Trusted Exchange Framework and Common Agreement

Qualified Health Information Network (QHIN) Technical Framework (QTF)

DRAFT Version 2.0

Draft for Stakeholder Feedback

TABLE OF CONTENTS

OVERVIEW

The 21st Century Cures Act, signed by President Obama in 2016, calls on the U.S. Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) to "develop or support a trusted exchange framework, including a common agreement among health information networks nationally." Starting in 2019, ONC established a relationship with The Sequoia Project to serve as the Trusted Exchange Framework and Common Agreement℠ (TEFCA℠) Recognized Coordinating Entity® (RCE™) to administer a network-of-networks enabled by the Common Agreement called for in the Cures Act.

The Qualified Health Information Network™ (QHIN™) Technical Framework (QTF), developed by the RCE, describes the functional and technical requirements that a Health Information Network (HIN) must fulfill to serve as a QHIN under the Common Agreement. The QTF specifies the technical underpinnings for TEFCA Exchange, QHIN technical capabilities and services, and certain other responsibilities described in the Common Agreement. The QTF is intended to be consistent with the Common Agreement, and the Common Agreement terms shall control.

The QTF focuses primarily on the technical and functional interoperability requirements QHINs must support, including specification of the standards that QHINs must implement to enable TEFCA Exchange of health information.

QTF Version 2.0 Scope

The technical and functional requirements described in this version of the QTF focuses on three information exchange modalities for QHINs:

- QHIN Query
- QHIN Message Delivery
- Facilitated FHIR

The QTF also describes high-level functional requirements QHINs must support for exchange within their health information networks. So long as QHINs are able to achieve the required functional outcomes within their networks, they generally have the operational flexibility to select appropriate standards and approaches consistent with the needs of their business environments. In limited instances, the QTF may specify a particular element of Participant or Subparticipant behavior in order to ensure consistency in QHIN-to-QHIN behavior.

This version of the QTF adds requirements for Facilitated FHIR exchange between QHINs, Participants, and Subparticipants including the use of the FHIR Provenance resource to track data transformation to and from FHIR resources and the HL7® *FAST* UDAP Security Implementation Guide. The QHIN-Facilitated Exchange model provides the opportunity for QHINs to make available selected network services to enhance Participants' and Subparticipants' use of FHIR APIs among themselves.

The technical and functional requirements described in the QTF reflect many of the technologies and standards used for network-based health information exchange today. For example, organizations supporting health information exchange nationally (e.g., CommonWell Health Alliance, eHealth Exchange, Carequality) generally use Integrating the Healthcare Enterprise (IHE) profiles such as Cross-Community Patient Discovery (XCPD)[1] and Cross-Community Access (XCA)[2] to enable clinical document exchange between disparate communities. In addition, the QTF acknowledges that patient matching algorithms vary today; there will be work with QHINs to develop matching recommendations and/or requirements in the future. Additionally, the QTF includes requirements for Participants and Subparticipants to engage in Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) API-based exchange.

The scope of data for TEFCA exchange is TEFCA Information as defined by the Common Agreement and maintained by QHINs, Participants, or Subparticipants. The United States Core Data for Interoperability (USCDI) is a named data standard in the QTF, but it is neither a "floor" nor a "ceiling" for data exchange. TEFCA Information maintained by QHINs, Participants, and Subparticipants could be more or less than the data in the version of USCDI specified in the QTF. There is no minimum requirement for QHINs, Participants, or Subparticipants to maintain all the data elements in the version of USCDI specified in the QTF. However, the USCDI provides conformance requirements when exchanged in TEFCA. When TEFCA Exchange occurs for the data in the USCDI version specified in the QTF, then the data needs to conform to the requirements specified in the USCDI. This could be done by the Participants, or Subparticipants, or by the Responding QHIN depending on the internal configuration and policies of each QHIN.

Definitions

Capitalized terms are used throughout the QTF. Many such terms are defined in the Common Agreement and are not duplicated in this list. Terms specific to the QTF are defined here:

- **Access Consent Policy (ACP)**: Policies that may influence access control decisions and which can be referenced in queries.
- **Actor**: A QHIN, Participant, or Subparticipant.
- **Assigning Authority**: The organization that issues a patient identifier.
- **Enterprise Master Patient Index (eMPI)**: A system that coordinates patient identification across multiple systems by collecting, storing, and managing identifiers and patient-identifying demographic information from a source system.

[1] IHE Cross-Community Patient Discovery (XCPD) profile in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

[2] IHE Cross-Community Access (XCA) profile in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

- **Exchange Modality:** QHIN Query, QHIN Message Delivery, and/or Facilitated FHIR
- **FHIR Push:** A PUT or POST operation that submits data to a QHIN, Participant, Subparticipant, or other Node.
- **FHIR Query**: A query operation that Requests information from a Responding Node
- **HomeCommunityID (HCID)**: A globally unique identifier for a Node.
- **Initiating QHIN**: A QHIN that initiates a QHIN Query or QHIN Message Delivery.
- **Instance Access Consent Policy (IACP)**: Policy instances (e.g., patient authorization forms) which may influence access control decisions, and which can be referenced by queries.
- **Message Delivery Solicitation**: A Request for a QHIN to initiate a QHIN Message Delivery.
- **QHIN Directory:** A system used by QHINs to record and resolve the identifiers and endpoints of members of their network (i.e., Participants and Subparticipants). The QHIN Directory includes a local copy of the RCE Directory.
- **QHIN Message Delivery:** The act of a QHIN delivering information to one or more other QHINs (i.e., TEFCA Exchange) for delivery to one or more Participants, Subparticipants, or Individuals. (Sometimes referred to as a "push").
- **QHIN Query:** The act of a QHIN Requesting information from one or more other QHINs (Sometimes referred to as a "pull").
- **Query Solicitation:** A Request for a QHIN to initiate a QHIN Query.
- **RCE Directory:** The individual organization entries that form the content of the RCE Directory Service.
- **Record Locator Service (RLS)**: A service that provides authorized users the location of records based on criteria such as a patient ID and/or record data type, as well as providing functionality for the ongoing maintenance of health record location information.
- **Responding QHIN**: A QHIN that receives (and responds to as appropriate) a QHIN Query or QHIN Message Delivery from an Initiating QHIN.
- **Uniform Resource Identifier (URI)**: A set of characters that identifies a specific logical or physical resource used by Internet related computer programs.

The following actor names are specific to IHE profiles and used within the QTF with the following definitions, for full definitions please see IHE Technical Frameworks General Introduction, Appendix A: IHE Actor Definitions.[3]

- **Initiating Gateway**: A transaction gateway that supports outgoing Requests and Responses for QHIN Query (Patient Discovery, Document Query, Document Retrieve) and QHIN Message Delivery.

[3] *IHE Technical Frameworks General Introduction, Appendix A* available at https://profiles.ihe.net/GeneralIntro/ch-A.html

- **Responding Gateway:** A transaction gateway that supports incoming Requests and Responses for QHIN Query (Patient Discovery, Document Query, Document Retrieve) and QHIN Message Delivery.

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF BCP 14.[4]

QHIN Exchange Scenarios

The following QHIN exchange scenarios present basic workflows for the supported exchange modalities. Each scenario depicts a real-world use case that stakeholders might encounter. The scenarios do not represent all possible workflows or use cases. Rather, they generally describe the various functions performed to enable QHIN-to-QHIN information exchange.

Document Query Scenario

In this scenario, a health care provider sees a new patient and seeks to find the patient's health information among the QHINs to inform diagnosis and treatment. This scenario assumes basic patient demographic information is available to the provider.

The health care provider is a participant in a health information network (e.g., state/local Health Information Exchange (HIE), vendor- or payer-based network, etc.), which is a Participant of a QHIN. To find health information about the patient, the provider first submits a Query Solicitation to the local network, which is routed to the QHIN over a secure channel. The Query Solicitation may include patient demographic information for patient identity resolution, query parameters indicating which information the provider is looking for, and/or a list of entities to query. The local network also transmits information about the provider's identity, as well as an Exchange Purpose specified by the provider (i.e., "Treatment" in this scenario).

The QHIN processes the Query Solicitation and uses the information to initiate a QHIN Query to any appropriate Responding QHINs. If the provider specified a target for the query, the Initiating QHIN checks its QHIN Directory to identify the appropriate Responding QHINs. Otherwise, the Initiating QHIN will initiate a QHIN Query with all other QHINs.

The Initiating QHIN connects to each Responding QHIN using the Internet Engineering Task Force (IETF) Transport Layer Security (TLS) protocol[5] to establish a secure channel for the QHIN Query transaction; each QHIN authenticates the other QHIN (i.e., mutual authentication). After

[4] *Key words for use in RFCs to Indicate Requirement Levels* and *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words* (IETF BCP 14) available at https://www.rfc-editor.org/info/bcp14.
[5] *The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) available at https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446.

establishing a secure channel, the Initiating QHIN sends each Responding QHIN a Security Assertion Markup Language (SAML)[6] assertion conforming to the IHE Cross-Enterprise User Assertion (XUA) profile along with the query transaction.[7] The SAML assertion preserves information from the Query Solicitation about the Initiating Node and the Exchange Purpose but is assembled by the QHIN and signed by the QHIN's digital certificate.

A QHIN Query typically involves two major workflows, patient discovery via IHE XCPD and document query (including location and retrieval) via IHE XCA. In the patient discovery workflow, the Initiating QHIN shares patient demographic information via an XCPD Request with the Responding QHIN(s). Each Responding QHIN uses the demographic information to resolve the patient's identity (i.e., "patient matching"), and returns an XCPD Response with the resolved identity, including a local patient identifier, demographic information about the patient, and other details.

In the document query workflow, the Initiating QHIN sends an XCA Request including a patient identifier (e.g., information obtained via the Patient Discovery workflow) and query parameters to the Responding QHIN(s) to discover whether clinical documents are available. Each Responding QHIN uses the query parameters and patient identity to discover clinical documents that meet the query criteria within their own network and sends an XCA Response with a list of document identifiers to the Initiating QHIN. The list of document identifiers is routed through the local network to the provider, who reviews the Response and selects the relevant documents for retrieval. The Initiating QHIN then Requests the relevant documents, which are retrieved and shared with the Initiating QHIN by the Responding QHIN(s).

After retrieving the relevant documents, the Initiating QHIN routes them back through the local network to the provider. Each QHIN involved in the query maintains audit logs of all activities and transactions the QHIN performed in the process of resolving the query, according to the IHE Audit Trail and Node Authentication (ATNA) profile.[8]

[6] *Security Assertion Markup Language* (SAML) available at https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[7] *IHE Cross-Enterprise User Assertion (XUA) profile* in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf.

[8] *IHE Audit Trail and Node Authentication (ATNA) profile* in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf.

Specified standards for a QHIN Query are included in *Table 1*.

Table 1. Specified Standards for QHIN Query

Query Functions	Specified Standard(s) / Profile(s)
Secure Channel	• IETF TLS 1.2 w/ BCP-195[9] or • IETF TLS 1.3 w/ BCP-195
Mutual Authentication	• IETF TLS w/ BCP-195
User Authentication	• IHE XUA
Authorization & Exchange Purpose	• IHE XUA
Query for Patients	• IHE XCPD
Document Query and Retrieve	• IHE XCA
Auditing	• IHE ATNA (Content only)

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.

Actors/Services	Cardinality	System Actor
Initiating Node	1..1	Any initiating Actor
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 Actor

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 Request such as who is sending, what their role is, and what their Exchange Purpose is.
   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 does not know both the patient identifier(s) and Responding Node(s) for a query.
   a) If the Patient Identifier(s) and Responding Node(s) are known, the patient discovery phase of the query workflow may be omitted.

[9] *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.

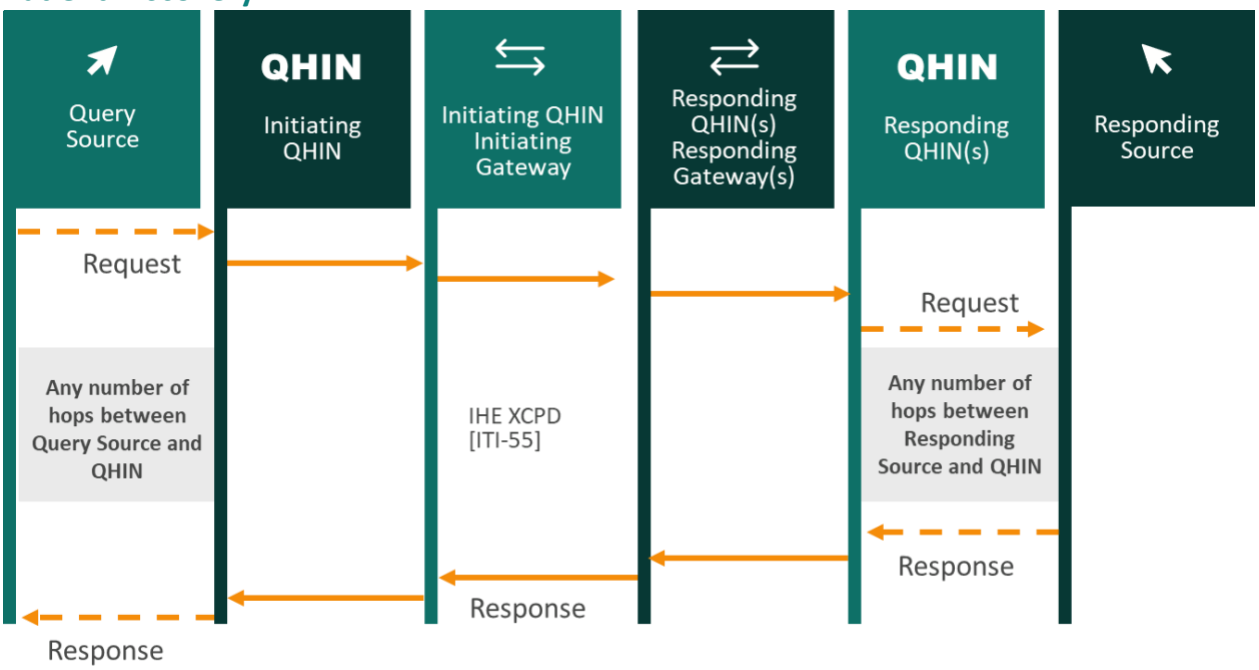
Pre-conditions

The following workflow assumes the following conditions:

- The Initiating Node knows sufficient patient demographics for a successful match as determined by the Responding Node.
- 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.
- The RCE Directory includes the organization facility name(s), and HomeCommunityID(s) for all current Participants and Subparticipants. Each Participant and Subparticipant is matched to the appropriate QHIN.
- Each QHIN maintains an up-to-date copy of the RCE Directory.
- Responding QHINs know the current HomeCommunityIDs for any Responding Nodes.
- 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[10].

Use Case Steps

Patient Discovery



[10] *QHIN Service Level Requirements Policy,* when available, to be located at https://rce.sequoiaproject.org/tefca-and-rce-resources

Nominal Flow (QHIN maintains an eMPI or RLS)

1) The Initiating Node sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to discover patient matches by demographics.
    a) The Query Solicitation includes all available patient demographics.
2) The Initiating QHIN creates an IHE Cross Gateway Patient Discovery [ITI-55] Request based on the Query Solicitation and sends it via the Initiating Gateway to the Responding Gateways of all Responding QHINs. See *IHE ITI TF-2b: 3.55*.
    a) The Initiating QHIN creates an audit log entry including the HCID of the Initiating Node and Responding QHIN(s).
3) Each Responding QHIN compares the demographics to its known patients, applying its own algorithm(s) to determine potential matches, and returns an IHE Cross Gateway Patient Discovery [ITI-55] Response to the Initiating QHIN's Initiating Gateway.
    a) The IHE Cross Gateway Patient Discovery [ITI-55] Response contains one or more patient matches from all potential Responding Nodes, including demographics and patient ID as known by the Responding Node. The Response may contain multiple entries where each entry reflects a different source of information but will include only one identifier per patient per Responding Node.
    b) The Responding QHIN creates an audit log entry including the HCID of the Initiating QHIN and Initiating Node.
4) The Initiating QHIN returns the Response(s) to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable).
    a) The Initiating QHIN creates an audit log entry including the HCID of the Initiating Node, and Responding QHIN(s), and patient identifiers.
    b) Note: Any QHINs participating in the transaction should include any errors in its audit log. QHINs should not include the contents of successful Responses in their audit logs but should include the XCPD query.

Alternate Flow 1: Querying Specific Organization(s)

The following flow may be used when the Initiating Node only wants to query one or more specific organizations:

1) The Initiating Node sends a Query Solicitation, through any intermediary Subparticipants or Participant as applicable, to the Initiating QHIN to find patient matches by demographics from specific organizations where a patient may have health care data.
    a) The Query Solicitation includes all available patient demographics as well as the HomeCommunityID(s) and/or other information about the target Responding Node(s) (e.g., organization name, city, and state). See *IHE ITI TF-1: 27 XCPD Integration Profile* and *IHE ITI TF-2b: 3.55*.
2) The Initiating QHIN queries its QHIN Directory to identify the appropriate Responding QHIN for each Responding Node provided by the Initiating Node.
3) Nominal Flow resumes at Step 2.

Alternate Flow 2: Initiating Node asserts an Instance Access Consent Policy or Access Consent Policy

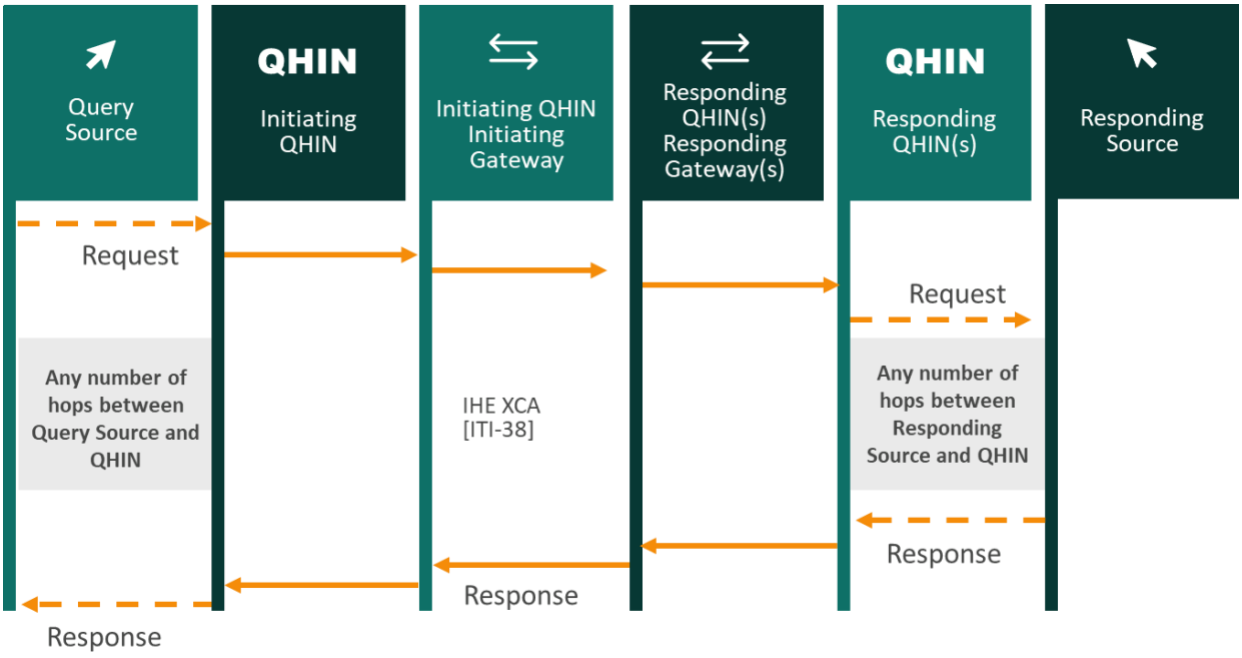
1) The Initiating Node includes the Uniform Resource Identifier (URI)(s) of one or more Access Consent Policies (ACPs) or Instance Access Consent Policies (IACP) in its Query Solicitation.
   a) An ACP may have an associated instance (IACP, e.g., a signed patient permission form) for a specific patient.
2) Each Responding Node obtains the (I)ACP per the Document Retrieve Workflow.
   a) A Responding Node may incorporate retrieved (I)ACPs into access control decisions made with respect to releasing information in Response to a query.
   b) If a Responding Node is unable to obtain the (I)ACP document or is unable to process a retrieved (I)ACP document and would not be able to disclose patient information without a valid (I)ACP, an error Response is returned. The flow ends for this Responding Node and the use case continues.
3) Nominal Flow resumes at Step 3.

Alternate Flow 3: QHIN does not maintain an eMPI or RLS

1) Workflow beings in step 3.
2) The Responding QHIN queries its Participants, based on its chosen method that meets Service Level Agreement(s) (SLAs), to discover patient matches using the patient demographics and returns an IHE Cross Gateway Patient Discovery [ITI-55] Response to the Initiating QHIN's Initiating Gateway.
   a) The Response contains one or more patient matches from all potential Responding Nodes, including demographics and patient ID as known by each Responding Node. The Response must also include the Responding Participant's HomeCommunityID and Assigning Authority, or the HomeCommunityID and Assigning Authority of any Subparticipants where a match was found. The Response may contain multiple entries, where each entry reflects a different source of information, but should not contain multiple patient identifiers for a match at a single Responding Node.

Document Query

Nominal Flow



1) The Initiating Node sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to query for document metadata.
   a) The Query Solicitation includes one or more patient identifiers and an Assigning Authority and HCID for each desired Responding Node.
   b) The Initiating QHIN queries its QHIN Directory to identify the appropriate Responding QHIN(s) for each HCID included in the Query Solicitation.
2) The Initiating QHIN creates an IHE Cross Gateway Query [ITI-38] FindDocuments Request based on the Query Solicitation and sends it via the Initiating Gateway to each Responding QHIN's Responding Gateway.
   a) The Initiating QHIN creates an audit log entry including the HCID and Assigning Authority of the Initiating Node and Responding QHIN(s).
3) Each Responding QHIN queries its QHIN Directory to identify the appropriate Responding Node(s) and sends a Request for document metadata, through any intermediary Participant or Subparticipants, as applicable, to each Responding Node.
   a) The Responding QHIN's Request includes the patient identifier as known by the Responding Node and may include some number of query parameters.
   b) The Responding QHIN creates an audit log entry including the HCID and Assigning Authority of the Initiating Node, Initiating QHIN, and Responding Node(s).
4) Each Responding Node returns a Response with document metadata and/or FHIR endpoint(s) based on any query parameters and/or local access control policies.

5) Each Responding QHIN combines the Responses from the Responding Node(s) and returns a single IHE Cross Gateway Query [ITI-38] FindDocuments Response to the Initiating QHIN's Initiating Gateway.
   a) The Responding QHIN creates an audit log entry including the HCID and Assigning Authority of the Responding Node(s), Initiating QHIN, and Initiating Node.
6) The Initiating QHIN returns the Response(s) to the Initiating Node, through any intermediary Participant or Subparticipants, as applicable.
   a) The Initiating QHIN creates an audit log entry identifying the Responding Node(s) and Initiating Node.

Alternate Flow 1: Query Returns Partial Success

1) This workflow begins at Step 4 of the Nominal Flow.
2) A Responding Node returns an error message (e.g., no document is found).
3) The Responding QHIN combines the Responses from the Responding Node(s) and returns a single IHE Cross Gateway Query [ITI-38] FindDocuments Response to the Initiating QHIN's Initiating Gateway.
   a) If the Responding QHIN is able to return some but not all available document entries, the Response includes all available DocumentEntry elements and/or FHIR endpoints, the status urn:ihe:iti:2007:ResponseStatusType:PartialSuccess, and some number of RegistryError elements.
4) The Initiating QHIN chooses to execute one of the following subflows:
   a) Subflow 1: If the Initiating Node is unable to process a Partial Success Response, the Initiating QHIN returns the Response to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable) as a Success. The Response does not indicate there were errors.
   b) Subflow 2: The Initiating QHIN returns the Response to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable), along with information about any errors.

Alternate Flow 2: Initiating Node asserts an Instance Access Consent Policy or Access Consent Policy

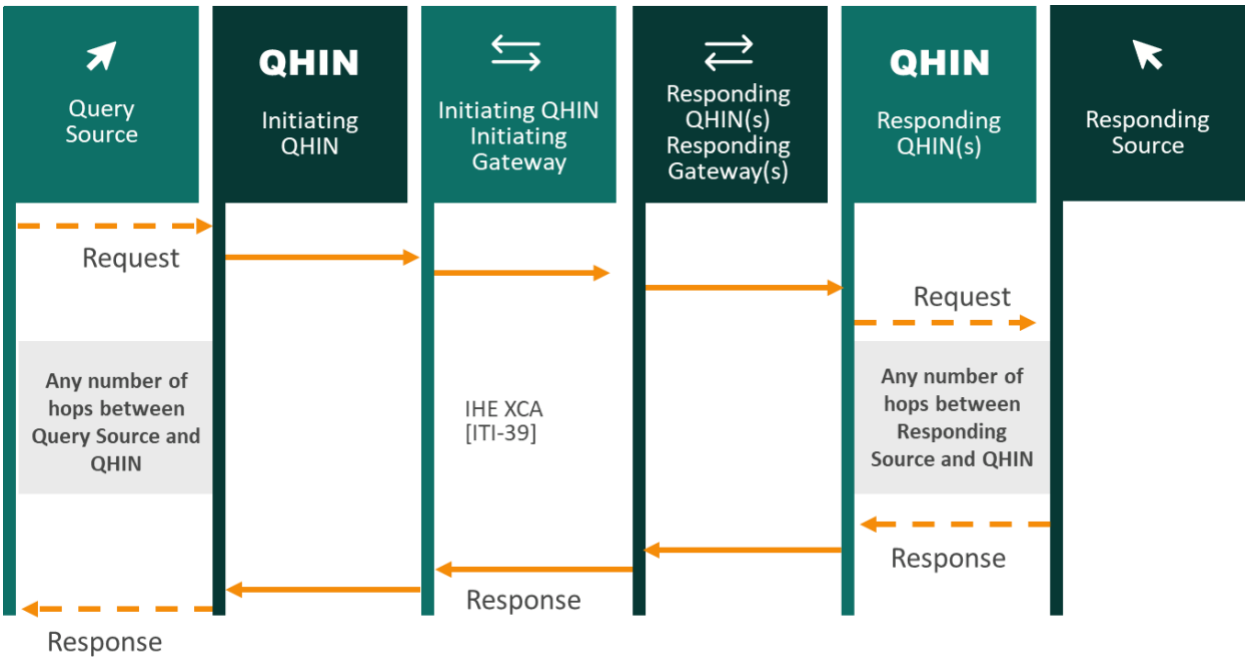
1) The Initiating Node includes the URI(s) of one or more Access Consent Policies (ACPs) or Instance Access Consent Policies (IACP) in its Query Solicitation.
   a) An ACP may have an associated instance (IACP, e.g., a signed patient consent form) for a specific patient.
2) Each Responding Node obtains the (I)ACP per the Document Retrieve Workflow.
   a) A Responding Node may incorporate retrieved (I)ACPs into access control decisions made with respect to releasing information in Response to a query.

b) If a Responding Node is unable to obtain the (I)ACP document or is unable to process a retrieved (I)ACP document, and would not be able to disclose patient information without a valid (I)ACP, an error Response is returned. The flow ends for this Responding Node and the use case continues.

3) Nominal Flow resumes at Step 4.

Document Retrieve

Nominal Flow



1) The Initiating Node sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to retrieve documents.
   a) The Query Solicitation includes the HomeCommunityID(s), Repository ID(s) if known, and Document IDs at the Responding Node(s).
   b) The Initiating QHIN queries its QHIN Directory to identify the appropriate Responding QHIN(s) for each HCID included in the Query Solicitation.
2) The Initiating QHIN creates an IHE Cross Gateway Retrieve [ITI-39] Request based on the Query Solicitation and sends it via the Initiating Gateway to each Responding QHIN's Responding Gateway.
   a) The Initiating QHIN creates an audit log entry including the HCID of the Initiating Node and Responding QHIN(s).
3) Each Responding QHIN queries its QHIN Directory to identify the appropriate Responding Node(s) and sends a Request to retrieve documents, through any intermediary Participant or Subparticipants, as applicable, to each Responding Node.
   a) The Responding QHIN's Request includes the repository ID, document ID, and/or any other document metadata as known by the Responding Node.

   b) The Responding QHIN creates an audit log entry including the HCID of the Initiating Node, Initiating QHIN, and Responding Node(s).
4) Each Responding Node returns a Response with the appropriate document(s) and associated document ID(s) to the Responding QHIN, through any intermediary Subparticipants or Participant. as applicable.
5) Each Responding QHIN combines the Responses from the Responding Node(s) and returns a single IHE Cross Gateway Retrieve [ITI-39] Response to the Initiating QHIN's Initiating Gateway.
   a) The Responding QHIN creates an audit log entry including the HCID and Assigning Authority of the Responding Node(s), Initiating QHIN, and Initiating Node.
6) The Initiating QHIN returns the Response(s) to the Initiating Node, through any intermediary Participant or Subparticipants, as applicable.
   a) The Initiating QHIN creates an audit log entry identifying the Responding Node(s) and Initiating Node.

Alternate Flow 1: Error Flow

1) This workflow begins at Step 4 of the Nominal Flow.
2) A Responding Node returns an error message (e.g., XDSRepositoryError).
3) The Responding QHIN returns a Response to the Initiating QHIN's Initiating Gateway including the status urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure and one or more regrep:ResponseStatusType:RegistryError elements.
4) The Initiating QHIN returns a failure message to the Initiating Node for dispositioning.

Alternate Flow 2: Retrieve returns partial success

1) This workflow begins at Step 4 of the Nominal Flow.
2) A Responding Node returns an error message (e.g., no document is found).
3) The Responding QHIN combines the Responses from the Responding Node(s) and returns a single IHE Cross Gateway Retrieve [ITI-39] Response to the Initiating QHIN's Initiating Gateway.
   a) If some, but not all, Requested documents are available, the Response includes all available documents, the status urn:ihe:iti:2007:ResponseStatusType:PartialSuccess, and some number of RegistryError elements.
4) The Initiating QHIN chooses to execute one of the following subflows:
   a) Subflow 1: If the Initiating Node is unable to process a Partial Success Response, the Initiating QHIN returns the Response to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable) as a Success. The Response does not indicate there were errors.
   b) Subflow 2: The Initiating QHIN returns the Response to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable), along with information about any errors.

Alternate Flow 3: Initiating Node asserts an Instance Access Consent Policy or Access Consent Policy

1) The Initiating Node includes the URI(s) of one or more Access Consent Policies (ACPs) or Instance Access Consent Policies (IACP) in its Query Solicitation.
   a) An ACP may have an associated instance (IACP, e.g., a signed patient consent form) for a specific patient.
2) Each Responding Node obtains the (I)ACP per the Document Retrieve Workflow.
   a) A Responding Node may incorporate retrieved (I)ACPs into access control decisions made with respect to releasing information in Response to a query.
   b) If a Responding Node is unable to obtain the (I)ACP document or is unable to process a retrieved (I)ACP document, and would not be able to disclose patient information without a valid (I)ACP, an error Response is returned. The flow ends for this Responding Node and the use case continues.
3) Nominal Flow resumes at Step 4.

Post-conditions

1) The Initiating QHIN has correlated the patient ID(s) and associated demographics received from the Initiating Node with the patient IDs and associated demographics as known by each Responding Node.
   a) Whether the Initiating QHIN persists this correlation for later use is beyond scope of this workflow and is not specified.
2) The Initiating Node has obtained all available patient matches.
3) The Initiating Node has obtained all Requested document metadata as known by each Responding Node, per the parameters of the query.
4) The Initiating Node has retrieved all available documents as known by each Responding Node that does not respond with an error.
5) All Requests and Responses have audit log entries showing source(s) and destination(s).

Message Delivery Scenario

In this scenario, a health care provider treats a patient in an emergency department and seeks to send a summary of the patient's care to the patient's primary care provider(s) through TEFCA Exchange.

The health care provider is a member of a local network (e.g., state/local HIE, vendor- or payer-based network, etc.), which is connected as a Participant of a QHIN. To send the patient's care summary, the provider first sends a Message Delivery Solicitation to the local network, which is routed to the QHIN over a secure channel. The Message Delivery Solicitation includes the content of the message (i.e., the care summary), patient demographics and/or identifiers for a single patient, and information about the intended Responding Node of the message. The local network also transmits information about the identity of the provider sending the message, as well as an Exchange Purpose specified by the provider (i.e., "Treatment" in this scenario).

The QHIN processes the Message Delivery Solicitation, checks its QHIN Directory to identify the appropriate Responding QHIN, and initiates a QHIN Message Delivery. The Initiating QHIN connects to the Responding QHIN using the TLS protocol to establish a secure channel for the QHIN Message Delivery transaction; each QHIN authenticates the other QHIN (i.e., mutual authentication). After establishing a secure channel, the Initiating QHIN sends the Responding QHIN a SAML assertion conforming to the IHE XUA profile along with the message delivery transaction. The SAML assertion preserves information from the Message Delivery Solicitation about the Initiating Node and the Exchange Purpose, but is assembled by the QHIN and signed by the QHIN's digital certificate.

The QHIN Message Delivery transaction uses the IHE Cross-Community Document Reliable Interchange (XCDR) profile[11] to send the provider's message and other metadata from the Initiating QHIN to the Responding QHIN. The Responding QHIN then converts the XCDR transaction into the appropriate internal format, if necessary, and transmits the message to the Responding Node. The message is routed through any intermediary Participant and Subparticipants, as necessary. The Responding Node returns an acknowledgement message with appropriate disposition information to the Responding QHIN, which forwards the acknowledgment to the Initiating QHIN. The Initiating QHIN routes the acknowledgement through its network, including any intermediary Participant and Subparticipants, as necessary, to the provider that sent the message.

Each QHIN involved in the QHIN Message Delivery maintains audit logs of all activities and transactions the QHIN performed in the process of delivering the message, according to the IHE ATNA profile.

Specified standards for QHIN Message Delivery are included in *Table 2*.

Table 2. Specified Standards for QHIN Message Delivery

Message Delivery Functions	Specified Standard / Profile
Secure Channel	• IETF TLS 1.2 w/ BCP-195 or • IETF TLS 1.3 w/ BCP-195
Mutual Authentication	• IETF TLS
User Authentication	• IHE XUA
Authorization & Exchange Purpose	• IHE XUA
Message Delivery	• IHE XCDR
Auditing	• IHE ATNA (Content Only)

[11] *IHE Cross-Community Document Reliable Interchange (XCDR) profile,* a supplement to the IHE IT Infrastructure (ITI) Technical Framework available at http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf.

Actors

Actors/Services	Cardinality	System Actor
Initiating Node	1..1	Any initiating Actor
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 Actor

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 Request such as who is Requesting, what their role is, and what their Exchange Purpose is.
   c. The ability of the QHIN's Responding Gateway and Participants to choose if/how to allow the transaction to proceed based on this information and the requirements of the Common Agreement.

Pre-conditions

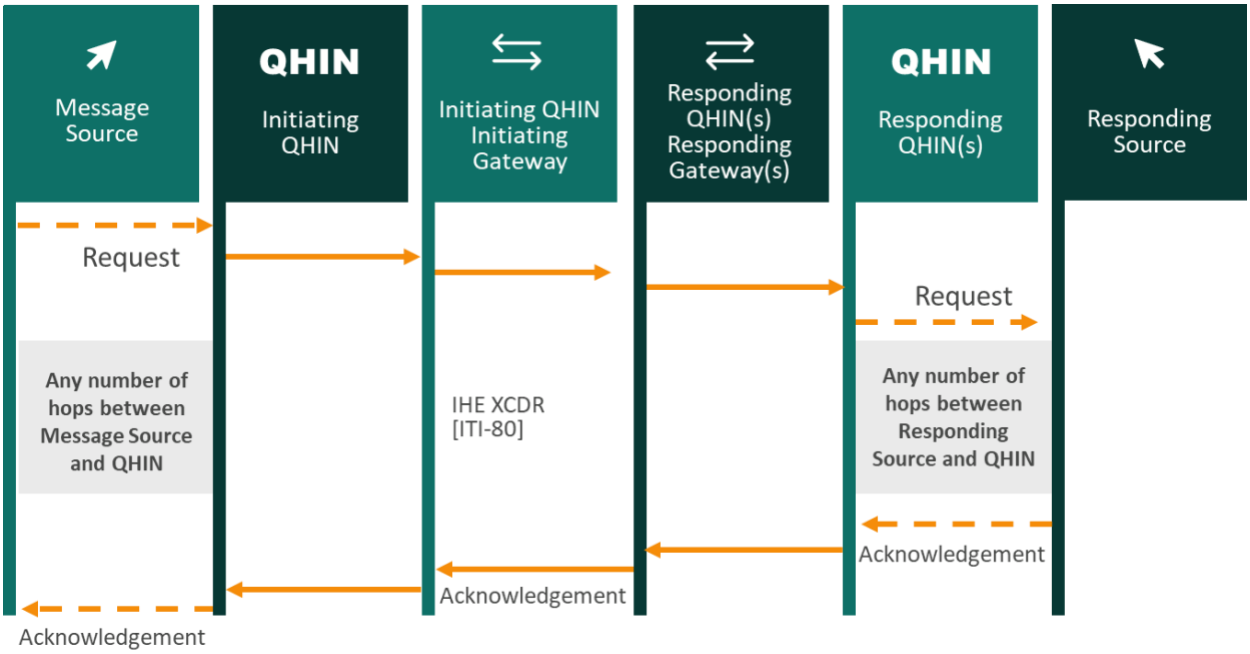
The following workflow assumes the following conditions:

- The Initiating Node knows a sufficient number of the patient's demographics for a successful match as determined by the Responding Node.
- The Initiating Node knows the HomeCommunityID or other organizational information (e.g., organization name, city, and state) necessary to determine the appropriate destination of the message.
- Each Actor has the appropriate service endpoint(s) and other connectivity information for any other Actors with which it connects directly.
- The RCE Directory includes the organization name(s) and HomeCommunityID(s) for all current Participants and Subparticipants who have chosen to participate as a Responding Node of QHIN Message Delivery. Each Participant and Subparticipant is matched to the appropriate QHIN.
- Each QHIN maintains an up-to-date copy of the RCE Directory.
- Responding QHINs know the current HomeCommunityIDs for any Responding Nodes.

Use Case Steps

Message Send

Nominal Flow



1) The Initiating Node sends a Message Delivery Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to send a message.
   a) The Initiating QHIN queries its QHIN Directory to identify the appropriate Responding QHIN for each message recipient included in the Message Delivery Solicitation.
2) The Initiating QHIN creates an IHE Cross-Gateway Document Provide [ITI-80] transaction and sends it via the Initiating Gateway to each Responding QHIN's Responding Gateway.
   a) The Initiating QHIN includes the HCID identifying the Responding Node.
   b) The Initiating QHIN creates an audit log entry including the HCID and Assigning Authority of the Initiating Node and Responding QHIN(s).
3) The Responding QHIN queries its QHIN Directory to identify the appropriate Responding Node and sends the message, through any intermediary Participant or Subparticipants, as applicable, to the Responding Node.
   a) The Responding QHIN creates an audit log entry including the HCID and Assigning Authority of the Initiating Node, Initiating QHIN, and Responding Node.
4) The Responding Node returns an acknowledgement, through any intermediary Participant or Subparticipants, as applicable.
5) The Responding QHIN creates and sends an XCDR acknowledgement to the Initiating QHIN's Initiating Gateway.
   a) The Responding QHIN creates an audit log entry including the HCID of the Responding Node, Initiating QHIN, and Initiating Node.

6) The Initiating QHIN returns each acknowledgement to the Initiating Node, through any intermediary Participant or Subparticipants as applicable.
   a) The Initiating QHIN creates an audit log entry identifying the Responding Node and Initiating Node of the Response.

Alternate Flow 1: Error Flow

1) This workflow begins at Step 4 of the Nominal Flow.
2) A Responding Node returns an error message (e.g., message cannot be delivered).
3) The Responding QHIN returns a Response to the Initiating QHIN's Initiating Gateway including the status urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure and one or more regrep:ResponseStatusType:RegistryError elements.
4) The Initiating QHIN returns a failure message to the Initiating Node for dispositioning.

Alternate Flow 2: Patient Verification

1) This Workflow **precedes** Step 1 of the Nominal Flow
2) The Initiating Node initiates a Patient Discovery including all available patient demographics and sufficient information to identify the desired message recipient(s), such as the organization name, city, and state, Assigning Authority ID, and/or HCID(s) of the recipient(s).
3) The Initiating Node includes the Patient Identity in the Message Delivery Solicitation.
4) The Workflow continues at Step 1.

Post-conditions

- The Responding Node has received the document sent by the Initiating Node.
- The Initiating Node has obtained acknowledgement of receipt from each Responding Node.
- All Requests and Responses have audit log entries showing source and destination.

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 IHE 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 (UDAP) 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 with the demographics held and begins to query for that patient's health care data.

Specified standards for a Facilitated FHIR Query are included in *Table 1*.

Table 3. Specified Standards for Facilitated FHIR Query

Query Functions	Specified Standard(s) / Profile(S)
Secure Channel	• IETF TLS 1.2 w/ BCP-195[12] or • IETF TLS 1.3 w/ BCP-195
Node Registration	• OAuth V2.0 • HL7 *FAST UDAP* Security for Scalable Registration, Authentication, and Authorization
User Authentication	• OAuth V2.0 • HL7 *FAST UDAP* Security for Scalable Registration, Authentication, and Authorization
Authorization & Exchange Purpose	• OAuth V2.0 • HL7 *FAST UDAP* Security for Scalable Registration, Authentication, and Authorization
Query for Patients	• IHE XCPD • FHIR R4 V 4.0.1 • HL7 FHIR US Core Implementation Guide
Information Query and Retrieve	• FHIR R4 V 4.0.1 • FHIR Implementation Guides as required
Auditing	• IHE ATNA (QHINs; Content only) • ASTM E2147-18 (Participant/Subparticipant; Content only)

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.

[12] *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.

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

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 Request such as: who is sending, what their role is, and what their Exchange Purpose is.
   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 both the patient identifier(s) and Responding Node(s) for a query.

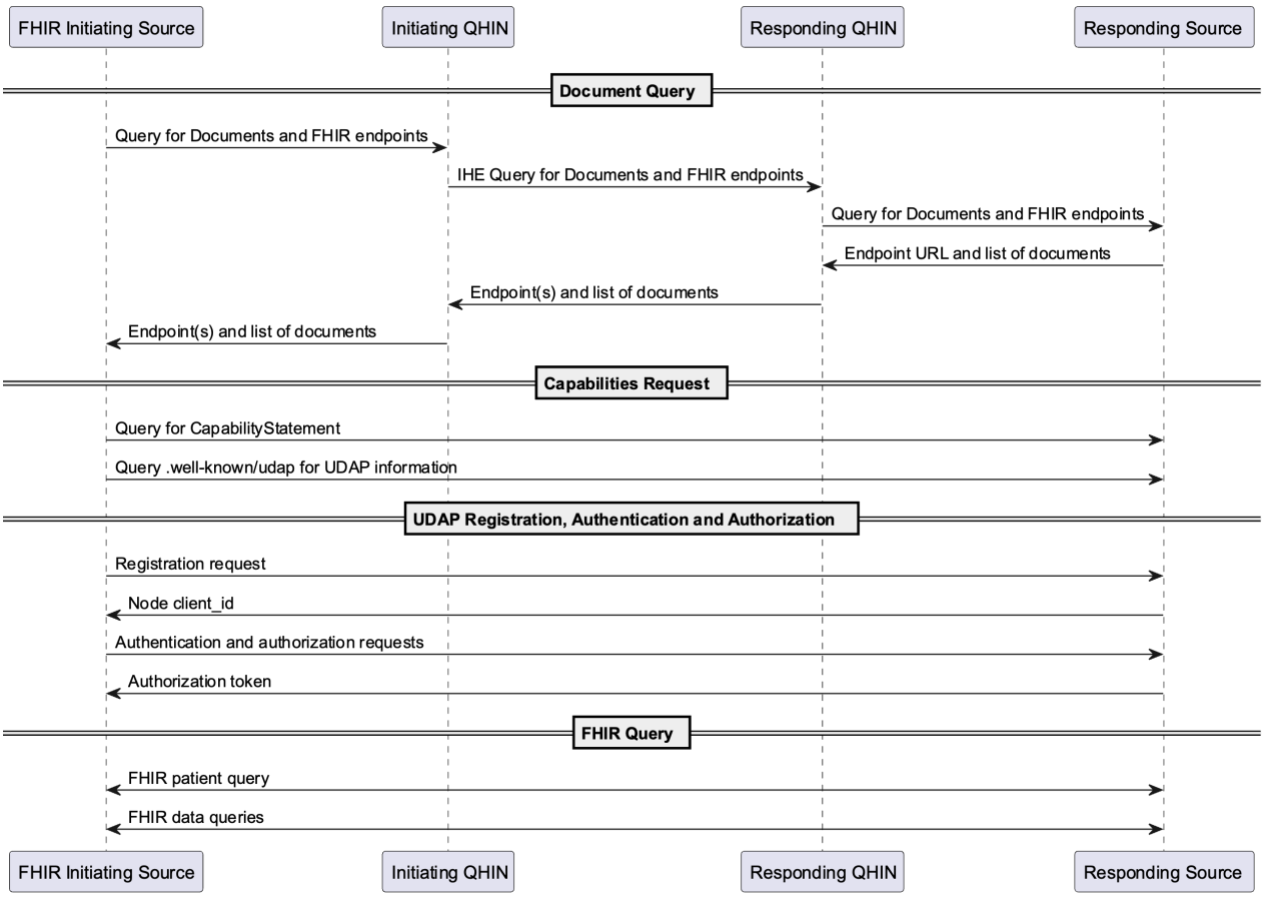
Pre-conditions

The following workflow assumes the following conditions:

- The Initiating Node knows sufficient patient demographics for a successful match as determined by the Responding Node.
- 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.
- The RCE Directory includes the organization facility name(s), and FHIR endpoints for all current Participants and Subparticipants.
- Each QHIN maintains an up-to-date copy of the RCE Directory.
- Responding QHINs know the current FHIR endpoints for any Responding Nodes.
- 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.

Use Case Steps

Nominal Flow



1) The Initiating Node sends a Query Solicitation, through any intermediary Subparticipants or Participant, as applicable, to the Initiating QHIN to query for endpoints.
   a) The Query Solicitation Response includes some number of patient identifiers and an Assigning Authority and HCID and/or FHIR endpoint for each.
   b) The Initiating QHIN creates an audit log entry identifying the Responding Node(s) and Initiating Node.
2) The Initiating Node selects which FHIR endpoint(s) they will be querying for data.
3) The Initiating Node queries for the Responding Node's CapabilityStatement and reviews all capabilities for match with the Initiating Node requirements.
4) 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.
5) The Initiating Node sends a UDAP Dynamic Client Registration Request to the Responding Node's authorization server with all relevant information and list of needed scopes.
   a) The Responding Node authorization server returns a client_id unique to that Initiating Node.

6) The Initiating Node uses the returned client_id and user information 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.

REQUIREMENTS FOR FUNCTIONS AND TECHNOLOGY TO SUPPORT EXCHANGE

Under the Common Agreement, QHINs are exchange hubs for participants in disparate health information networks. QHINs, Participants, and Subparticipants may Request to send or receive information through TEFCA Exchange and may offer Individual Access Services through which Individuals may send or receive their information through TEFCA Exchange.

QHINs are responsible for providing a set of Connectivity Services that support QHIN Query, Facilitated FHIR and QHIN Message Delivery. To effectively deliver Connectivity Services, QHINs must perform a consistent set of technical functions.

This section outlines these functions, specifying constraints, standards, and implementation approaches where applicable.

QTF-1 All requirements pertaining to the IHE ITI Technical Framework profiles, unless otherwise specified, refer to IHE IT Infrastructure Technical Framework Revision 17.0 – Final Text, published July 20, 2020.[13]

Connectivity and Remediation

The basis for TEFCA Exchange is connectivity. As such, QHINs must maintain connectivity with their Participants and with other QHINs.

QTF-2 Each QHIN MUST be able to connect successfully, i.e., able to transact without error, with every other QHIN. Any failure in connectivity MUST be addressed and resolved in the shortest time that is not infeasible, with infeasibility to be determined and demonstrated consistent with 45 CFR 171.204(a)(1) or (3), as applicable based on the reason and circumstances for the failure in connectivity.

QTF-3 Each QHIN MUST be able to connect successfully, i.e., able to transact without error, to all of its Participants. Any failure in connectivity MUST be addressed and resolved in the shortest time that is not infeasible, with infeasibility to be determined and demonstrated consistent with 45 CFR 171.204(a)(1) or (3), as applicable based on the reason and circumstances for the failure in connectivity.

Certificate Policy

Public key infrastructure (PKI) often serves as the basis for securing electronic communications over the internet. PKI involves the use of digital certificates to assert and authenticate identities, encrypt data, and sign communications.

[13] The *IHE IT Infrastructure Technical Framework Revision 17* and appropriate Supplements can be found via https://www.ihe.net/resources/technical_frameworks/technical_framework_archives/#IT

QHINs must possess appropriate digital certificates for authentication, encryption, and signing. QHIN certificates will be chained to root certificates issued by Certificate Authorities approved by the RCE. The RCE may also establish a broader certificate policy (e.g., including certificate life-cycle operational requirements, certificate usage policies, naming conventions, etc.).

QTF-4 QHINs MUST obtain TLS server certificates which are X.509 version 3 certificates with a signature that is at least 112 bits in length, and a public key of at least 256 bits in length; such certificates MUST be obtained, installed, and used in accordance with Applicable Law, and any relevant SOPs or implementation guides adopted by the RCE.

QTF-5 QHINs MUST deploy cryptographic modules certified to meet Federal Information Processing Standards (FIPS) Publication 140-2[14] or 140-3.[15]

Secure Channel

Protecting the privacy and security of health information is essential for building trust among participating entities. As such, QHINs must provide a secure channel to ensure transport-level security for all transactions under their domain. Modern networked systems typically rely on the TLS protocol to communicate over the internet. TLS provides privacy and data integrity between systems, using cryptographic techniques to encrypt communications. Specified standards for Secure Channel are included in *Table 3.*

Table 3. Specified Standard for Secure Channel

Function	Specified Standard / Profile
Secure Channel	• IETF TLS 1.2 w/ BCP-195 or • IETF TLS 1.3 w/ BCP-195

QTF-6 When interacting with another QHIN or Participant, a QHIN MUST establish a secure channel using TLS protocol version 1.2 or above.

QTF-7 Use of the TLS protocol MUST be consistent with IETF BCP 195.

QTF-8 A secure channel MUST conform to National Institute of Standards and Technology (NIST) Special Publication 800-52 Revision 2[16] with the exceptions of:

a. The following extensions MUST NOT be used:
   - TLS 1.2 Extension Client Certificate URL
   - TLS 1.3 Extension Early Data Indication
   - TLS 1.3 Zero Round Trip Time Resumption.

[14] *Security Requirements for Cryptographic Modules* (FIPS Publication 140-2) - available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[15] Security Requirements for Cryptographic Modules (FIPS Publication 140-3) - available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

[16] *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (Special Publication 800-52 Revision 2) – available at https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

QTF-9 Use of TLS 1.3 MUST be prioritized as of January 2024.

QTF-10 Servers MUST support both TLS 1.2 and TLS 1.3 connections until TLS 1.2 is deprecated by this framework.

Mutual Authentication

TLS also provides a "handshake" authentication protocol to verify the identities of systems establishing a secure channel. Whereas TLS can be implemented such that only "one side" (e.g., the server in a server-client relationship) is authenticated, this QTF specifies mutual authentication for all QHIN-to-QHIN and QHIN-to-Participant communication. Specified standards for Mutual Authentication are included in *Table 4*.

Table 4. Specified Standard for Mutual Authentication

Function	Specified Standard / Profile
Mutual Authentication	• IETF TLS 1.2 w/ BCP-195 or • IETF TLS 1.3 w/ BCP-195 • OAuth 2.0

QTF-11 When interacting with another QHIN, QHINs MUST mutually authenticate using TLS protocol version 1.2 or higher.

QTF-12 Authentication between QHINs and Participants MUST use TLS 1.2 or higher or OAuth 2.0.

QTF-13 Use of the TLS protocol MUST be consistent with IETF BCP 195.

QTF-14 Use of TLS 1.3 SHOULD be prioritized prior to January 2024 and MUST be prioritized by January 2024.

QTF-15 Servers MUST support both TLS 1.2 and TLS 1.3 connections until TLS 1.2 is deprecated by this framework.

User Authentication

Authentication involves establishing confidence in the identity of an entity or person. All entities and persons Requesting TEFCA Exchange must be authenticated, and authentication information must be shared "upstream," i.e., the entities' or persons' Participant and/or QHIN, for access control and auditing purposes. A QHIN, for example, needs to know and record the identity of any Subparticipant or user attempting to query for or send information via TEFCA Exchange. Because there may be a multi-layer hierarchy of Subparticipants under each Participant, the QHIN relies on each entity to obtain and share authentication information about those "downstream" from it, i.e., further removed from the QHIN in the hierarchy.

The IHE XUA Profile leverages SAML to communicate claims about an authenticated entity in transactions that cross enterprise boundaries. This QTF specifies that QHINs implement IHE XUA

to support exchange of authentication information among QHINs. Specified standards for User Authentication are included in *Table 5*.

Table 5. Specified Standard for User Authentication

Function	Specified Standard / Profile
User Authentication	• IHE XUA

Authentication involves establishing confidence in the identity of an entity or person. All entities and persons Requesting TEFCA Exchange must be authenticated, and authentication information must be shared "upstream," i.e., the entities' or persons' Participant and/or QHIN, for access control and auditing purposes. A QHIN, for example, needs to know and record the identity of any Subparticipant or user attempting to query for or send information via TEFCA Exchange. Because there may be a multi-layer hierarchy of Subparticipants under each Participant, the QHIN relies on each entity to obtain and share authentication information about those "downstream" from it, i.e., further removed from the QHIN in the hierarchy.

The IHE XUA Profile leverages SAML to communicate claims about an authenticated entity in transactions that cross enterprise boundaries. This QTF specifies that QHINs implement IHE XUA to support exchange of authentication information among QHINs. Specified standards for User Authentication are included in *Table 6*.

Table 6. Specified Standard for User Authentication

Function	Specified Standard / Profile
User Authentication	• IHE XUA

QTF-16 Use of SHA-1 is deprecated within TEFCA; all use of SHA in SAML metadata MUST use SHA-256 as defined in NIST FIPS Publication 180-4 Secure Hash Standard (SHS)[17].

QTF-17 When initiating a QHIN Query or QHIN Message Delivery, a QHIN MUST transmit a SAML assertion using IHE XUA, identifying the user or staff member at the QHIN, Participant, or Subparticipant or identifying the Individual who Requested use of the QHIN's Connectivity Services.

QTF-18 When a QHIN creates a new SAML assertion or rewrites the SAML information to sign it using the QHIN SAML certificate, the new SAML assertion MUST persist the originating user and, as applicable, organization information.

[17] See https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

QTF-19 Following the IHE XUA[18] requirements, the SAML assertion MUST include:

a. User information including name, UserID, Subject-Role, and, if appropriate, National Provider Identifier (NPI),
b. Organization name and HomeCommunityID of the Query or Initiating Node initiating the transaction, and
c. Patient Identifier including Assigning Authority, if known.

QTF-20 The SAML assertion MAY include the Authz-Consent Option.[19]

QTF-21 QHINs MUST be capable of receiving authentication information from Participants, including the authenticated identity of any Subparticipants and/or Individuals and/or users Requesting the use of Connectivity Services.

QTF-22 QHINs MUST specify the mechanism(s) (i.e., format and content) by which Participants transmit authentication information to the QHIN.

Authorization & Exchange Purpose

Authorization involves verifying whether an entity or person is eligible to access a Requested network or service. The Common Agreement requires that all Requests to send and receive information through TEFCA Exchange fall under a defined set of Exchange Purposes.

QHINs use SAML assertions based on the IHE XUA profile to identify the Exchange Purpose when initiating a QHIN Query or QHIN Message Delivery. Specified standards for *Authorization & Exchange Purpose* are included in *Table 7*.

Table 7. Specified Standard for Authorization & Exchange Purpose

Function	Specified Standard/Profile
Authorization & Exchange Purpose	• IHE XUA

QTF-23 QHINs MUST be capable of receiving and transmitting authorization information, including a representation of the Exchange Purpose, along with any Request for use of Connectivity Services.

QTF-24 When initiating a Patient Discovery, QHIN Query or QHIN Message Delivery, a QHIN MUST transmit a SAML assertion using IHE XUA, including the Exchange Purpose as identified by the staff or users at the QHIN, Participant, or Subparticipant Requesting the use of Connectivity Services.

[18] See IHE IT Infrastructure Technical Framework Volume 2b section 3.40, available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol2b_FT_2020-07-20.pdf
[19] See *IHE IT Infrastructure Technical Framework Volume 2b section 3.40.4.1.2.2*, available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol2b_FT_2020-07-20.pdf

QTF-25 The Initiating QHIN MUST verify the Initiating Node's asserted Exchange Purpose against those listed for the Initiating Node in the RCE Directory Service. A transaction without an Exchange Purpose that is listed in that Initiating Node's directory entry MUST NOT be accepted.

QTF-26 The PurposeOfUse in the SAML assertion MUST be 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.

QTF-27 The XUA PurposeOfUse Option[20] MUST be used and the purpose of use MUST be consistent with the SAML Purpose of Use information.

QTF-28 All XUA and SAML metadata MUST be consistent. Where discrepancies exist, they MUST be resolved prior to the next step in the workflow.

QTF-29 QHINs MUST specify the mechanism (i.e., format and content) by which Participants transmit authorization information, including an Exchange Purpose, to the QHIN.

Patient Discovery Query

Health information exchange workflows typically begin with a search for matching patients. IHE provides a widely implemented profile supporting patient discovery: XCPD.

XCPD enables entities to locate communities that hold relevant patient health data and correlate patient identifiers across communities holding the same patient's data. XCPD is frequently used to discover patients prior to an XCA query.

QHINs will return both HomeCommunityIDs and FHIR endpoints where available. The FHIR Endpoint will not contain patient context information as that information will be searched for independently using a FHIR query.

QHINs must implement the IHE XCPD profile to enable query-based QHIN-to-QHIN patient discovery. The specified standard for patient discovery is included in *Table 8*.

Table 8. Specified Standard for Query

Function	Specified Standard / Profile
Patient Discovery	• IHE XCPD

QTF-30 QHINs MUST ensure that Query Solicitations unambiguously and accurately identify the Initiating Node.

QTF-31 QHINs MUST implement the IHE XCPD profile for QHIN Patient Discovery.

[20] See *IHE IT Infrastructure Technical Framework* Volume 2b Section 3.40.4.1.2.3 PurposeOfUse Option for details: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol2b_FT_2020-07-20.pdf

QTF-32 Initiating QHINs MUST be capable of receiving Query Solicitations from a Participant.

QTF-33 Initiating QHINs MUST be capable of processing Query Solicitations to determine the appropriate Responding QHIN(s) via their QHIN Directory.

QTF-34 If the Initiating Node does not indicate specific providers or facilities to be queried, all QHINs MUST be queried using provided demographics.

QTF-35 Initiating QHINs MUST be capable of processing Query Solicitations to identify patient demographic information to include in XCPD Requests to Responding QHINs.

QTF-36 Responding QHINs MUST be capable of processing XCPD Requests to resolve patient identity (see Patient Identity Resolution function).

QTF-37 Initiating QHINs MUST be capable of processing XCPD Responses and sending the results to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable).

QTF-38 Initiating QHINs MUST include all patient demographics provided in the Query Solicitation in the XCPD Request resulting from that Query Solicitation, unless demographics are provided that are not supported by the XCPD profile.

QTF-39 Each Patient Discovery match (i.e., RegistrationEvent) MUST include the code NotHealthDataLocator to indicate that the corresponding community does not maintain externally available location information about this patient. See *IHE ITI TF-2b: 3.55.4.2.2.5 Specifying Support as a Health Data Locator*.

QTF-40 Patient Discovery Responses returning HomeCommunityIds MUST include the Responding Node's HomeCommunityId, Assigning Authority, and the patient identifier when a successful patient match is found.

QTF-41 Patient Discovery Responses returning FHIR Endpoints MUST include the Responding Node's FHIR endpoint not constrained to a patient context when a successful patient match is found.

QTF-42 Data for address fields used in Patient Discovery Queries MUST be converted, if needed to conform to Project US@ Technical Specifications[21], by the Initiating QHIN prior to being transmitted to any Responding QHINs. However, if the field does not contain a street address but contains other geographical details, it is recommended that whatever information that the patient provided not be abbreviated.

QTF-43 A Responding QHIN MUST NOT reply to a query with the demographics used to initiate the Patient Discovery Query. The Responding Node MUST return the demographics as known in its system.

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

QTF-44 A Responding QHIN MUST NOT respond to a Patient Discovery query with a Request for additional demographics.

Document Query and Retrieve

Locating patient records for retrieval involves multiple steps, including determining what information in the form of documents is available, and actual retrieval of the desired documents. The IHE XCA profile specifies this process.

XCA supports the means to query and retrieve relevant patient health data held by other communities in the form of documents. Using XCA requires knowledge of patient identity and the HomeCommunityID of the Responding Node when querying for and retrieving clinical documents.

IHE does not define a document beyond "a collection of bytes, including proprietary and textual formats."[22] Therefore an XCA document may be any form of information including C-CDA 2.1, FHIR® resources, PDF, or other formats. For purposes of Document Query and Retrieve, C-CDA 2.1 is the expected format for all patient information. If a Responding Node is unable to return a C-CDA 2.1 document, the data may be converted to the C-CDA 2.1 format by a Responding QHIN, Participant, or Subparticipant prior to transmission to the Initiating QHIN.

QHINs must implement the IHE XCA profile to enable query-based QHIN-to-QHIN document exchange. The specified standard for Document Query and Retrieve is included in *Table 9*.

Table 9. Specified Standard for Document Query

Function	Specified Standard / Profile
Document Query and Retrieve	• IHE XCA

QTF-45 QHINs MUST implement the IHE XCA profile for QHIN Document Query and Retrieve.

QTF-46 Initiating QHINs MUST be capable of processing Query Solicitations to identify query parameters to include in XCA Requests to Responding QHIN(s).

QTF-47 When initiating a QHIN Query, an Initiating QHIN MUST use ITI-38 Cross Community Query and ITI-39 Cross Community Retrieve, even if using a non-IHE transaction to receive the query from their Participant.

QTF-48 A Responding QHIN MUST accept only ITI-38 Cross Community Query and ITI-39 Cross Community Retrieve from an Initiating QHIN for QHIN Query IHE transactions but may use any exchange method with their Participants.

[22] *IHE IT Infrastructure White Paper Health Information Exchange: Enabling Document Sharing Using IHE Profiles*– available at https://profiles.ihe.net/ITI/HIE-Whitepaper/index.htmlf

QTF-49 When a Responding Node is unable to generate C-CDA 2.1 format documents, QHINs MAY offer document conversion services, except where the use of another format is consistent with QTF-51 and QTF-54.

QTF-50 A QHIN converting a document to C-CDA 2.1 format MUST convert to one of the templates as defined in HL7 CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes – US Realm.[23]

QTF-51 Responding QHINs SHOULD transmit any specific document format Requests (provided by the Initiating QHIN via the IHE XDSDocumentEntryFormatCode XCA parameter) to Responding Nodes.

QTF-52 Responding QHINs SHOULD provide C-CDA 2.1 documents that follow recommendations as presented in Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes.[24]

QTF-53 All C-CDA 2.1 format documents adhering to the Continuity of Care Document template MUST include all appropriate data classes and elements from United States Core Data for Interoperability (USCDI) V1.[25] The RCE will update the QTF to enable the use of future versions of USCDI that are consistent with ONC rules for health IT certification compliance.

QTF-54 Responding QHINs MAY provide patient information in other document formats if required by Applicable Law or if an alternative format is Requested by the Initiating QHIN via the IHE XDSDocumentEntryFormatCode XCA parameter.

QTF-55 The minimum required parameters for a FindDocuments transaction are the Responding Node's HomeCommunityID, patientId, and Assigning Authority for each patient record returned, and the status of the document entries to return, typically urn:oasis:names:tc:ebxml-regrep:StatusType:Approved. "Approved" in this context means that the document is available for patient care and has not been superseded by a new version.

QTF-56 If such a Request is indicated by the Query Solicitation, Initiating QHINs MAY specify a document status of urn:oasis:names:tc:ebxml-regrep:StatusType:Deprecated to obtain historical document entries that have been superseded or are not considered the most current version.

QTF-57 Responding QHINs SHOULD provide to Responding Nodes any specific document status Requests provided by the Initiating QHIN in the FindDocuments transaction.

---

[23] C-CDA (HL7 CDA® R2 Implementation Guide: Consolidated CDA Templates for Clinical Notes - US Realm) available at: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=492

[24] *Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes* -- available at https://carequality.org/wp-content/uploads/2022/04/Improve-C-CDA-Joint-Content-WG-v2.0-20220316-DISTRO.pdf

[25] *The United States Core Data for Interoperability (USCDI*) – available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

QTF-58 QHINs MUST support the $XDSDocumentEntryServiceStartTimeTo and $XDSDocumentEntryServiceStopTimeFrom parameters for limiting the number of documents returned from a query and Responding QHINs SHOULD transmit any such parameters to the Responding Node.

QTF-59 $XDSDocumentEntryServiceStartTimeTo and $XDSDocumentEntryServiceStopTimeFrom are optional parameters that MAY be included in the FindDocuments query to limit the number of documents returned. Usage MUST follow the guidance of Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes Appendix A.3 IHE XDS Query Parameters. serviceStartTime and serviceStopTime are defined ITI TF-3 Table 4.1.3.2-1. These query parameters are among the metadata parameters that MUST be returned with objects in all LeafClass Query for Documents Responses. serviceStartTime and serviceStopTime MUST be Requested as UTC in DTM format.

QTF-60 The FindDocuments Request MAY include both DocumentEntryType parameters with values of urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1 and urn:uuid:34268e47-fdf5-41a6-ba33-82133c465248 to specify that Stable and On-Demand Documents should be included where both are available. If only Stable or On-Demand Documents are available, only those DocumentEntries should be sent.

QTF-61 The Initiating QHIN MUST specify a returnType parameter value of LeafClass, which means to return full metadata contents. See *IHE ITI TF-1: 18 Cross-Community Access (XCA) Integration Profile*, *IHE ITI TF-2b: 3.38*, and *IHE ITI TF-2a: 3.18*.

QTF-62 Responding QHINs MUST be capable of processing XCA Requests to identify and retrieve appropriate documents.

QTF-63 Initiating QHINs MUST be capable of processing XCA Responses and sending the results to the Initiating Node (through any intermediary Participant or Subparticipants, as applicable).

QTF-64 The QHIN Initiating Gateways MUST support the XDS Affinity Domain XCA option for both IHE Cross Gateway Query [ITI-38] and IHE Cross Gateway Retrieve [ITI-39] as specified in section 18.2.1 of the IHE Technical Framework Volume 2.

Message Delivery

In addition to query-based document exchange, many health information networks also provide capabilities for users to send (i.e., push) patient data to other entities. The TEFCA Exchange enabled by the Common Agreement supports push capabilities using the IHE XCDR[26] profile. QHINs function as hubs for routing messages sent to and from their networks.

[26] *IHE Cross-Community Document Reliable Interchange (XCDR)* - available at https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf

The specified standards for message delivery are included in *Table 10*. Message delivery transactions between QHINs and Participants may use the XCDR profile or may negotiate a different delivery method that supports the local workflow.

Table 10. Specified Standard for Message Delivery

Function	Specified Standard / Profile
Message Delivery	• IHE XCDR

QTF-65 All QHINs MUST implement Cross-Community Document Reliable Interchange (XCDR) Rev. 1.6 for message exchange with other QHINs.

QTF-66 All QHIN XCDR Responding Gateways MUST also support the IHE XDR Document Recipient.

QTF-67 QHINs MAY implement the XCDR profile for exchange with their Participants or negotiate other methods of exchange.

QTF-68 Initiating QHINs MUST be capable of processing Message Delivery Solicitations to determine the appropriate Responding QHIN(s) via their QHIN Directory.

QTF-69 All Initiating QHINs MUST return acknowledgement of delivery of the message to the Initiating Node (via any intermediary Participant and Subparticipants, as applicable).

QTF-70 QHINs MUST specify the format and content of acceptable message delivery acknowledgements from Participants.

QTF-71 Initiating QHINs MUST be capable of receiving Message Delivery Solicitations from a Participant.

QTF-72 Initiating QHINs MUST be capable of processing Message Delivery Solicitations to identify documents and associated metadata to include in XCDR transactions to the appropriate Responding QHIN(s).

QTF-73 Responding QHIN(s) MUST be capable of processing XCDR transactions to send documents and associated metadata to the Responding Node (via any intermediary Participant and Subparticipants, as applicable).

QTF-74 QHINs MUST be capable of sending and receiving message delivery acknowledgements to and from QHINs and Participants.

QTF-75 A Responding QHIN MUST transfer the content of the XCDR transaction to the appropriate Participant for management or transfer to their Subparticipant.

QTF-76 A Responding QHIN that is unable to deliver the content of a Message Delivery transaction must return the XDSUnavailableCommunity error.

Patient Identity Resolution

Patients frequently cross network boundaries when receiving care, contributing to fragmentation of records, duplicate records, and inconsistent representations of patient identity across disparate providers. Accurately resolving patient identity is necessary for ensuring appropriate access to information, particularly in query-based contexts. Some QHINs might use a centralized master patient indexing service to manage identity information associated with patients under the QHIN's domain. Other QHINs might rely on more federated approaches to resolve patient identity (e.g., by sending patient demographic information and Requesting matches from each Participant connected to the QHIN).

QTF-77 A QHIN MUST be capable of accurately resolving Requests to match patient demographic information with patient identities under its domain via an Enterprise Master Patient Index (eMPI) or Record Locator Service; OR

QTF-78 A QHIN MAY use other innovative methods or delegate the patient identity resolution function to its Participant(s).

QTF-79 A QHIN MUST fulfill service-level agreement (SLA) requirements for all Patient Discovery queries.

QTF-80 A patient identity resolution function MUST be able to respond to a QHIN Query within any service-level agreement (SLA) requirements adopted by the RCE for TEFCA Exchange.

Record Location

The exchange functions enabled by TEFCA Exchange depend on accurately determining which entities maintain relevant information. Query functions, in particular, rely on accurate and comprehensive record location. This QTF does not specify a particular technology or standard for QHINs to use to locate patient records.

QTF-81 A Responding QHIN MUST be capable of identifying which, if any, of its Participants and/or Subparticipants are the Responding Node.

Directory Services

Directory services enable entities to manage information associated with health care organizations and persons. A provider directory, for example, may include information about a provider's demographics (e.g., name, date of birth), relationships (e.g., where a provider works), and electronic endpoints (e.g., a Direct address, HL7® FHIR® server URL). QHINs will rely on directories to route transactions. For instance, a QHIN might use a directory to identify the appropriate recipient(s) of a QHIN Message Delivery or QHIN Query.

The RCE Directory Service is an HL7 FHIR-based service using a profile on the Organization resource and custom transactions. The RCE Directory Service will be the primary location for

determining the HomeCommunityID and Responding QHIN for QHIN-to-QHIN data exchange. QHINs will be responsible for updating the RCE Directory Service with HomeCommunityIDs of their connected Participants and Subparticipants. QHINs are expected to maintain a local copy of the contents of the RCE Directory Service to support their Connectivity Services and facilitate query and message delivery transactions.

This QTF specifies the following directory service constraints:

QTF-82 The QHIN Directory MUST maintain the Responding QHIN and HomeCommunityID for all Participants and Subparticipants.

QTF-83 An Initiating QHIN MUST be capable of accurately identifying the Responding QHIN for a QHIN Query or QHIN Message Delivery via its QHIN Directory.

QTF-84 All connections to the RCE Directory Service MUST conform to the requirements of the RCE Directory Service Implementation Guide.[27]

QTF-85 A QHIN MUST update the RCE Directory Service with any new Participant and Subparticipant Initiating Nodes at least 48 hours prior to the Participant and Subparticipant commencing production activities.

QTF-86 A QHIN MUST create a directory entry for each individual facility within a Participant's or Subparticipant's organization.

QTF-87 A QHIN MUST include all intended Exchange Purpose codes a Participant or Subparticipant will use for all initiated transactions.

QTF-88 A QHIN MUST ensure that all updates and changes to Participant or Subparticipant HomeCommunityID(s) are submitted to the RCE Directory Service prior to taking effect.

QTF-89 QHINs MUST retrieve all changes to the RCE Directory Service and merge them into their QHIN Directory no more often than once per hour and no less often than once per day.

Auditing

Maintaining records of activities and transactions supported by the Connectivity Services can assist with troubleshooting and help facilitate monitoring for improper use. Moreover, audit records support a QHIN's ability to maintain and produce an accounting of disclosures, where required by Applicable Law and/or the Common Agreement.

The IHE ATNA profile describes several foundational elements of secure systems, including node authentication, user authentication, telecommunications encryption, and event audit logging. QHINs must implement the IHE ATNA profile requirements specific to event audit logging for

[27] *RCE Directory Service Implementation Guide*, when available, to be located at: https://rce.sequoiaproject.org/tefca-and-rce-resources

activities and transactions between QHINs and between QHINs and Participants, including the standard schema for encoding reported events, standard reportable events, and standard transport methods. Other elements of secure systems defined by ATNA, such as authentication, are specified elsewhere in this QTF. Specified standards for auditing are included in *Table 11*.

Table 11. Specified Standards for Auditing

Function	Specified Standard / Profile
Auditing	• IHE ATNA (content only) • ASTM E2147-18

QTF-90 A QHIN MUST be able to export all relevant audit records with format requirements as specified in the IHE ATNA profile for all activity and transaction events involving another QHIN or Participant.

QTF-91 A QHIN MUST follow auditing content guidance in any of the IHE transactions and profiles specified by this QTF including all codes and elements.

QTF-92 A QHIN MUST create and store audit records for all activity events related to the QHIN's operation.

Error Handling

Activities and transactions enabled by a QHIN's Connectivity Services may fail or otherwise generate errors. Error messages should clearly communicate the cause of the error along with any other appropriate details to assist in resolving the issue.

QTF-93 A QHIN MUST be capable of generating, sending, and receiving error messages for activities and transactions involving other QHINs as defined in IHE profiles specified by this QTF.

QTF-94 A QHIN MUST be capable of sending and receiving error messages for activities and transactions originating from Participants, translating them as needed into error messages as defined in IHE profiles specified by this QTF, and returning them in Responses to the Initiating or Responding QHIN, as necessary.

Constraints for QHIN Query for Initiating Node(s) and Responding Node(s)

For proper operation of the transactions enabled by TEFCA Exchange, QHINs will need to ensure that Participants and Subparticipants provide information necessary for QHIN functions. The following requirements must be complied with at the level of Query or Initiating Node and/or Responding Node, as applicable, regardless of whether the Initiating Node, Initiating Node, or Responding Node is a QHIN, Participant, or Subparticipant:

QTF-95 A Initiating Node MUST include all known demographics supported by the IHE XCPD profile in its Query Solicitations for Patient Discovery with the exception of a Social Security Number, which MAY be included.

QTF-96 A Responding Node MUST send only one patient identity for each matching patient in Response to a patient discovery query.

QTF-97 Data for address fields used for patient discovery query SHOULD conform to Project US@ Technical Standards. However, if the field does not contain a street address but contains other geographical details, it is recommended that whatever information that the patient provided not be abbreviated.

QTF-98 A Responding Node SHOULD provide C-CDA 2.1 documents that follow recommendations as presented in Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes[28], when the information held by that Responding Node is organized around a clinical encounter construct.

QTF-99 A Responding Node MUST use nationally standardized code systems for all data exchange, where such code systems exist (e.g., LOINC, RxNORM, SNOMED-CT, etc.).

QTF-100 All C-CDA 2.1 format documents adhering to the Continuity of Care Document template MUST include all appropriate data classes and elements from USCDI v1 The RCE will update the QTF to enable the use of future versions of USCDI that are consistent with ONC rules for health IT certification compliance.

QTF-101 A Responding Node SHOULD NOT respond to a patient discovery query with a Request for additional demographics.

QTF-102 A Responding Node MUST NOT reply to a query with the demographics used to initiate the Patient Discovery Query. The Responding Node MUST return the demographics as known in its system.

QTF-103 The QHIN Initiating Gateways and Responding Gateways SHOULD support the On-Demand Document option.

QTF-104 An (I)ACP document reference MUST be accompanied by one of the following OIDs to declare the format of the consent document:

OID	Representation
urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.2.1	(I)ACP Document contains access consent and is in scanned PDF format of a signed document
urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.2.2	(I)ACP Document contains access consent and is in XACML format
urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.2.3	(I)ACP Document contains access consent and is in HL7 FHIR® Consent resource format
urn:oid: 2.16.840.1.113883.3.7204.1.1.1.1.2.4	(I)ACP Document contains access consent and is in Kantara Consent Receipt format

[28] *Concise Consolidated CDA: Deploying Encounter Summary CDA Documents with Clinical Notes* -- available at https://carequality.org/wp-content/uploads/2022/04/Improve-C-CDA-Joint-Content-WG-v2.0-20220316-DISTRO.pdf

QTF-105 Any (I)ACP asserted by a Initiating Node MUST be available for retrieval using the Document Retrieve Workflow.

QTF-106 If a query Request is accompanied by an (I)ACP document, the Responding Node SHOULD attempt to retrieve the document via the Document Retrieve Workflow, prior to responding to the query.

QTF-107 If an (I)ACP cannot be retrieved and the Responding Node is not able to disclose patient information without a valid (I)ACP, an appropriate error Response MUST be returned.

QTF-108 If a retrieved (I)ACP cannot be processed by a Responding Node and the Responding Node is not able to disclose patient information without a valid (I)ACP, that Responding Node MUST respond with an appropriate error indicating that the (I)ACP could not be verified.

QTF-109 If a query Request is not accompanied by an (I)ACP document and the Responding Node is not able to disclose patient information without a valid (I)ACP, an appropriate error Response (e.g., AccessDenial) SHOULD be returned.

QTF-110 All transactions between QHINs and Participants and/or Participants and Subparticipants MUST be represented in audit log entries that adhere to the content requirements in ASTM E2147-18[29] §7 Audit Data and Audit Report Content as a minimum requirement.

QTF-111 Participants and Subparticipants MUST provide all necessary information to their QHIN for the RCE Directory Service entry prior to the information affecting the production environment.

QTF-112 Participants and Subparticipants MUST communicate all changes to their RCE Directory entry to their QHIN no less than 48 hours prior to the changes being implemented in the production environment.

CONSTRAINTS SPECIFIC TO FACILITATED FHIR EXCHANGE

With the addition of FHIR to the exchange modalities used within the QTF, the following constraints are specific to FHIR transactions using Facilitated FHIR Exchange. All QHINs, Participants and Subparticipants must follow these constraints when utilizing Facilitated FHIR for TEFCA Exchange.

[29] ASTM E2147 – 18 *Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*– available at https://www.astm.org/e2147-18.html

General Requirements

To enable exchange using the FHIR standard, specific versions of the standard and of specific FHIR Implementation Guides are necessary to achieve basic interoperability. For exchange that does not apply to specific FHIR Implementation Guides, including US Core, FHIR Core requirements apply.

QTF-113 All FHIR transactions MUST conform to FHIR R4 Version 4.0.1.

QTF-114 Where profiles and requirements exist, FHIR Transaction resources and operations MUST conform to the current version of US Core listed in appropriate regulation.

QTF-115 The following FHIR Implementation Guides SHOULD be supported:

a. Bulk Data Access IG v1.0.1,

b. Mobile access to Health Documents (MHD) v4.2.0, and

c. Da Vinci Payer Data Exchange v1.0.0.

QTF-116 All Nodes SHOULD support the extensions for version conversion as specified in the FHIR Core section 2.7.0.7 Extensions for converting between versions.

QTF-117 Actors MUST continue to support any capabilities previously supported for TEFCA Exchange under a particular FHIR Release (e.g., FHIR R4) or FHIR Implementation Guide, until support for that FHIR Release or Implementation Guide has been officially sunsetted by the RCE.

QTF-118 If an Actor updates its endpoints listed in the QHIN/RCE Directory for any reason other than FHIR Release support, the Actor MUST continue to support transactions received at its previously listed endpoint(s) for a minimum of 48 hours after the QHIN has submitted the new endpoints in the RCE Directory.

FHIR Endpoints & Endpoint Discovery

Patient discovery and required endpoint listing will remain executed through a query to the QHINs which will be done by the QHINs as IHE transactions. These transactions will return both IHE Home Community IDs and/or FHIR endpoints for locations where patient data exists. FHIR endpoints returned in these transactions will not be limited to patient context and a patient search will be necessary to identify the specific patient.

QTF-119 All discovery of Endpoints by Participants and Subparticipants MUST be executed by a query to the QHIN Directory service which will have the FHIR endpoint(s) for Responding Nodes.

QTF-120 The DocumentEntry for a FHIR endpoint MUST have the following:

a. The URI element MUST be the FHIR endpoint of the Responding Node,
b. The Name element MUST be “FHIR Endpoint”,
c. The list of document UUIDs must be a single null UUID.

QTF-121 All FHIR-capable Responding Nodes MUST provide access to Patient resource and at least one FHIR resource.

QTF-122 Responding Nodes MUST use the FHIR CapabilityStatement resource to define FHIR server capabilities.

QTF-123 All FHIR-capable Responding Nodes MUST provide at least one publicly discoverable CapabilityStatement where CapabilityStatement.kind=”instance”.

QTF-124 All FHIR-capable Responding Nodes MUST provide a CapabilityStatement for each endpoint associated with a FHIR server, defining the capabilities available at that endpoint.

QTF-125 Capabilities listed within the CapabilityStatement MUST include all FHIR Implementation Guide operations supported by the Responding Node, in addition to any other capabilities specific to that system.

QTF-126 Capabilities listed within the CapabilityStatement SHOULD include all FHIR Implementation Guides supported by the Responding Node, in addition to any other capabilities specific to that system.

Patient Matching

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

QTF-127 All FHIR-capable Nodes MUST support the FHIR $match operation using a US Core Patient resource with demographics matching those used in the Patient Discovery query as payload to allow for full Responses to Patient queries from Initiating Nodes.

QTF-128 Responding Nodes SHOULD have the capability to return more than one potential patient match when a patient search yields more than one match.

QTF-129 Responding Nodes MUST NOT return more than one potential match when such action could be a violation of HIPAA or other Applicable Law.

QTF-130 When Initiating Nodes specify “onlyCertainMatches”=true within a $match Request Responding Nodes MUST honor that Request by returning only a unique match, if a unique match can be found.

QTF-131 Responding Nodes MUST NOT return more than 100 potential matches when onlyCertainMatches is set to false.

QTF-132 All Initiating Nodes MUST include all known demographics supported, 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.

QTF-133 Initiating Nodes SHOULD transform all patient demographic data elements to follow the vocabulary standards in USCDI v1 before attempting to query.

QTF-134 Initiating Nodes SHOULD normalize addresses to the Project US@ Technical Specification. However, if the field does not contain a street address but contains other geographical details, it is recommended that whatever information that the patient provided not be abbreviated.

QTF-135 Demographics used in all queries and query Responses SHOULD follow, at a minimum, USCDI v1 defined demographics.

QTF-136 Responding Nodes MUST NOT require more than all USCDI v1 demographics plus administrative gender before returning a patient list Response.

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 needed to be converted so that appropriate follow-ups can be made, where necessary. Use of Provenance only applies where data has been transformed.

QTF-137 A FHIR Provenance resource MUST be available for query for any data has been transformed.

QTF-138 Responding Nodes MUST use the FHIR 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.

QTF-139 Provenance.target MUST be references to all FHIR resources extracted from the document referenced by the Provenance.entity element.

QTF-140 Provenance.policy MUST contain the static URI “urn:oid:2.16.840.1.113883.3.7204.1.5.1.2”.

QTF-141 Provenance.agent MUST contain at least one entry [1..*] describing the system that extracted the elements from the document.

QTF-142 Provenance.agent.type MUST contain code “assembler” from the code system http://hl7.org/fhir/ValueSet/provenance-agent-type.

QTF-143 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.

QTF-144 Provenance.entity MUST contain one element [1..1] describing the source document the information was extracted.

QTF-145 Provenance.entity.role MUST be the code “source” from the http://hl7.org/fhir/provenance-entity-role codesystem.

QTF-146 Provenance.entity.what MUST be a reference to the DocumentReference resource pointing to the original document.

Error Responses

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

QTF-147 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.

QTF-148 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.

Security

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

QTF-149 Authorization Servers SHOULD issue access tokens with a lifetime no longer than 60 minutes.

QTF-150 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”.

QTF-151 All implementations MUST support RS256, and SHOULD support ES256, ES384 and RS384.

QTF-152 All X.509 certificates MUST have RS256 keys and SHOULD have ES256, ES384 and RS384 keys.

OAuth Discovery

Client Discovery MUST Conform to HL7 *FAST* UDAP Security for Scalable Registration, Authentication, and Authorization Section 2 with the following constraints:

QTF-153 The `udap_certifications_supported` metadata returned MUST include https://rce.sequoiaproject.org/udap/profiles/basic-app-certification.

QTF-154 The `udap_certifications_required` metadata returned MUST include https://rce.sequoiaproject.org/udap/profiles/basic-app-certification.

QTF-155 The `scopes_supported` metadata MUST be present and MUST list all scopes supported including all supported wildcard scopes.

OAuth Client Registration

Client Registration MUST Conform to HL7 *FAST* UDAP Security for Scalable Registration, Authentication, and Authorization Section 3 with the following constraints:

QTF-156 The software statement MUST contain a `certification_name` element of "TEFCA Basic App Certification".

QTF-157 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.

QTF-158 A previously registered client application MAY Request a modification of its previous registration with an Authorization Server by submitting another registration Request to the same Authorization Server's registration endpoint using a certificate with a Subject Alternative Name client URI entry matching the original registration Request.

QTF-159 A registration modification Request MUST include all parameters required for a new registration and all parameters for which modification is Requested.

QTF-160 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.

QTF-161 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 Requests.

QTF-162 Any retired client_ids MUST be preserved by the Authorization Server so that it can be associated with log entries and the Requester.

QTF-163 A client may only Request a wildcard scope if wildcards are specified in the scopes_supported metadata list.

QTF-164 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.

QTF-165 If wildcard scopes are not supported, the server SHOULD respond with an “invalid scope”.

QTF-166 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.

QTF-167 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.

QTF-168 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.

QTF-169 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.

QTF-170 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.

OAuth Access Grant

QTF-171 Then scope list as part of an access grant Request may be the same as the list from registration or may be a subset.

QTF-172 A grant time Request to the server MAY return a full or subset of the Requested scopes.

QTF-173 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.

QTF-174 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.

OAuth Authentication

Business to Business

Business to Business Client Registration MUST Conform to Authorization Code Grant Type as specified in the HL7 *FAST* UDAP Security for Scalable Registration, Authentication, and Authorization Section 5 with the following constraints:

QTF-175 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.

QTF-176 The hl7-b2b extension MUST conform to the requirements in **Error! Not a valid bookmark self-reference.**

Table 1 TEFCA Specific hl7-b2b Extension Requirements

organization_id	required	String containing the URL of Requestor's Organization resource in the RCE Directory service
Organization_name	required	String containing the Requestor's human readable organization name
subject_id	conditional	String containing the human readable name of the person responsible for originating the Request. MUST be present when applicable
purpose_of_use	required	An array of strings containing the purpose for which the data is Requested, from the code set of authorized Exchange Purposes found in the Exchange Purposes SOP

QTF-177 The Requesting application MUST provide metadata about the user to the data holder as additional authorization information at the time of the token Request by adding this information to the authentication JWT in the form of the TEFCA-specific authorization extension as customized in Table 2 TEFCA User Authorization Extension Object.

Table 2 TEFCA User Authorization Extension Object

Extension Name: “tefca_user”		
Element	**Optionality**	**Requirement**
version	required	Fixed string value: "1"
purpose_of_use	required	String value matching Purpose of Use for that user.
user_information	required	FHIR US Core Patient resource with all known demographics.
Ial_vetted	required	A comma separated list of demographic attributes provided within the Patient resource as specified in the Individual Access Services Implementation SOP.
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 Appendix B that represent identity proofing levels of assurance, each expressed as a URI, e.g. ["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.12"]
consent_reference	optional	An array of FHIR DocumentReference 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"]

QTF-178 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 Authorization Extension Error object in the ‘extensions’ object of the error Response.

Table 3 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.

QTF-179 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 or Consent resource included in the `consent_reference` array.

Individual Access Services (IAS) Requests

QTF-180 Responders MUST support the Authorization Code Grant type for IAS Requests.

QTF-181 The Initiating Node MUST provide both the tefca_user and tefca_ias extensions.

QTF-182 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.

Extension Name: "tefca_ias"		
Element	**Optionality**	**Requirement**
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 QTF-104 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

QTF-183 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.

QTF-184 The user metadata submitted by the Requesting application in the TEFCA IAS extension object MUST correspond to the verified identity attributes of the permitted user who is making the Request.

QTF-185 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 Patient Requests, it MUST return an invalid_grant error in Response to the token Request.

TESTING PROCEDURE SUPPORTING REQUIREMENTS

QHINs will need to complete testing procedures as part of the initial Designation process and must be prepared to engage in testing activities on an ongoing basis. Details of these processes are outlined in the Onboarding & Designation SOP[30].

QTF-186 All QHINs MUST create and maintain a test instance of the QHIN system to support testing and operations.

QTF-187 Each QHIN MUST create a test patient record and have a test clinician record created for diagnostic and onboarding testing per the Onboarding & Designation SOP, in both test and production environments.

[32] To be available at: https://rce.sequoiaproject.org/tefca-and-rce-resources/#StandardOperatingProceduresSOPs

QTF-188 QHIN test patients MUST be named with given name "QTF TEST" and family name QTFTEST-### (e.g., QTFTEST-001).

QTF-189 QHINS MUST NOT register test data into the production RCE Directory Service. During testing procedures, QHINs MUST determine facility routing information via their QHIN Directory.

QTF-190 The test patient data MUST include at least one C-CDA 2.1 document with fictional clinical data that can be queried and retrieved.

QTF-191 All QHINs SHOULD create at least one C-CDA Discharge Summary and Progress Note template document for the test patient. QHINs serving outpatient clinics and inpatient hospitals MUST create such documents. Any encounters, etc. MUST be linked to the clinician created for QTF-195.

QTF-192 Additional test data records MAY be created and made available as desired by the QHIN.

QTF-193 An outgoing patient discovery query using the test data as per the Onboarding & Designation SOP MUST include all available demographics.

QTF-194 An outgoing patient discovery Response using the test data as per the Onboarding & Designation SOP MUST return all available demographics.

QTF-195 A test clinician record per the Onboarding & Designation SOP MUST be available for QHIN Message Delivery receipt and be available in both test and production environments.

QTF-196 A "Document Query Nominal Flow" of the test data per QTF-186 MUST return the C-CDA 2.1 document(s) associated with a test patient.

PERFORMANCE MEASURES

In order to accurately measure the effectiveness of TEFCA Exchange, the RCE will collect several performance measures from QHINs. These data are meant to assess the performance of QHINs for each use case. The measures by themselves will not directly impact a QHIN's Designation status.

The following data MUST be submitted to the RCE for each calendar month by the 15th of the following month:

- Downtime for the QHIN's gateway Actors (e.g., Initiating Gateway, Responding Gateway) in minutes in the reporting month. Reports MUST include planned and unplanned downtime by Actor.
- As a QHIN Initiating Gateway:

a. Raw count of successful (i.e., completed without error) QHIN-to-QHIN transactions, per Responding QHIN, within the reporting period for each of:
    i. Patient discovery,
    ii. Document query,
    iii. Document retrieve, and
    iv. Message delivery.

b. Raw count of errors in QHIN-to-QHIN transactions, per Responding QHIN per IHE metadata error code[31] received within the reporting period.
c. Raw count of connectivity errors per Responding QHIN received within the reporting period.
d. Average Response time for each QHIN-to-QHIN transaction, per Responding QHIN transacted with during the reporting period. Each data point must include the message type, average Response time, and Responding QHIN.
e. Total number of documents retrieved via QHIN Query within the reporting period.
f. Total number of documents successfully delivered via Message Delivery within the reporting period.

- As a QHIN Responding Gateway:
    a. Average Response time for each QHIN-Participant transaction by HCID within the reporting period.
    b. Total number of messages received via QHIN Message Delivery within the reporting period.

The following data must be submitted to the RCE for each calendar quarter (three-month period):

a. Total number of member organizations and/or facilities connecting as or through the QHIN's Participants and Subparticipants with counts for each hospital, clinic, mental health center, post-acute/long-term care facility, public health entities, and payer organizations as well as an aggregate count of any other member organizations and/or facilities not matching these categories.
b. Total number of clinicians connecting through the QHIN's Participants and Subparticipants.
c. Total number of consumers/patients participating in Individual Access Services through the QHIN, its Participants, or Subparticipants.

QTF-197 A QHIN MUST execute a test of the *Nominal Flow* defined for each QHIN-to-QHIN transaction in Production on a quarterly (three-month) basis with all QHINs not transacted within the preceding three months. If one or more tests fail, the results MUST be immediately reported to the RCE, and corrections MUST be executed as per QTF-2 and communicated to the RCE.

QTF-198 When initiating a transaction per QTF-126 in Production, a QHIN may claim any Exchange Purpose within the transactions used for the connectivity test, including Treatment, as long as: (i) the patient record used in the transaction is a dummy record deliberately constructed so that it is reasonably expected not to match legitimate patient records; and (ii) the QHIN is acting in good faith to perform a test as required by the QTF and is not knowingly attempting to access data for a real patient.