result of authenticating an Individual, the Responding Node's authorization server MUST include the FHIR Patient Resource ID of the authorized Patient in the SMART launch context of the access token response.

6.13. Scope Negotiation Requirements

FHIR Server scope negotiation MUST conform to following constraints:

1. The scopes_supported metadata MUST be present in the .well-known/smart-configuration or .well-known/udap object, as applicable, and MUST list all scopes supported including all supported wildcard scopes.
2. A client may only request a wildcard scope if wildcards are specified in the scopes_supported metadata list.
3. If a wildcard scope is specified and the server supports wildcards, the server SHOULD respond with either the wildcard or with an exploded list of scopes that the client has been granted.
4. If wildcard scopes are not supported, the server SHOULD respond with an “invalid scope”.
5. For OIDC or SMART on FHIR access scopes, servers SHOULD put "openid", "offline_access", "email", "fhirUser", etc. in their scopes_supported metadata if they are supported.
6. A server MAY respond with fewer scopes than requested if the application cannot have a scope specified in the registration request or the server does not recognize one or more of the requested scopes.
7. A server SHOULD only respond with “invalid scope” if the wildcard is requested and not supported, or if none of the requested scopes are supported.
8. An authorization server MAY respond with scopes that are not part of the requested set, if the application has been registered with the server with a different set than was requested at registration based on technical or policy guidelines at the responding organization.
9. The scope list as part of an access grant request MAY be the same as the list from registration or MAY be a subset.
10. A grant time request to the server MAY return a full or subset of the requested scopes.
11. An application SHOULD be able to receive a superset of the scopes requested if the server’s policies dictate that a request with a certain system or user/user role is granted specific scopes that are not part of the original request.
12. A server SHOULD only return “invalid scope” if none of the scopes requested are available and/or not part of the scopes requested during registration.

7 VERSION HISTORY

Version	Revision Date	Section #(s) of Update
Version 1.0	Released July 1, 2024	N/A