



ONC  
TEFCA  
RECOGNIZED  
COORDINATING  
ENTITY

# Standard Operating Procedure (SOP): Facilitated FHIR Implementation

Version 2.0 DRAFT

October 2025

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

Deleted: 1

## TABLE OF CONTENTS

|          |                                             |           |
|----------|---------------------------------------------|-----------|
| <b>1</b> | <b>Common Agreement References .....</b>    | <b>3</b>  |
| <b>2</b> | <b>SOP Definitions .....</b>                | <b>3</b>  |
| <b>3</b> | <b>Purpose .....</b>                        | <b>3</b>  |
| <b>4</b> | <b>Facilitated FHIR Query Scenario.....</b> | <b>4</b>  |
| 4.1.     | Actors.....                                 | 5         |
| 4.2.     | Assumptions .....                           | 5         |
| 4.3.     | Pre-conditions.....                         | 6         |
| <b>5</b> | <b>Use Case Steps .....</b>                 | <b>7</b>  |
| <b>6</b> | <b>Procedure.....</b>                       | <b>9</b>  |
| 6.1.     | Overarching Requirements.....               | 9         |
| 6.2.     | FHIR Security.....                          | 10        |
| 6.3.     | Exchange Partners .....                     | 10        |
| 6.4.     | Exchange Purposes .....                     | 11        |
| 6.5.     | General Requirements.....                   | 11        |
| 6.6.     | FHIR Endpoints & Endpoint Discovery .....   | 11        |
| 6.7.     | Patient Matching .....                      | 12        |
| 6.8.     | Provenance Use .....                        | 13        |
| 6.9.     | Error Responses.....                        | 14        |
| 6.10.    | Security.....                               | 14        |
| 6.11.    | Requirements for Use of HL7 SSRAA .....     | 14        |
| 6.12.    | Scope Negotiation Requirements.....         | 17        |
| <b>7</b> | <b>Version History.....</b>                 | <b>19</b> |

## 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<sup>1</sup> 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

<sup>1</sup> 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 TECA 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 TECA 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.

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)                                                                                                                                                      |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>Time Management</u> | <ul style="list-style-type: none"> <li>• <u>IHE Consistent Time (CT)</u></li> </ul>                                                                                                     |
| Secure Channel         | <ul style="list-style-type: none"> <li>• IETF TLS 1.2 w/ BCP-195<sup>2</sup> or</li> <li>• IETF TLS 1.3 w/ BCP-195</li> </ul>                                                           |
| Node Registration      | <ul style="list-style-type: none"> <li>• OAuth V2.0</li> <li>• HL7 <i>FAST UDAP</i> Security for Scalable Registration, Authentication, and Authorization V1.1.0<sup>3</sup></li> </ul> |
| User Authentication    | <ul style="list-style-type: none"> <li>• OAuth V2.0</li> <li>• HL7 <i>FAST UDAP</i> Security for Scalable Registration, Authentication, and Authorization V1.1.0</li> </ul>             |

**Deleted:** ; alternate flows may use manual registration and/or SMART on FHIR.

**Deleted:** .0

**Deleted:** 0.0  
SMART Application Launch Framework Implementation Guide Release ...

**Deleted:** .0  
SMART Backend Services: Authorization Guide

<sup>2</sup> 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>.

<sup>3</sup> <https://hl7.org/fhir/us/udap-security/STU1.1/>

| Query Functions                  | Specified Standard(s) / Profile(S)                                                                                                                                                                                                                                                                           |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authorization & Exchange Purpose | <ul style="list-style-type: none"> <li>OAuth V2.0</li> <li>HL7 FAST UDAP Security for Scalable Registration, Authentication, and Authorization V1.1.0</li> <li>SMART Application Launch Framework Implementation Guide Release 1.0.0: <a href="#">SMART App Launch: Scopes and Launch Context</a></li> </ul> |
| Query for Patients               | <ul style="list-style-type: none"> <li>IHE XCPD</li> <li>FHIR R4 V4.0.1</li> <li>HL7 FHIR US Core Implementation Guide <a href="#">V6.1.0</a> or higher</li> </ul>                                                                                                                                           |
| Information Query and Retrieve   | <ul style="list-style-type: none"> <li>FHIR R4 V4.0.1</li> <li>HL7 FHIR US Core Implementation Guide <a href="#">V6.1.0</a> or higher</li> <li>FHIR Implementation Guides as required by the Exchange Purposes (XP) SOP and XP Implementation SOPs, as applicable</li> </ul>                                 |
| Auditing                         | <ul style="list-style-type: none"> <li>IHE ATNA (QHINs; Content only)</li> <li>ASTM E2147-18 (Participant/Subparticipant; Content only)</li> </ul>                                                                                                                                                           |

Deleted: 0

Deleted: 1

Deleted: Backend Services: Authorization Guide

Deleted: V3

Deleted: 1

Deleted: V3

Deleted: 1

#### 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

- All Initiating and Responding Nodes agree on transport level details (specified for transactions between QHINs elsewhere in this document) that allow for the following:
  - System authentication and encrypted communications over a secure channel;
  - 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
  - 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.

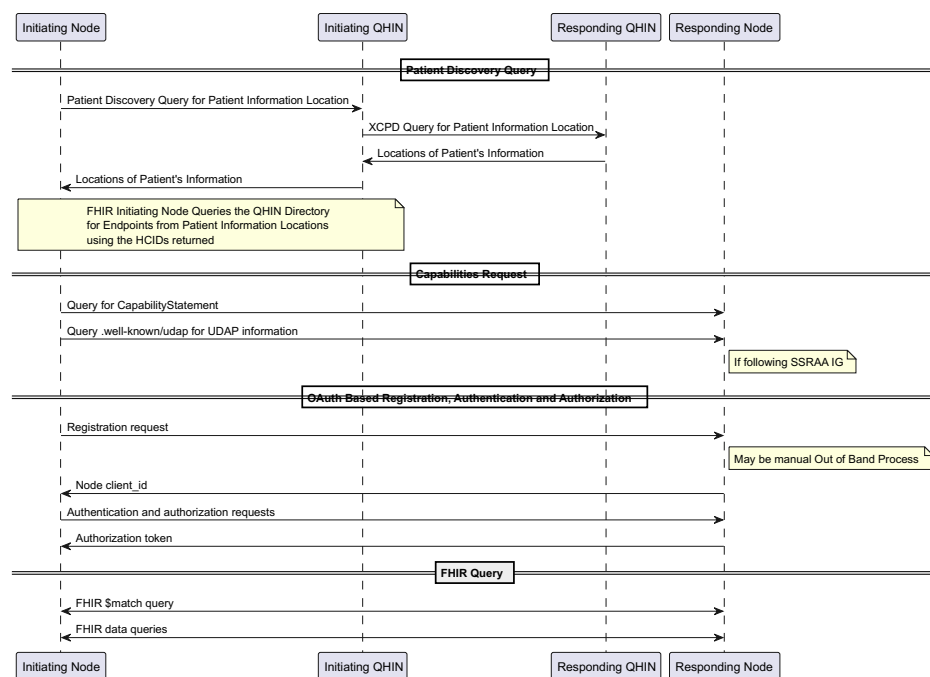
#### **4.3. Pre-conditions**

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



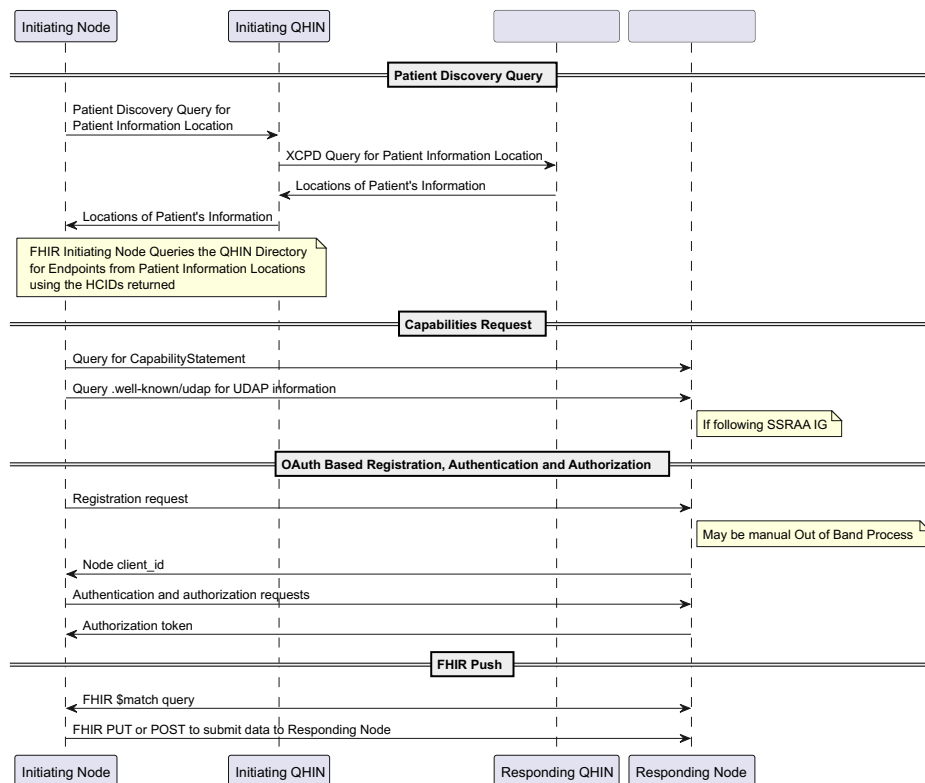
1. The Initiating Node sends a Patient Discovery Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to Query for patient information as per the QTF.
  - a. The Patient Discovery returns a list of HCIDs with relevant patient information.
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 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.

Deleted: UDAP



### 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 TECCA 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 TECCA certificate requirements as set out in the Technical Trust Requirements document.
  - a. All FHIR Adopters MUST indicate in their Directory Entry the supported registration and authentication/authorization standards used and the FHIR Endpoint to be used for TECCA FHIR exchange.
  - b. Each FHIR Responding Node SHALL publish UDAP Server Metadata at {baseUrl}/.well-known/udap for every {baseUrl} published as a FHIR Endpoint in the RCE Directory.
  - c. All JWTs used for completing UDAP flows according to the SSRAA IG SHALL be signed with a certificate corresponding to the TECCA Facilitated FHIR Technical Trust Requirements policy.
    - i. The x5c element of the JWT header SHALL contain the leaf certificate used to sign the request followed by the intermediate certificate which issued the leaf certificate.

## 6.2. FHIR Security

As of Q1 2027, all registration, authentication, and authorization of a FHIR client to a Responding Node MUST follow the requirements in HL7 SSRAA FHIR IG 1.1.0 – STU 1 US Sections 2, 3, 4, and 5. All FHIR Registrations SHALL use SSRAA dynamic registration for all clients. Specific milestones prior to this date include:

- Availability of testing systems for all production nodes by July 1, 2026
- All QHINs will have the capability to onboard and support SSRAA based authentication by November 1, 2026
- All new FHIR Nodes published to the production Directory after January 1, 2027 SHALL support SSRAA.

## 6.3. Exchange Partners

FHIR Adopters MAY determine their own exchange partners for purpose of testing for a limited time. FHIR Adopters will be responsible for coordinating directly with each other to identify which FHIR Adopters have (1) a compatible registration and authorization approach.

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

**Deleted:** as follows:

**Deleted:** ¶  
T

**Deleted:** <#>Indicate support for the HL7 SSRAA FHIR IG 1.0.0 STU 1 – US Dynamic Registration (True/False)¶  
Indicate support for one or more of: ¶  
HL7 SSRAA FHIR IG 1.0.0 – STU 1 US, Sections 4 and 5;¶  
SMART Backend Services or Application Launch Framework Implementation Guide Release (SMART) 1.0.0; and¶  
Some other authentication and authorization framework that adheres to the requirements of the QTF, based on out-of-band agreements between exchange partners.¶  
**FHIR Security Roadmap**¶  
Requirements surrounding the

**Deleted:** The

**Deleted:** these requirements:

**Deleted:** <#>Prior to January 1, 2026: ¶  
All FHIR Adopters MAY follow the requirements of HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Section 3 Registration. ¶  
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. ¶  
All FHIR adopters MUST use one of the following:¶  
HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Sections 4 and 5;¶  
SMART Release 1.0.0; or¶  
Some other authentication and authorization framework that adheres to the requirements of the QTF, based on out-of-band agreements between exchange partners.¶  
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.¶

**Deleted:** Prior to January 1, 2026,

**Deleted:** and (2) a compatible approach to patient discovery...

**Deleted:** to be

## 6.4. Exchange Purposes

1. All transactions using HL7 FAST SSRAA Sections 4 and 5 Authentication and Authorization MUST use codes from 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, within the appropriate JWT and/or extension(s).
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.

Deleted: ,

Deleted: .

## 6.5. General Requirements

1. FHIR Adopters MUST share all patient data via US Core V6.1.0 requirements conformant resources, where such data exists and is available, consistent with applicable law. Adopters MAY make available resources conforming to versions higher than 6.1.0 or resources not included in US Core.
  - a. All Responding Nodes with FHIR Capabilities listed in the RCE Directory Service MUST provide access to the Patient Resource and at least one additional US Core profiled patient compartment<sup>4</sup> FHIR Resource.
  - b. In addition, all Responding Nodes MUST provide a CapabilityStatement resource and MUST use the FHIR CapabilityStatement resource to define FHIR server capabilities.
2. Any FHIR Implementation Guides MAY be used within the network as desired.

Deleted: make available

Deleted: V3

Deleted: 1 or higher Resources

Deleted: .

Deleted: The following

## 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 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 FHIR-capable Responding Nodes MUST provide at least one publicly discoverable CapabilityStatement where CapabilityStatement.kind="instance".
3. 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.

Deleted: SHOULD

Deleted: supported:

**Deleted:** <#>Bulk Data Access IG V1.0.1,<sup>¶</sup>  
 Mobile access to Health Documents (MHD) V4.2.1,<sup>¶</sup>  
 ITI-67 and ITI-68 transactions SHOULD be supported, all  
 other transactions MAY be supported.<sup>¶</sup>  
 HL7 Da Vinci Clinical Data Exchange FHIR  
 Implementation Guide Version 2.0.0,<sup>5¶</sup>  
 HL7 Da Vinci Payer Data Exchange FHIR  
 Implementation Guide Version 1.0.0,<sup>5</sup> and<sup>¶</sup>  
 Any other FHIR IG included in an XP Implementation  
 SOP.<sup>¶</sup>

**Deleted:** <#>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<sup>7</sup> FHIR Resource.<sup>¶</sup>  
 All Responding Nodes MUST provide a  
 CapabilityStatement resource.<sup>¶</sup>  
 Responding Nodes MUST use the FHIR  
 CapabilityStatement resource to define FHIR server  
 capabilities.<sup>¶</sup>

<sup>4</sup> See <https://www.hl7.org/fhir/r4/compartментdefinition-patient.html> for a complete definition

4. Capabilities listed within the CapabilityStatement MUST include all FHIR Implementation Guide operations supported by the Responding Node.
5. 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. 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@<sup>8</sup> Technical Specification. However, if the field does not contain a street address but contains other geographical

---

<sup>8</sup> Project US@ Technical Specification. – available at <https://oncprojectracking.healthit.gov/wiki/pages/viewpage.action?pagelid=180486153>

details, it is recommended that whatever information the patient provided not be abbreviated.

11. Demographics used in all [\\$match](#) 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 [document-based](#) interoperability standard.
  - a. [Information transformed from non-document-based standards MAY make a Provenance resource available](#)
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 [guidance provided in the FHIR R4 Provenance Resource section 6.3.4.5 Use of Provenance to record Import and Transform](#).
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.
  - a. Provenance.agent.type MUST contain code "assembler" from the code system <http://hl7.org/fhir/ValueSet/provenance-agent-type>.
  - b. 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.
6. Provenance.entity MUST contain one element [1..1] describing the source document [or other source](#) from which the information was extracted.
7. Provenance.entity.role MUST be the code "source" from the <http://hl7.org/fhir/provenance-entity-role> code system.
8. Provenance.entity.what MUST be a reference to the DocumentReference Resource pointing to the original document [or other source](#).

Deleted: FHIR Core



## 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<sup>9</sup> to further enable interoperability without reducing the security of transactions.

1. Registration, Authorization and Authentication for FHIR exchange **MUST** follow the requirements specified in [section 0](#),
2. Authorization Servers SHOULD issue access tokens with a lifetime no longer than 60 minutes.
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.

Deleted: SHOULD

Deleted: sections

Deleted: and 6.12

## 6.11. Requirements for Use of HL7 SSRAA

### Discovery

1. [The metadata endpoint MUST include the community parameter with the URI: urn:oid:2.16.840.1.113883.3.7204.1.5](#)
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 for all TECCA registrations.](#)

### Registration

4. [FHIR Initiating Nodes that initiate for multiple exchange purposes MUST register multiple client applications, one for each exchange purpose, to allow FHIR Responding Nodes'](#)

<sup>9</sup> <https://oauth.net/2/>



Authorization Servers to provision them with the correct authorization policies for the given exchange purpose.

5. All client applications MUST register with an iss value corresponding to one of the client Subject Alternative Name URIs present in its Facilitated FHIR Certificate.

- a. The SAN MUST correspond to the exchange purpose for which the client application will conduct exchange.

6. The basic-app-certification JWT MUST contain:

|                          |                                                                               |
|--------------------------|-------------------------------------------------------------------------------|
| <u>exchange_purposes</u> | <u>An array of one Exchange Purpose from the TEFCA Exchange Purposes SOP.</u> |
|--------------------------|-------------------------------------------------------------------------------|

7. 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.
8. 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.
9. Any retired client\_ids MUST be preserved by the Authorization Server so that it can be associated with log entries and the Initiating Node.
10. If the client attempts to register for either a Client Credentials Grant or an Authorization 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 authentication JWT 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    | <u>RCE Directory Service entry Organization Resource id at the most granular level (e.g., lowest level Subparticipant or child) formatted as a relative URI to the RCE Directory base URL (e.g., 'Organization/1.2.3').</u> |
| 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    | <u>A length 1</u> 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                                               |

**Deleted:** <#>The udap\_certifications\_supported metadata returned MUST include <https://rce.sequoiaproject.org/udap/profiles/basic-app-certification>.¶  
The udap\_certifications\_required metadata returned MUST include <https://rce.sequoiaproject.org/udap/profiles/basic-app-certification>.¶  
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”.¶  
The software statement MUST contain a certification\_name element of “TEFCA Basic App Certification”.¶  
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>¶

**Deleted:** Authentication

**Deleted:** software statement

**Deleted:** String containing the URL of Initiating Node's

**Deleted:** resource in

**Deleted:** service

**Deleted:** An



- 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 TEFCAspecific error extension as specified in Table 3 TEFCAs Authorization Extension Error Object. in the 'extensions' object of the error Response.

TABLE 1. TEFCAs 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 each expressed as a URI. |
| consent_form              | optional    | A URL as a string where the required consent form may be downloaded, if applicable.                                                                                                                                      |

Deleted: in Appendix A of this IG,

- 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<sup>10</sup> or Consent<sup>11</sup> Resource included in the consent\_reference array.

#### Individual Access Services (IAS) Queries

- Responders MUST support the Authorization Code Grant type for IAS Queries.
- The responder MUST support the TEFCAs IAS Authorization Extension Object identified by the extension key "tefca\_ias" as defined in Table 4 TEFCAs IAS Authorization Extension Object.
- A client application requesting a token for patient requests using Client Credentials Grant MUST include the TEFCAs IAS Authorization Extension Object in its token request in addition to the hl7-b2b Authorization Extension object during the authorization flow.

Deleted: &lt;#&gt;The Initiating Node MUST provide the tefca\_ias extension during the Authorization flow.¶

TABLE 4. TEFCAs IAS AUTHORIZATION EXTENSION OBJECT

| Extension Name: "tefca_ias" |             |                                                                                                                                                 |
|-----------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Element                     | Optionality | Requirement                                                                                                                                     |
| version                     | Required    | Fixed string value: "1"                                                                                                                         |
| 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" |

Deleted: purpose\_of\_use

<sup>10</sup> See <https://hl7.org/fhir/R4/documentreference.html>

<sup>11</sup> See <https://hl7.org/fhir/R4/consent.html>



| Extension Name: "tefca_ias" |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Element                     | Optionality | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| patient_information         | Required    | FHIR US Core Patient Resource with all known demographics                                                                                                                                                                                                                                                                                                                                                                                                             |
| id_token                    | Required    | OIDC token <u>representing the user's information</u> provided by Identity Verifier when the Identity Verifier is not the Responding Node. Responding server <u>SHOULD</u> respond with invalid_grant if missing.                                                                                                                                                                                                                                                     |
| consent_policy              | Conditional | <u>If user is not the patient, this element represents the</u> 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 <b>Error!</b> <b>Reference source not found.</b> that represent identity proofing levels of assurance, each expressed as a URL, e.g. ["urn:oid: 2.16.840.1.113883.3.7204.1.1.1.2.1"] |
| 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"]                                                                                                                                                                                                                       |

- 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.
- 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. Scope Negotiation Requirements

FHIR Server scope negotiation MUST conform to following constraints:

- The scopes\_supported metadata SHALL be present in the .well-known/udap object, and SHALL list all supported wildcard scopes.
- Client applications and servers MAY support wildcard scopes.
- A client application MAY request a wildcard scope only if wildcards are specified in the server's scopes\_supported metadata list.
- If a client application requests a wildcard scope and the server supports wildcards, then the server SHOULD return either the wildcard scope or an expanded set of scopes that the client has been granted in its response.

Deleted: and validated

Moved down [1]: Conditional

Deleted: ial\_vetted

Deleted: MAY

Moved (insertion) [1]

Deleted: Required

Deleted: The

Deleted: Id\_token

... [2]

**Deleted: <#>Requirements for Use of SMART Backend Services or App Launch Implementation Guide**

The SMART capabilities MUST include "launch-standalone", "client-public", "context-standalone-patient", "permission-patient", and "permission-user".  
The SMART grant\_types\_supported MUST include "authorization\_code".

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 5. TEFCA CLIENT REGISTRATION INFORMATION**

**Element**

The SMART capabilities MUST include "launch-standalone", "client-public", "context-standalone-patient", "permission-patient", and "permission-user".  
The SMART grant\_types\_supported MUST include "authorization\_code".

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 5. TEFCA CLIENT REGISTRATION INFORMATION**

**Element**

... [3]

Deleted: MUST

Deleted: smart-configuration or .well-known/

Deleted: , as applicable,

Deleted: MUST

Deleted: scopes supported including all

Deleted: may only

Deleted: is specified

Deleted: respond with

Deleted: with

Deleted: exploded list

5. If a client application requests a wildcard scope and the server does not support wildcard scopes, then the server **SHOULD** respond with an error of "invalid\_scope" or "invalid\_client\_metadata", as appropriate.
6. If a server supports OIDC or SMART App Launch scopes, the server **SHOULD** put the corresponding scopes (e.g. "openid", "offline\_access", "email", "fhirUser", etc.) in their scopes\_supported metadata.
7. A server **MAY** grant fewer scopes than requested by the client application if the client application cannot have a scope specified in the request based on technical or policy guidelines at the responding organization or if the server does not recognize one or more of the requested scopes.
8. A server **SHOULD** respond with "invalid\_scope" or "invalid\_client\_metadata", as appropriate, only if a wildcard scope is requested and not supported, or if none of the requested scopes are supported.
9. At the time of a token request, an authorization server **MAY** grant additional scopes that are not in the set of scopes requested by the client application if the application has been registered with the server with a different set of scopes than was requested at registration based on technical or policy guidelines at the responding organization.
10. Scopes granted by a server to a client application at the time of an access token request may be the same as the set from registration or be a subset.
11. Scopes granted by a server to a client application at the time of an access token request may be the same as the set of scopes requested by the client application or be a subset.
12. 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.
13. A server **SHOULD** return "invalid\_scope" or "invalid\_client\_metadata", as appropriate, only if none of the scopes requested are available and/or not part of the scopes requested during registration.
14. A server **SHALL** include the scope parameter in a token response if the set of scopes granted by the server to the client application is not identical to the set of scopes requested by the client application, or if the client application does not include a set of requested scopes in its request.

Deleted: are not supported,

Deleted: scope".

Deleted: For

Deleted: on FHIR access

Deleted: servers

Deleted: "

Deleted: ", "

Deleted: ", "

Deleted: ", "

Deleted: ,

Deleted: .

Deleted: if they are supported.

Deleted: respond with

Deleted: registration

Deleted:

Deleted: respond with "invalid scope"

Deleted: the

Deleted:

Deleted: An

Deleted: respond with

Deleted: part

Deleted: the

Deleted: set,

Deleted: The scope list as part

Deleted: grant

Deleted: MAY

Deleted: list

Deleted: MAY

Deleted: A grant

Deleted: to the server MAY return a full or subset of

Deleted: scopes.

Deleted: only

Deleted:



## 7 VERSION HISTORY

| Version                           | Revision Date         | Section #(s) of Update |
|-----------------------------------|-----------------------|------------------------|
| Version 1.0                       | Released July 1, 2024 | N/A                    |
| Draft <a href="#">Version 2.0</a> | October 2025          | Sections 4, 5, and 6   |

