FHIR-Based Exchange Implementation Guide - DRAFT

Version 2.0

Feb 1, 2024

Table Of Contents

Deleted:
... [1]

1. Introduction

This Implementation Guide outlines policy, technical, and process requirements for Implementers of the

FHIR-Based Exchange Use Case, under the terms of the Carequality Connected Agreement (CCA), and their Carequality Connections (CCs), under the Carequality Connection Terms.

The FHIR-Based Exchange Use Case addresses the need for FHIR Resources/Bundles containing relevant healthcare information to be made available to appropriate parties across the healthcare ecosystem. A hospital may need information held by a primary care physician, who in turn may need information from a specialist or emergency department. A payer may need information from any of these clinical settings. Government agencies may need information from private sector organizations. This Implementation Guide provides for flexibility across a wide array of access purposes and healthcare settings. Access to information for treatment purposes may have some additional requirements, but widespread exchange across a broad swath of permitted purposes is envisioned for this FHIR ecosystem. Sections 3-7 outline the policy and process requirements, while Sections 8-9 detail the technical pieces.

Deleted: 6

Deleted: 7

Deleted: 8

2. Roles

The concept of a role within this Use Case is central to this Implementation Guide and to defining the rights, obligations, and responsibilities of Carequality Implementers and CCs. Implementers and CCs play a declared role or roles, and Implementers must indicate to Carequality, during the application process for each use case, which role or roles the Implementer will fill, and which role or roles each of its CCs fill.

By default, any requirement specified herein applies to any Implementer or CC regardless of role. Requirements that apply only to those Implementers or CCs with a particular role or roles will clearly indicate the role or roles to which they apply.

An Implementer may fill different roles than its CCs, or may not actually fill any role at all. For example, an Implementer may provide network support, services, and oversight but play no direct role in the transactions specified for this Use Case. The only roles defined in this Use Case are those who initiate queries ("clients") and those who respond to queries ("servers").

2.1 Query Initiator

An Implementer or CC with the declared role of a Query Initiator institutes queries to retrieve information held by Implementers or CCs in the Query Responder role. An Implementer or CC with the declared role of a Query Initiator shall support the technical actor(s) specified in Sections 8-9 of this Guide and comply with any other requirements throughout this Guide that are specifically described as applying to the Query Initiator (client) role.

Deleted: 7

Deleted: 8

Deleted: ,

2.2 Query Responder

An Implementer or CC with the declared role of a Query Responder provides information in response to queries by Implementers or CCs in the Query Initiator role. An Implementer or CC with the declared role of a Query Responder shall support the technical actor(s) specified in Sections 8-9 of this Guide and comply with any other requirements throughout this Guide that are specifically described as applying to the Query Responder (server) role.

3. Customizable Principles of Trust

3.1 Permitted Purposes

Please refer to the Carequality Framework Policies document, section 3.1 found here:

Resources - Carequality

3.2 Full Participation

Please refer to the Carequality Framework Policies document section 3.2.

3.2.1 Treatment

Please refer to the Carequality Framework Policies document section 3.2.1

3.2.1.1 Provider Organizations Without Electronic Clinical Information

Please refer to the Carequality Framework Policies document section 3.2.1.1

3.2.1.2 Emergency Medical Services (EMS) Providers with Alternative Data Sharing Methods

Please refer to the Carequality Framework Policies document section 3.2.1.2

Formatted: Space After: 0 pt

Deleted: 7

Deleted: 8

Deleted: ,

Deleted: Carequality Implementers and Carequality Connections (CCs) represent a diverse set of stakeholders that wish to exchange health information for a variety of reasons. In order to establish trust, it is important to identify a shared set of acceptable reasons to initiate a query for information (Permitted Purposes). The Permitted Purposes for queries to be made under this Use Case are: ¶
1. Treatment ¶
2. Payment ¶
3. Health Care Operations ¶
4. Public Health Activities ¶
5. Patient Request ¶
6. Coverage Determination ¶
7. Other Authorization-Based Disclosures ¶
The first four terms are used as defined in the Health Insurance Portability and Accountability Act ("HIPAA") and its implementing regulations, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E, Standards for Privacy of Individually Identifiable Health Information, and 45 C.F.R. Part 164, Subpart C, Security Standards for the Protection of Electronic Protected Health Information. Public Health Activities are those permitted pursuant to 45 C.F.R. Part 164.512(b). ¶
An Implementer or CC may claim the Patient Request permitted purpose for queries that are directly initiated by the patient or the patient's personal representative as defined by 45 CFR 164.502(g), via a personal health record or other consumer-facing application. Note that any requests initiated by individuals other than the patient ... [2]

Deleted: ¶
Please refer to the Carequality Framework Policies document, section 3.1 found here:¶
Resources - Carequality¶

Deleted: It is important that all Implementers, CCs and their End Users understand that others are committed to participate in this Use Case so that all those who participate can realize value for their investment of time and resources. An Implementer or CC that plays the role of Query ... [3]

Deleted: Further, an Implementer or CC that plays the role of Query Responder for this Use Case, as defined in Section 2 of this Guide, SHALL provide information in response to valid queries for the Permitted Purpose of Patient Request, if the user making the request authenticates using vali ... [4]

Deleted: 2

Deleted: An Implementer or CC is considered to be an EMS Provider if its primary healthcare activity is patient transport with paramedic support. For clarity, taxi and other transport services lacking skilled support are not EMS Providers. Additionally, organizations providing patient transport ... [5]

3.3 Permitted Users

Implementers SHALL require users to be identity proofed at a minimum of Identity Assurance Level two (IAL2)[1] prior to issuance of credentials. Non-patient request users that are not identity proofed to IAL2, but were proofed to Level of Assurance three (LOA3)[2] and have maintained that level of identity proofing will be sufficiently identity proofed for Carequality. Exception: When using credentials from a data holder system for a Patient Request to that data holder, IAL2 identity proofing of the user by the client app operator is not required.

Formatted: Space After: 0 pt

Requests for equipment information via FHIR queries, including but not limited to bed availability, SHALL be restricted to agencies or authorities of a State, a territory, or a political subdivision of a State or territory, that are responsible for public health matters as part of their official mandate. Such agencies or authorities shall be responsible for identifying individuals within the agency or authority that SHALL have access to such data via a Carequality Implementer.

Formatted: Space After: 0 pt

When a user is authenticating to a datasource, the authentication MUST follow one of the two following flows:

1. The user MUST present the data source credentials provided by that data source and client app implementer MAY additionally present proof of IAL2 identity proofing of the user

2. The client app implementer which completed IAL2 identity verification of the user SHALL provide proof of IAL2 identity proofing and demographic attributes sufficient for a demographic match

For Patient Requests, a Query Responder(1) MUST accept its own credentials to allow exchange of data or (2) MAY accept IAL2 credentials plus demographic data as defined in 3.3.2 to allow exchange of data. When a Query Responder supports the latter method (2), the Query Responder SHALL NOT refuse to exchange data when sufficient demographic attributes have been provided to obtain an accurate demographic match.

3.4 Data Sufficiency and Integrity

Deleted: 3

Formatted: Space After: 0 pt

It is clear to all stakeholders that the health information stored in EHRs would be more easily transacted over data sharing networks if the information was better structured into universally accepted formats. As of 2024, these formats do not exist or, if they exist, they are not universally accepted. The clear goal of Carequality is to make progress toward greater structure over time. While that work is being done, Implementers that are Query Responders are allowed to decide whether they share information that

Deleted: 2

[1] NIST Special Publication 800-63-3 Digital Identity Guidelines, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[2] NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems, available at: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

the Implementer, or its CCs, hasn’t yet been confirmed as being accurate or clinically relevant. Some refer to the process of confirming the accuracy or clinical relevance of information as “vetting”. An Implementer that is a Query Responder may choose not to share with Query Initiators information that has not been vetted. A Query Responder that does respond to a query with information will assure that whatever information is sent is an accurate representation of the information contained in the responding system.

3.4.1 Provenance

Deleted: 3

Implementers SHALL use the Provenance Resource[3] as a means to define the source of the data.

3.4.2 Patient Matching

Deleted: 3

Query Responders SHOULD have the capability to return more than one potential patient match when the patient search yields more than one match. Query Responders SHALL NOT return more than one potential match when such action would be a violation of HIPAA or other Applicable Law, as with the Patient Request Permitted Purpose for example. When Query Initiators request only "certain" matches of operation $match (i.e. require “onlyCertainMatches”=true), Query Responders SHALL honor that request by returning only a unique match. Query Responders SHALL NOT return more than 100 potential matches when onlyCertainMatches is set to false. Query initiators SHOULD (to the fullest extent possible) normalize all patient demographic data elements according to USCDI standards before attempting to query. The lone exception to this rule is for address, which MUST conform to the USPS standard[4]. Queries for information MUST include all demographic parameters that are available and can be sent and are not constrained by local policy. Demographics SHOULD follow, at a minimum, USCDI defined demographics. [5] Query responders SHALL NOT require more than all USCDI demographics plus administrative gender before returning a patient list response.

3.4.3 Propagating Corrections

Deleted: 3

Implementers SHOULD propagate corrections, after the fact, upon discovery of sending an incorrect patient correlation. Example: Yesterday, a Query Responder sent John Smith as a patient match to a Query Initiator. Today, the Query Responder identified that Jake Smith was actually the correct patient for that query. Query Responders SHALL make all reasonable efforts to contact the Query Initiator, make it aware of the error, and provide the correct patient information.

[3] For information on the Provenance resource, see: https://www.hl7.org/fhir/provenance.html

[4] USPS Publication 28, Postal Address Standards, available at: https://pe.usps.com/cpim/ftp/pubs/Pub28/pub28.pdf

[5] *United States Core Data for Interoperability* (USCDI v1 Summary of Data Classes and Data Elements) - available at: https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

3.5 Secondary Use and Disclosure

Please refer to the Carequality Framework Policies document section 3.5

Moved (insertion) [3]

3.6 Patient Request – Identity Verification and Demographics

Please refer to the Carequality Framework Policies document section 3.6

Moved up [3]: 3.5 Secondary Use and Disclosure¶
Please refer to the Carequality Framework Policies document section 3.53.6 Patient Request – Identity

3.7 Best Practices

Deleted: ¶

Deleted: 4

While this guide does contain Service Level Agreements (SLAs), the following “Best Practices” SHOULD be followed and may be converted to SLAs at a later date. To the extent that Implementers or CCs discover that any of these Best Practices are impractical or would benefit from modification, Carequality should be informed promptly so that the feedback can be considered in the future conversion of these Best Practices into SLAs.

3.7.1 Error Responses

Deleted: 4

FHIR errors SHOULD use the OperationOutcome capability 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, such as via a retry operation due to the resource being busy, or a fatal error. Implementers MAY choose to obscure some of these details for security reasons. Any such choices SHOULD be linked to identified security concerns.

3.7.2 Version Compatibility

Deleted: 4

Implementers and Connections shall continue to support any capabilities previously supported for Carequality purposes under a particular FHIR version, until support for that FHIR version has been officially sunsetted by Carequality. Carequality will provide advance notice of such sunsetting and will collaborate with the Implementer community to develop reasonable timelines for such sunsetting.

3.7.3 Response times

Deleted: 4

Implementers SHOULD achieve the quickest response time possible per resource. Implementers MAY prioritize response times based on the Permitted Purpose and/or relevant metadata, if present, of the request.

3.7.4 Access Token Lifetime

Deleted: 4

Authorization Servers SHALL issue access tokens with a lifetime no longer than 60 minutes. An Authorization Server MAY also 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” scope, the refresh token lifetime SHALL be no less than three months unless a shorter lifetime aligns with applicable institutional policies.

3.8 Service Level Agreements (SLAs)

Deleted: 5

Carequality believes the following SLAs are reasonable and Implementers SHALL make every attempt to comply with them. However, because the industry has very limited experience with FHIR deployed across a national exchange ecosystem, Carequality will undertake a one-year evaluation of these SLAs. During the evaluation period and until otherwise determined by Carequality, a violation of the SLAs will not be treated as a breach of the Carequality Connected Agreement or Carequality Connection Terms. The one-year evaluation period will begin on the date of the first production transaction governed by the terms of this Implementation Guide. Upon completion of this evaluation period, Carequality MAY provide further guidance, adopt updates to the SLAs in a subsequent version of this Guide, or extend the evaluation period at its discretion.

3.8.1 Planned downtime

Deleted: 5

Implementers and CCs SHOULD schedule planned downtime for time periods with the lowest transaction volume, ideally after 3 a.m. Eastern Time and before 6:00 a.m. Eastern Time, as long as this time period in fact has the lowest transaction volume in the Implementer's or CC's experience with FHIR transactions enabled by Carequality. Downtime is considered to be "planned" if it occurs with at least 48 hours advance notice and SHALL be denoted as such in the Carequality Directory, once the necessary data fields are supported by the Carequality Directory and further guidance is provided in Carequality's Directory Policy. Planned downtime SHALL NOT be scheduled to exceed 72 hours, although Carequality acknowledges that downtime may last longer than anticipated when the downtime was planned, due to unexpected events.

3.8.2 Unplanned downtime notification

Deleted: 5

A CC MUST attempt to communicate an inability to respond to a request, for any reason, to its Implementer within a reasonable amount of time. An implementer MUST disseminate a CC's or Implementer's own inability to respond within a reasonable time of discovery of the outage via an update to their Carequality Directory record indicating their status (this requirement becomes operational only when the Carequality Directory supports such a status indicator.)

3.8.3 Uptime

Deleted: 5

Implementers SHOULD measure uptime on a monthly basis at the Gateway level. Such measurements should only take into account unplanned downtime. Implementers SHOULD strive to achieve 99.9% uptime. The proposed uptime for enforcement by a future SLA is 99.5%

3.9 The Role of Vendor App Stores

Deleted: 8

Notable in the value proposition discussion for Carequality is the lack of any mention of integration into user workflows within EHRs. Carequality can provide standardization and access to data, but does not provide any assurance of integration at the workflow level into an individual EHR. For some use cases, including virtually all use cases involving cross-organization exchange, access to the data is all that is needed. For many intra-organization use cases, however, there is a need for not only access to data, but meaningful integration at a workflow level with an organization's core IT systems.

Some EHR vendors have developed "app store" constructs to address this factor, with a process for vetting an app's ability to meaningfully interoperate with the EHR. For a subset of potential Carequality participants that can loosely be described as "provider apps", this process can be expected to continue to provide value independent of the value provided by Carequality. Stated differently, having access to data, while necessary, may not be sufficient to actually enroll users to request that data. The target users of provider apps are far more likely to adopt a product if it has been validated by the relevant vendor from a workflow and integration standpoint. For this reason, Carequality SHALL permit a vendor validation process, including the charging of fees by the vendor to those app providers who go through such a process, as long as the process carries no implication for data access via Carequality.

Deleted: ¶

Formatted: Don't keep with next, Don't keep lines together

4. Non Discrimination

Please refer to the Carequality Framework Policies document section 4

4.1 Non Discrimination – Treatment and Patient Request

Carequality has the goal of enabling widespread exchange of health information on a nationwide scale, between many partners who do not have any direct relationship with one another outside of Carequality. Recognizing that the time and effort required to reach individual contractual agreements, including those whose purpose is to define fee payment terms, between all of these potential partners can be a barrier to widespread exchange, Implementers and CCs cannot impose any additional fees, terms, or conditions on other Implementers or CCs with respect to queries/responses for treatment or patient request purposes. No additional agreements beyond the Carequality legal framework are allowed to be required in order to honor queries for these two permitted purposes.

With respect to treatment, the type of organization initiating the query is not a factor (although organizations claiming treatment must actually be providing treatment, or be making the request on behalf of a network member that is providing treatment.)

With respect to patient requests, Implementers MUST respond to these types of requests, if the request is successfully authenticated via OAuth. Honoring queries without credentials, i.e. based solely on demographics matching, will be permitted but not required. Additional policy details regarding patient requests are noted in Section 3.2 of this Implementation Guide.

4.2 Non Discrimination – Other Permitted Purposes

Please refer to the Carequality Framework Policies document section 4.2

4.3 Non Discrimination – Consistency in Additional Terms and Conditions

Please refer to the Carequality Framework Policies document section 4.3

4.4 Access and Patient Permission

Please refer to the Carequality Framework Policies document section 4.4

4.5 Record Locator Services

Not applicable for this Use Case.

5. Performance Measures

Not applicable for this Use Case.

6. Evidence of Compliance

Prior to implementing production connectivity for the workflows/transactions specified for this Use Case, each Implementer SHALL complete a non-production test with 3 other Implementers whose connectivity relies on software provided by a different technology vendor or provider (the Test Partner). Implementers who themselves do not play a role in this Use Case may designate a CC to perform the test, or perform the test using an internal environment as long as that environment has the same code base that will be delivered to the Implementer's CCs.

The non-production partner test will consist of successful execution of each transaction required for the role or roles declared by the Implementer as being played either directly by that Implementer or by its

Deleted: Implementers and CCs are permitted, but not required, to impose fees, terms and conditions on the Implementers or CCs with respect to queries or responses for any permitted purpose other than treatment and patient requests (as noted in section 4.1). Any fees, terms, and conditions must comply with the entirety of Section 4 of this Implementation Guide. ¶
Implementers that play the role of Query Responder are not REQUIRED to honor queries other than for the treatment or patient request permitted purposes. However, Query Responders may CHOOSE to honor queries for other permitted purposes. If a Query Responder does choose to honor queries beyond treatment and patient requests purposes, it must honor said queries (for that permitted purpose) from all Query Initiators, unless (i) to do so would violate applicable law; (ii) it has chosen to honor queries only from particular government agencies as further outlined in Section 4.3; (iii) it has chosen to impose terms and conditions on Query Initiators, and has not reached agreement on such terms and conditions with a particular Query Initiator, as further described in Section 4.3; or (iv) the permitted purpose is Other Authorization-Based Disclosures. ¶
For example, Peaceful Valley Hospital has received queries for John Smith's record from payers Acme Healthcare and Insure America for the purpose of payment. Peaceful Valley Hospital has a contract with Acme Healthcare outlining additional terms for the exchange, including data element requirements. Peaceful Valley Hospital may choose to honor payment queries from Acme Healthcare, but not Insure America, if Insure America has not agreed to similar terms, subject to the additional requirements of Section 4.3 b ... [6]

Deleted: If a Query Responder will accept a particular Policy Assertion(s) from one Query Initiator, it MUST accept that Policy Assertion(s) from any other Query Initiator for the same permitted purpose. This requirement applies equally to unsolicited Policy Assertions from the Query Initiator and to those assertions made after the Query ... [7]

Deleted: Non Discrimination – Access Policies

Deleted: Record Locator Services

Deleted: Query Responders are prohibited from enforcing different access policies based on attributes of the organization making the request. Stated differently, if a Query Initiator can legitimately claim a particular permitted purpose, the Query Responder must treat the request the same as any other for that permitted purpose, regardl ... [8]

Deleted: Resource Usage

Deleted: If an Implementer or CC updates its endpoints listed in the Carequality Directory for any reason other than FHIR version support, the Implementer or CC MUST continue to support transactions received at its previously listed endpoint(s) for a minimum of 14 days after upda ... [9]

Formatted: Font color: Auto

CCs. The success of the test will be at the discretion of the Test Partner, but Test Partners SHOULD NOT report success unless each transaction has been completed and data returned to the other party in that transaction. Specifically, matching patient data MUST be found, at least one FHIR resource MUST be available, and one or more resources MUST be retrieved. Data should be coordinated among the test partners such that patient matching is successful. Upon completion of the test to the Test Partner's satisfaction, the Test Partner will independently inform Carequality that the Implementer's non-production partner test was successfully completed.

After completing the non-production partner test and meeting the applicable requirements of the Carequality Application Process, an Implementer MAY configure its production system for connectivity via the transactions specified for this Use Case. Prior to being recognized as a live Implementer of this Use Case, the Implementer must complete connectivity validation in production. Until this validation is successfully completed, Implementers are not considered live and MAY NOT claim such status. Further, until this validation process is successfully completed, other Implementers are not obligated to engage in exchange activities with the Implementer, other than those required for the connectivity validation as described in this Section.

The connectivity validation will consist of two steps. In the first step, basic connectivity is confirmed through authentication. Implementers in the Query Initiator role, or who support CCs in the Query Initiator role, must then be able to retrieve a FHIR resource with at least 50% of all other live Implementers. The aforementioned Initiator requirements/validation rules also apply to Implementers in the Query Responder role.

7. Directory Requirements

Please refer to the Carequality Framework Policies document section 7.

7.1 Resource Usage

If an Implementer or CC updates its endpoints listed in the Carequality Directory for any reason other than FHIR version support, the Implementer or CC MUST continue to support transactions received at its previously listed endpoint(s) for a minimum of 14 days after updating its endpoints in the Carequality Directory.

8. Use Cases/Workflows

8.1 Patient Discovery

Assumptions:

- The Query Initiator knows a sufficient number of the patient's demographics for a successful match
- The Service Directory has all endpoints for the Query Responder
- The user is either a Healthcare Provider or other Healthcare system user with acceptable Purpose of Use, or, a Patient/Caregiver with allowed access to the Patient record
- If a Patient/CareGiver is using Query Responder portal credentials, those credentials have been granted to that user and sufficient identity proofing has been done by the Query Responder prior to granting the credentials

Nominal Flow:

1. The workflow begins when the Query Initiator queries the Carequality Service Directory for the Endpoint and information for the Query Responder.
2. If the Query Initiator does not have a valid client_id for use with the Query Responder, then:
    a. The Query Initiator asserts a dynamic registration to the Query Responder authorization server providing their Carequality certificate, a software statement and other JWT metadata as per section 9.3.3. The Query Initiator's Purpose of Use matches one of those listed in the Query Initiator's Service Directory Entry and is one supported by the Authorization server, if required.

    b. The Authorization Server returns the client_id assigned or, in case of renewal, re-assigned according to the capabilities of the server.
3. Query Initiator, using the provided client_id, requests an access token as per Section 9.3.4 or 9.3.5. The request includes, as part of the authorization extension object, one of the six supported NHIN Purpose of Use codes. If the authorization_code grant type is used as specified in Section 9.3.4, the credentials supplied follow one of the two following options:
    a. The Query Initiator provides the user credentials and may include proof of IAL2 proofing. These credentials are accepted by the Query Responder and an access token is granted

b. If supported by the Query Responder, the Query Initiator provides proof of IAL2 identity proofing and all known demographics

  i. If the Query Responder does not accept demographic authorization, the Query Responder will return a Invalid Request error.

  ii. If supported, the Query Responder executes a user match against the demographics collected by the Query Responder out of band and one of the following outcomes occurs:

    1. Accepts the match and proofing as sufficient for access and grants an access token.

    2. Requests additional demographics from the Query Initiator. In this case, the Query Initiator may collect and provide further demographics and re-initiate the access request.

    3. Deny the access request due to insufficient confidence in the user demographic match. The workflow ends.

4. The Query Initiator executes a Patient search using the $match operation as per Section 9.5.2

   a. Patient Resource includes all known demographics. The following optional results may occur

      i. The Query Responder returns the requested Patient Resource identifier

      ii. The Query Responder rejects the request, requiring additional demographics. In this case, the Query Initiator can collect and provide further demographics and re-initiate the query

5. The Query Initiator, once the Patient search has been successfully executed, begins an Information Query

6. An audit log of the request is made by both the Query Responder and Query Initiator

Alternate flow 1: The Query Initiator includes Access Consent

1. The Query Initiator includes, as part of their access request, an Access Consent Policy as follows:

   a. The acp element includes OID as appropriate from Policy Assertion Table in Section 4.4 of the Carequality Framework Policies Document

   b. The acp_reference element includes a link to a Consent or DocumentReference resource which holds the information as needed according to the OID in the acp field.

   c. One of the two following results occurs:

      i. The ACP is accepted and the access token returned

    ii. The ACP is not accepted and, as part of the response, an OID from the Policy Assertion Table in Section 4.4 of the Carequality Framework Policies Document and a URL to the appropriate policy or form required is returned, indicating further or different requirements.

2. The workflow continues.

Post Conditions:

- The Query Initiator has an access token necessary for a follow-up information query.
- The Access Token is valid for the period as per section 9.3.5.

8.2 Information Query

Assumptions:

- The Query Initiator has fulfilled the requirements of Section 8.1 and has a valid access token.

Nominal Flow:

1. The Query Initiator queries the Query Responder for their FHIR server's CapabilityStatement.
2. The CapabilityStatement is checked against the Query Initiator's requirements for Resource, Profile and FHIR Implementation Guide requirements. The following options result:
    a. No match between the Query Initiator's requirements is found, the workflow ends The Query initiator may need to contact the Query Responder out-of-band to resolve the mis-match or may need to fall back to core/US Core profiles for the information needed. How this is done is out of scope for this IG.
    b. The CapabilityStatement matches, in whole or in part, the requirements and the workflow continues.
3. The Query Initiator executes query(ies) for the information regarding the Patient queried in Section 8.1 as limited by the scopes in the software statement provided in the authorization request.
4. The Query Responder returns Resources that match the Query Initiator's request.
5. An audit log of the request(s) is made by both the Query Responder and Query Initiator.

Post Conditions:

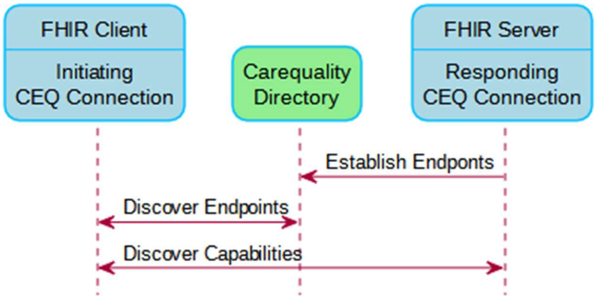
The Query Initiator has the information needed for proper patient care.

9. Infrastructure

9.1 FHIR Endpoints

To enable a lookup of Carequality Connections that support HL7® FHIR® based access and exchange, Carequality needs to establish a common place to query for such information. Carequality SHALL deploy a single Carequality FHIR directory to be utilized for all Use Cases (including this FHIR Use Case IG) instead of spinning up a brand new directory for FHIR. A value SHALL be added, called "FHIR R4", to the existing directory extension named "UseCases." This will allow Implementers to distinguish between all other Use Case endpoints and FHIR based endpoints.

The FHIR CapabilityStatement resource SHALL be used to define the FHIR capabilities for an endpoint. This CapabilityStatement will only be made available by the server and will not be copied into the Carequality Directory. This approach will minimize redundant data and associated maintenance, thus reducing out-of-date/sync capability statements while reducing the number of centralized points to establish a connection that could fail. Further implementation experience MAY yield adding other data to the Carequality Directory, but that will be addressed later based on implementation feedback.



Link to Directory IG: https://carequality.org/healthcare-directory/index.html

9.2 Discovery of Endpoint Capabilities

Discovery of Endpoints shall be executed by a query to the Carequality directory service which will have the FHIR endpoint(s) for the implementers and connections. If multiple endpoints exist for an implementer or connection, the CapabilityStatement for each endpoint would list the capabilities of the instance. Carequality Implementers supporting the FHIR-Based Exchange Use Case shall deploy at least one FHIR CapabilityStatement that is publicly discoverable, where CapabilityStatement.kind="instance", and is supported/endorsed by Carequality. Implementers must also support at least one FHIR resource per Capability Statement that they deploy.

9.3 Authentication/Trust

The goal is to establish an approach that supports establishing trust at scale, i.e., when an organization is ready to become a Carequality Connection endpoint for FHIR based access/exchange, there should be minimal steps for that connection and implementer to “connect” that organization to Carequality, while connecting to existing Carequality Connections that can use FHIR.

To support scaling of authentication, Carequality will deploy a decentralized authentication approach where the Carequality Implementer establishes one or more authorization servers to support their connections or may share an authorization server with one or more other Carequality Implementers.

Carequality trusted X.509 certificates will be used to enable establishing trust of the calling application. Note that no “client secret” will be utilized as part of this approach as interactions described above using the Carequality certificate sufficiently enable the server to assess whether the calling application is trusted and that trust has not expired.

9.3.1 Carequality Certificates

Introduction

The Use of Carequality certificates for the FHIR ecosystem SHALL conform to the certificate policy and profile requirements described in the Carequality Technical Trust Policy, with the additions and exceptions as noted below.

Issuance

Certificates used for FHIR exchange SHALL be chained to Carequality trust anchor certificates. For Implementers requiring 100 (or more) certificates, they may establish, or subcontract to a third party, a Certificate Authority for issuance of certificates to their Connections. The Implementer will be issued a single certificate to be used as an intermediate CA certificate within their own Certificate Authority. For Implementers requiring fewer than 100 certificates, Carequality may act as the Certificate Authority for all Connections or the Implementer may establish their own Certificate Authority and use an intermediate CA Certificate issued from a Carequality trust anchor to issue Certificates to their Connections. Certificate Authorities set up by Implementers will be required to follow industry best practices for creation and management of the CA as outlined in section 9.3.2 below and are subject to audit by Carequality or its designated representative.

Certificates SHALL be issued to the Implementer or Connection responsible for the security of a FHIR Application, as determined by the Implementer’s deployment model, also referred to as the Operator. A FHIR Application is a client application and/or a service that makes or responds to requests described in this guide.

If multiple instances of the same application are secured by different Operators, then each Operator MUST be issued a separate certificate. However, for convenience, a single Operator MAY group various client and/or server functions together as a single Application using a single certificate, or divide them into separate Applications using separate certificates, subject to the restrictions below. Depending on organization policy, certificates issued to a single Operator MAY be issued on a per-organization basis (e.g. when one Operator secures the same application on behalf of multiple organizations) or MAY be issued more granularly on a per-application basis (e.g. when one Operator wishes to use separate certificates for software components that run on different servers or perform different functions).

Note that grouped software components that share one certificate will be treated as one application by Authorization Servers and, thus, MUST be able to use a single client_id assigned by the Authorization Server. If using a single client_id is not practicable, then using separate certificates for each component would be an appropriate alternative.

For organizations that use individual client ids per client Purpose of Use, the Implementer MAY assign multiple Subject Alternate Names (SANs) for each certificate issued to a Connection. This would allow for the SAN field + the iss key within the JSON Web Token (JWT) to uniquely identify each client and purpose of use pair. Each certificate could be used to represent multiple client_ids for one client who has multiple purposes of use. A request would indicate which unique client it was for by the iss key URI, which would match one of the SANs listed in the certificate.

TLS certificates used in the Carequality QBDE environment SHALL NOT be used by FHIR Applications.

Structure

The value of the Common Name SDN attribute SHALL be a human readable name for the Application as provided by the Operator. The Operator's legal business name, city, and state SHALL be included in the Subject Distinguished Name (SDN) of the certificate as the values of the Organization, Locality, and State attributes.

The Operator and the FHIR Application SHALL be jointly identified by a unique URI listed in a uniformResourceIdentifier entry in a certificate's Subject Alternative Name (SAN) extension, i.e. each Carequality certificate is issued in the context of an Operator and an Application. If a Carequality certificate is used to secure an https service endpoint, then the host's DNS name SHALL also be included in the SAN extension as a dnsName entry. However, Implementers MAY also use a separate Internet TLS certificate issued from a well-known CA trusted by common browsers and bound to the server DNS host name to secure their TLS endpoint.

Responders (servers) and Initiators (servers) SHALL have a subject key that is an RSA key (2048 bit). Clients MAY also utilize a subject key that is an elliptic curve key (P-256 or P-384 curves). Note, however, that servers are NOT required to support elliptic curve signatures at this time, so clients may need to fall back to their RSA key if the server does not support elliptic curve keys.

Server Considerations

On the server side, Carequality Implementers can deploy as either a single-tenant gateway or multi-tenant gateway. In the single-tenant case, there is a one-to-one relationship between X.509 certificates and Carequality Connections (CCs). In the multi-tenant case, where a single certificate is used and there is more than one CC per host, the Implementer SHALL be identified as the Operator. Both scenarios are allowed.

A Carequality Implementer with multiple CCs hosted behind a single gateway MAY be deployed with only one certificate for all of their CCs. In this case, a single certificate will be issued for that Implementer and that Implementer will be entered into the Directory. Subsequently, as that Implementer's CCs become ready to exchange, each CC will be added to the Directory, but no additional certificate will need to be issued since it is behind the same gateway. Stated differently, multi-tenant scenarios will result in one Carequality Directory entry per CC.

Unlike the SOAP-based QBDE transactions in which a client authenticates to the server during a mutual TLS handshake with the server, client authentication for the workflows described in this guide is achieved using tokens that are digitally signed by the client as described in section 9.3.2. Thus, a server SHALL NOT additionally require client authentication at the time of the TLS handshake to access the OAuth 2.0 and FHIR endpoints identified for these workflows.

9.3.2 Carequality Authorized Implementer Certificate Authority

All certificates issued by a Carequality Authorized Implementer Certificate Authority (CAICA) must follow the requirements as stated in this document and conform to applicable published Carequality Certificate Profiles for this purpose.

CA Certificate Requirements

All certificates issued by the CAICA should have a minimum key size of 2048 bits for RSA keys and 384 bits for Elliptic Curve. Certificates should be valid for a maximum of 3 years.

All Device Certificates issued by the CAICA SHALL be chained directly to the CAICA intermediate certificate provided by Carequality. In other words, no additional subordinate intermediate certificates may be issued by the CAICA or used within the authentication chain. To promote interoperability in the early stage, entities signing JWTs that will be validated by relying parties using certificates issued by a CAICA SHOULD include both the end entity certificate and CAICA intermediate certificate in the x5c header of the JWT.

A CAICA SHALL implement a publicly available certificate revocation list (CRL). All revoked certificates SHALL be added to the CRL in accordance with the requirements of the applicable Certificate Policy.

CA Roles

Role of CA Administrator and Certificate Officer SHALL be separate and SHALL be held by distinct individuals.

Role	Security permission	Description
CA Administrator	Manage CA	Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate.
Certificate Officer	Issue and Manage Certificates	Approve certificate enrollment and revocation requests. This role is sometimes referred to as Certificate Manager or CA Officer.

CA Administrator SHALL NOT be able to approve new certificates or revocations.

CAICA Certificate Enrollment Requirements

An authorized representative of Carequality Implementer or Connection to provide to the CAICA the following information:

- Equipment identification (e.g., Health Domain Name, DNS name, Device identifier, or Health Endpoint Name associated with Device);
- Equipment Public Keys;
- Equipment authorizations and attributes (if any are to be included in the Certificate); and
- Contact information.

This information must be available to Carequality or its Agent upon request.

Registration of a Device SHALL also include identity proofing of the authorized representative of the Sponsor to an assurance level commensurate with the Certificate assurance level IAL2.

9.3.3 Use of JWT Signatures

This guide makes use of the JSON Web Token (JWT) and JSON Web Signature (JWS) specifications to create digitally signed JWTs that establish the authenticity of participants requesting client registration or client authentication. All JWTs defined in this guide MUST be constructed in accordance with the requirements of Section 1.2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

9.3.4 Scope Negotiation

Commented [DP1]: This is a copy of the scopes doc that was worked on starting in the May 2023 Connectathon. It is the prose version of the constraints used in TEFCA Facilitated FHIR

Discovery

The discovery process, automated in UDAP, sets a baseline for the accesses to be requested by applications. The scopes supported OAuth metadata entry must be present and will give a specific list of possible scopes and should include wildcard entries, if supported. This ensures that a client application does not request wildcard access when wildcards are not supported. This discovery process should be segregated by community if possible through a queryable section in the UDAP file. An application should parse the scopes supported prior to any registration request.

Registration

During the registration for client credentials code grant, the client should request only those scopes that are necessary for the application to run successfully but may be more than needed by any one application if the registration will be used for more than one application.

A client should only request a wildcard scope if wildcards are specified in the scopes supported metadata list. If a wildcard scope is specified and the server supports wildcards, the server may respond with either the wildcard or with an exploded list of scopes that the client has been granted. If wildcard scopes are not supported, the server should respond with an “invalid scope”.

The server may respond with fewer scopes than requested if the application cannot have a scope specified in the registration code grant or the server does not recognize one or more of the requested scopes. The server should only respond with “invalid scope” if the wildcard is requested and not supported, or if none of the requested scopes are supported. It is also possible that a

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.

Code Grant

Minimum Necessary[6] as specified with HIPAA is a required guidance for all access requests in the United States. The server is not required to audit the requests for minimum necessary. It is fully the responsibility of the application to only request the minimum necessary set of scopes needed for the application to succeed. This scope list may be the same as the list from registration or may be a subset.

As with all requests a Grant time request may result in a full or subset of the requested scopes. The application should also 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.

[6] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html

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.

9.3.5 Client Registration

Deleted: 4

These requirements are based on Unified Data Access Profiles as specified in the HL7/UDAP Scalable Registration, Authentication, and Authorization FHIR IG.

Before proceeding, the Initiating Carequality Connection’s solution MUST have been registered with the Responding Carequality Connection’s authorization server. This process MUST be scalable and MUST NOT require manual steps for every Responding Carequality Connection’s authorization server. Carequality Implementers SHALL support dynamic registration as described in section 2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG to enable the necessary scaling without manual intervention. Carequality participants MUST register their applications with the authorization servers that protect the FHIR servers with whom they wish to exchange data. Beyond establishing details about application names and ownership, registration also establishes intended authorization workflows and FHIR resources that they wish to exchange.

9.3.5.1 Dynamic Registration

Carequality FHIR implementation does not allow for Public clients, which do not have a private key, in this version. Future versions of the Guide may allow for this use case. Two use cases are currently supported:

1. Confidential clients: Conventional server-based web applications that can maintain a secret,
2. Backend services: for business-to-business connections, backend services can access data directly, without a user directly in the loop.

9.3.5.2 Registration API

Deleted: 4

Deleted: 1

Discovery

A FHIR Server MUST make its UDAP server metadata, including the Authorization Server’s authorization, token, and registration endpoints, available to client applications as per Section 2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

Required UDAP Metadata

The metadata returned from the UDAP metadata endpoint defined above SHALL conform to the requirements listed in the table below and SHALL represent the server’s capabilities for the workflows described in this guide. Additional required metadata elements defined in Section 2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG SHALL also be populated. For elements that are represented by arrays, returning an empty array SHALL be interpreted by clients to mean that the corresponding capability is NOT supported by the server.

The following are requirements specific to Carequality. All other parameters are listed within the HL7/UDAP FHIR IG

scopes_supported	required	An array of one or more strings containing scopes supported by the Authorization Server. The array MUST contain all wildcard scopes supported. The server **MAY** support different subsets of these scopes for different client types or entities. Example for a server that also supports SMART App Launch v1 scopes: ["openid", "launch/patient", "system/Patient.read", "system/AllergyIntolerance.read", "system/Procedures.read"]

Software Statement

The software statement is a JWT signed by the client using the private key that corresponds to the public key listed in its X.509 certificate. The software statement is constructed as per section 3.1 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG. The client signs the software statement using one of the RS256, ES256, RS384, or ES384 signature algorithms as defined in RFC 7518; the algorithm used will depend on whether the client app's X.509 certificate contains an RSA or EC key. All implementations SHALL support RS256, SHOULD support ES256, and MAY support ES384 and RS384.

Inclusion Of Certifications And Endorsements

This model supports the optional certifications framework outlined in HL7/UDAP FHIR IG Sec 3.3 Inclusion of Certifications and Endorsements. Operators of consumer-facing applications MAY include a self-signed certification as defined by the Carequality Consumer-Facing App Certification Profile. Please follow the link for more details. Carequality may publish additional certification profiles.

Request Body

The registration request is submitted by the client to the Authorization Server's registration endpoint as per section 3.2.3 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

9.3.5.3 Carequality Basic App Certification Profile

The certification JWT included by the client app MUST conform to the header requirements in Section 9.3.3 and the Carequality specific claims requirements in the following table:

Deleted: udap_versions_supported ... [10]

Deleted: recommended

Deleted: authorization_endpoint ... [11]

Deleted: The unique client URI used for the 'iss' claim SHALL match the uriName entry in the Subject Alternative Name extension of the client app's X.509 certificate. The software statement is intended for one-time use with a single OAuth 2.0 server. As such, the 'aud' claim SHALL list the URL of the OAuth Server's registration endpoint, and the lifetime of the software statement ('exp' minus 'iat') SHALL be 5 minutes.¶

Formatted: Font color: Auto

Deleted: UDAP Certifications and Endorsements for Client Applications

Moved (insertion) [1]

Moved (insertion) [2]

Field Code Changed

Deleted: Authorization Servers MAY support the inclusion of certifications by Application operators. Authorization Servers SHALL ignore unsupported or unrecognized certifications, i.e., the inclusion of an unsupported or unrecognized certification SHALL NOT be a reason for an Authorization Server to return an error response. ¶
Authorization Servers MAY require client apps to include one or more certifications that are referenced in this guide in a registration request. If a certification is required, the Authorization Server SHALL communicate this by including the corresponding certification URI in the udap_certifications_required metadata element defined above.

Moved up [1]: Operators of consumer-facing applications self-signed certification as defined by the Carequality Consumer-Facing App Certification Profile. We welcome Early Adopter feedback to this documentation. Please follow the link for more details. Carequality may publish additional certification profiles.¶

Moved up [2]: Please follow the link for more details. Carequality may publish additional certification profiles.

Deleted: This guide defines the Carequality Basic App Profile in Section 9.3.4.2. Application operators MAY ... [12]

Deleted: `POST /register HTTP/1.1¶`
`Host: as.example.net¶` ... [13]

Deleted: 4

Deleted: 2

Deleted: In most cases, the Application Operator will provide additional authorization metadata to the dat ... [14]

Deleted: 3

Deleted: 2

Carequality Basic App Certification JWT Claims		
certification_name	required	String with fixed value: "Carequality Basic App Certification"
certification_uris	required	Fixed array with single string element: ["https://wiki.carequality.org/udap/profiles/basic-app-certification"]
extensions	required	A JSON Object containing the key "carequality" with a value equal to a Carequality Authorization Extension Object, as defined in Section 9.3.5, with the additional requirements discussed below.

When an Application Operator includes a Carequality Basic App Certification in its registration request, an Authorization Server MAY reject subsequent token requests by this app that contain authorization metadata that does not match the corresponding values declared in the certification. In addition, an Authorization Server MAY require that one or more elements of the Carequality Basic App Certification, such as purpose_of_use, be supplied at registration time. Authorization servers that reject a registration request due to a missing element SHOULD respond with an informative error identifying that element.

9.3.5.4 Modifying Registrations

Such requests SHALL be processed as described in Section 3.4 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

9.3.6 Authorization Code Grant Type (3-legged OAuth 2.0)

Applications that wish to exchange data with a FHIR server must authenticate and authorize themselves and their users with an Authorization Server first in order to obtain an FHIR access token. This flow can vary depending on whether an application is a public app or a confidential app. This section will outline the flows for user-facing applications. Only confidential apps are supported in this version of this guide. Clients and servers MAY optionally support UDAP Tiered OAuth for User Authentication.

A responder SHOULD indicate support or lack of support for the Carequality User extension object by including or omitting the "carequality_user" key from its list of supported authorization extension objects in its UDAP metadata. If a responder does not support this extension object, it MAY ignore the associated metadata. Alternatively, if the responder has explicitly indicated in its UDAP metadata that this extension object is not supported, it MAY instead return an invalid_request error response for a token request containing this extension object.

Deleted: iss ... [15]

Deleted: For the purposes of this certification profile, inclusion of the 'version' element of the Carequality Authorization Extension Object defined in Section 9.3.5 SHALL be required. However, inclusion of all other extension object elements SHALL be optional for this certification profile. Specifically, the App Operator MAY include only those extension object keys whose values will not vary across subsequent token requests. For example, if all subsequent data requests by the App will be made by one organization and only for the purpose of treatment, then the 'organization_id', 'organization', and 'purpose_of_use' keys and the corresponding values could be included in the Carequality Authorization Extension Object within this self-declaration. Elements whose value may vary in subsequent token requests SHALL NOT be included in this certification. An App Operation SHOULD NOT submit a Carequality Basic App Certification with the authorization object containing only the 'version' element, as such a certification provides no additional information to the data holder's Authorization Server.

Deleted: 4

Deleted: 3

Deleted: The client URI in the Subject Alternative Name of an X.509 certificate uniquely identifies a single application and its operator over time. 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. Note that this may be a different certificate than the one used in the previous registration, such as in the case of certificate renewals or re-keyings. The registration request SHALL include all parameters required for a new registration and all parameters for which modification is requested.

Deleted: If the Authorization Server returns a different client_id in the registration response, the client application SHALL use only the new client_id in subsequent transactions with the Authorization Server.¶

Deleted: 5

Deleted: 9.3.5.1 Obtaining an Authorization Code¶
The client application SHALL obtain an authorization code as per the profile outlined by the HL7 SMART App Launch Framework at: http://hl7.org/fhir/smart-app-launch/#step-1-app-asks-for-authorization¶
9.3.5.2 Obtaining an Access Token¶
The approach for confidential clients will follow the procedure defined in Section 4 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.¶ ... [16]

Deleted: is

The authentication JWT submitted by the client app MUST conform to the requirements in Section 4.2.1 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG. If the "carequality_user" authorization extension object is used by the client, the client SHALL additionally include an “extensions” claim in the authentication JWT containing this authorization extension object, as per the UDAP JWT-Based Client Authentication profile.

Table 1 Carequality User Authorization Extension Object

Extension Name: “carequality_user”		
version	required	Fixed string value: "1"
purpose_of_use	required	Fixed array with one string element: ["urn:oid:2.16.840.1.113883.3.18.7.1#REQUEST"] The purpose for which the data is requested, from the code set of permitted purposes in the NHIN PurposeOfUse code system as per Section 3.1 of the Carequality Framework Policies Document.
user_information	Required	FHIR US Core Patient resource with all known demographics.
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 section 4.4 of the Carequality Framework Policies Document 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"] to represent identity proofing of the user at IAL2

Deleted: ¶
If the responder supports the use of the Carequality User Authorization Extension object, the responder is responsible for validating that verified user identity metadata submitted by the application reasonably matches the responder’s own records for the app user that was authenticated by the responder before issuing an access token. If the data holder cannot validate the user information, it SHALL return an invalid_grant error in response to the token request.¶
¶

Formatted: Caption, Keep with next

Deleted: **Carequality User Authorization Extension object**

Commented [DP2]: The TEFCA version uses the FHIR US Core Patient Resource instead of the individual fields

Deleted: user_person ... [17]

Commented [DP3]: Create IAS extension with user info RelatedPerson for user, patient info separate field, Patient for patent

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://implementer1.example.com/fhir/R4/DocumentReference/consent-12345"]

The parameters for the POST request to the Authorization Server's token endpoint MUST conform to the requirements of section 4.2.2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

Servers SHALL process and respond to such token requests as per Section 4.2.2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG. If the Authorization Server issues a refresh token to an application that has requested and has been authorized to use the "offline_access" scope, the refresh token lifetime SHALL be no less than three months unless a shorter lifetime aligns with applicable institutional policies. If an application that has requested and has been authorized to use the "offline_access" scope presents a valid refresh token to an Authorization Server to obtain a new access token, the Authorization Server SHOULD also issue a new refresh token valid for a new period of no less than three months unless a shorter lifetime aligns with applicable institutional policies.

9.3.7 Client Credentials Grant Type (2-legged OAuth 2.0)

For this workflow, clients and servers SHALL conform to the requirements for use of client credentials grants in Section 5 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

Since users do not interact directly with the data holder's authorization endpoint when using the client_credentials grant type, clients provide additional authorization information to the data holder at the time of the token request by adding this information to the authentication JWT in the form of the B2B Authorization Extension Object, as defined in Section 5.2.1.1 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG. The table below defines Carequality-specific values for the B2B Authorization Extension Object that SHALL be followed in addition to the requirements defined in the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.

Table 2 Carequality-specific Values for the B2B Authorization Extension object

Extension Key Name: "hl7-b2b"

Deleted: ¶
Non-normative example (white space and line breaks added for clarity, not URL-encoded):¶
¶
Request:¶

```
POST /token HTTP/1.1¶
Host: as.example.com¶
Content-type: application/x-www-form-
urlencoded¶
¶
grant_type=authorization_code&¶
  code=authz_code_from_resource_holder&¶

client_assertion_type=urn:ietf:params:oa
uth:client-assertion-type:jwt-bearer&¶
  client_assertion=eyJh[…remainder of
AnT omitted for brevity…]&¶
  udap=1¶
¶
```

Response (success):¶

```
HTTP/1.1 200 OK¶
Content-Type: application/json¶
¶
{¶
   "access_token":
"example_access_token_issued_by_AS",¶
   "token_type": "Bearer",¶
   "expires_in": 3600¶
}
```

Page Break

¶

Deleted: 6

Deleted: Privileged applications acting on their own behalf, or without direct user action required via the data holder's authorization endpoint, use the client_credentials grant type. In this flow, the authorization endpoint is not used and the application communicates directly to the token endpoint.

Deleted:

Deleted: ¶

Deleted: **Carequality-specific Values for the B2B Authorization Extension object¶**

version	required	Fixed string value: "1"
organization_id	required	String containing the URL of requestor’s Organization resource at the Carequality Directory server:https://prod-dir-ceq-01.sequoiaproject.org/fhir-stu3/1.0.1/ "https://https://prod-dir-ceq-01.sequoiaproject.org/fhir-stu3/1.0.1//Organization/2.16.840.1.113883.19.347473"
purpose_of_use	required	An array of one or more strings, each containing a purpose for which the data is requested, from the code set of permitted purposes in the NHIN PurposeOfUse code system as per Section 3.1 of the Carequality Framework Policies Document: TREATMENT | PAYMENT | OPERATIONS | PUBLICHEALTH | REQUEST | COVERAGE
consent_policy	optional	The Access Consent Policy Identifier corresponding to the asserted Access Policy, array of string values from the list of valid policy OIDs in section 4.4 of the Carequality Framework Policies Document, each expressed as a URI, e.g. ["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.1"]
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://implementer1.example.com/fhir/R4/DocumentReference/consent-12345"]

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 data holder requires one or more Access Consent Policies to be asserted but the requestor has omitted the acp parameter or has asserted a policy that is not acceptable to the data holder, then the Authorization Server SHALL return an invalid_grant error response to the token request, and this error response SHOULD include the B2B Authorization Extension Error object in the 'extensions' object of the error response.

Table 3 Carequality-specific Values for the B2B Authorization Extension Error object

Deleted: ¶

Deleted: Carequality-specific Values for the B2B Authorization Extension Error object

Extension Name: "hl7-b2b"		
consent_policy	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 section 4.4 of the Carequality Framework Policies Document, each expressed as a URI, e.g. ["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.1"]
consent_form	optional	A URL as a string where the required consent form may be downloaded, if applicable, e.g. "https://implementer1.example.com/consentForms/sample1.pdf"

Responders supporting use cases that require transmission of consent information SHALL support the consent and consent_reference claims and SHALL be able to resolve a DocumentReference or Consent resource included in the consent_reference array.

If the requested purpose of use is not supported by the responder, the responder SHALL return an invalid_grant error response to the requesting application.

Patient Requests

Responders MAY support the client credentials grant type for Patient Requests (i.e. where the purpose_of_use code is REQUEST) but are not required to do so. This corresponds to authorization workflow (2) defined in Section 3.2. If the responder does support this workflow, the responder SHALL support the Carequality Patient Request Authorization Extension object, defined below and identified by the extension key "carequality_patient".

Extension Name: "carequality_patient"		
Element	**Optionality**	**Requirement**
version	Required	Fixed string value: "1"
purpose_of_use	Required	Fixed Value "PATIENT".
user_information	Required	FHIR RelatedPerson resource with all known demographics. Where the user is the patient, the value of the relationship element SHALL be "ONESELF"
Patient Information	Required	FHIR US Core Patient resource with all known demographics
lal_vetted	Conditional	OIDC token provided by Identity Verifier when the Identity Verifier is not the Responding Source. Responding server MAY respond with invalid_grant if missing.
consent_policy	Required	The Access Consent Policy Identifier corresponding to the asserted Access Policy that represents the identity proofing level of assurance of the user, array of string values from the subset of valid policy OIDs in section 4.4 of the Carequality Framework Policies Document that represent identity proofing levels of assurance, each expressed as a URI, e.g. ["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.1"]
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.

Deleted: User

Deleted: in Section 9.3.5.2

Deleted: user

Commented [DP4]: Create IAS extension with user info RelatedPerson for user, patient info separate field, Patient for patent

Commented [DP5]: Not sure if this is part of the CEQ Patient Request setup

		["https://implementer1.example.com/fhir/R4/DocumentReference/consent-70796b65"]

A client application requesting a token for Patient Requests using the client credentials grant type SHALL include the Carequality Patient Authorization Extension Object in its token request as well as the B2B Authorization Extension object. The user metadata submitted by the requesting application in the Carequality User extension object SHALL correspond to the verified identity attributes of the permitted user (verified as per Section 2.2) who is making the request. Note that this user is not necessarily the patient who is the transaction subject, i.e., the verified user MAY instead be a patient's authorized representative. Before issuing an access token, the responder SHALL validate that the verified user identity metadata submitted by the application matches the responder's own records for a person that is authorized to make patient requests in accordance with Section 3.2 and SHALL limit the patient data accessible using the access token accordingly. 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 SHALL return an invalid_grant error in response to the token request.

Deleted: User

Deleted: instead of

Example:

Below is an example of complete authentication JWT header and claims with authorization information prior to Base64URL-encoding and signing (non-normative, the "." between the header and claims objects is a convenience notation only):

```
{
   "alg": "RS256",
   "x5c": ["MIIEczCCA1ugA…remainder of Base64 encoded certificate
omitted for brevity…"]
}.{
   "iss": "myClientID",
   "sub": "myClientID",
   "aud": "https://implementer2.example.net/token",
   "exp": 1557843252,
   "iat": 1557843852,
   "jti": "Q1E6g2PY91nmj5bSJJ-CZQ",
   "extensions": {
      "hl7-b2b": {
         "version": "1",
         "subject_name": "Dr. Mary Johnson",
         "subject_id": "urn:oid:2.16.840.1.113883.4.6#1234567890",
         "organization_name": "ABC Hospital",
         "organization_id":
"https://directory.carequality.org/Organization/2.16.840.1.113883.19.3
47473",
         "purpose_of_use":
["urn:oid:2.16.840.1.113883.3.18.7.1#TREATMENT"],
         "consent_policy":
["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.5"],
         "consent_reference":
["https://implementer1.example.com/fhir/R4/DocumentReference/consent-
12345"]
       }
    }
}
```

9.4 Clinical Data Exchange

9.4.1 FHIR Version and FHIR Implementation Guide Support Requirements

For participation in the Carequality FHIR information exchange, Carequality FHIR implementers MUST support FHIR US Core Implementation Guide V3.1.1 where data is available (e.g., US Core Pediatric BMI for Age Observation Profile need not be supported if the information is not collected) and MAY support subsequent version(s). In addition, FHIR Implementation Guides MUST be supported to the requirement levels specified in this link.

9.4.2 Patient Discovery

Except for the SMART on FHIR auth code flow in which the `launch/patient` SMART scope is requested, granted and the Patient ID is subsequently provided, Patient Discovery SHALL be performed using the FHIR Patient Resource $match operation. Each query SHALL include, but is not limited to, all available USCDI patient demographics with a minimum of (where known): first name, last name, date of birth, birth sex, current address (normalized as per section 3.3.2), phone number(s), and email address(es) plus administrative gender. All implementers SHALL support these demographics. A responder MAY ignore any other demographic not supported.

The $match request operation SHALL have the following parameters:

Parameter	Required Value
onlyCertainMatches	SHALL be set to true for Patient Requests; when set to true, the server SHALL return only certain matches; when absent or set to false, the server MAY return probable matches, but is not required to do so if its organizational policy allows only certain matches to be returned
count	Optional, server MAY send fewer results than specified

Deleted: ¶

Deleted: After generating an authentication JWT, the client requests a new access token via HTTP POST to the FHIR authorization server's token endpoint URL as per section 5.2.2.2 of the HL7/UDAP Security for Scalable Registration, Authentication, and Authorization FHIR IG.¶
Examples (non-normative, white space, and line breaks added for clarity, not URL-encoded):¶
Request:¶
POST /token HTTP/1.1¶
Host: as.example.com¶
Content-type: application/x-www-form-urlencoded¶
¶
grant_type=client_credentials&¶
scope=system/Patient.read&¶
client_assertion_type=urn:ietf:params: :client-assertion-type:jwt-bearer&¶
client_assertion=eyJh[…remainder omitted for brevity…]&¶
udap=1¶
Response (success):¶
HTTP/1.1 200 OK¶
Content-Type: application/json¶
{¶
  "access_token": "example_access_token_issued_by_AS",¶
  "token_type": "Bearer",¶
  "expires_in": 3600¶
}¶
¶
Response (failure, Authorization Server requires a specific Access Consent policy to be asserted):¶
HTTP/1.1 400 Bad Request¶
Content-Type: application/json¶
{¶
  "error": "invalid_grant",¶
  "error_description": "An Access Consent policy must be asserted for this purpose of use.",
  "extensions": {¶
    "hl7-b2b" : {
      "consent_policy":
["urn:oid:2.16.840.1.113883.3.7204.1.1.1.1.1"]
    }¶
  }¶
}¶

	Note that clients should be careful when using this, as it may prevent probable - and valid - matches from being returned
resource	Patient resource with included demographic parameters formatted as per US Core Patient profile

Appendix A: CEQ Person Resource Profile for UDAP

```
{
  "resourceType": "StructureDefinition",
  "id": "CEQPerson",
  "url": "http://carequality.org/fhir/udap-
person/StructureDefinition/CEQPerson",
  "name": "CEQPerson",
  "title": "Carequality UDAP Person",
  "status": "active",
  "description": "Profile on Person for use with the Carequality UDAP
implementation",
  "fhirVersion": "4.0.1",
  "kind": "resource",
  "abstract": false,
  "type": "Person",
  "baseDefinition": "http://hl7.org/fhir/StructureDefinition/Person",
  "derivation": "constraint",
  "differential": {
      "element": [
      {
      "id": "Person.name.family",
      "path": "Person.name.family",
      "min": 1
      },
      {
      "id": "Person.name.given",
      "path": "Person.name.given",
      "min": 2
      },
      {
      "id": "Person.telecom",
      "path": "Person.telecom",
      "slicing": {
            "discriminator": [
            {
            "type": "pattern",
            "path": "system"
            }
            ],
            "rules": "open",
            "description": "Forcing both a phone and an email contact"
      },
      "min": 2
      },
      {
      "id": "Person.telecom:tphone",
      "path": "Person.telecom",
      "sliceName": "tphone",
      "min": 1,
      "max": "*"
      },
      {
      "id": "Person.telecom:tphone.system",
      "path": "Person.telecom.system",
      "min": 1,
      "patternCode": "phone"
      },
      {
      "id": "Person.telecom:email",
      "path": "Person.telecom",
      "sliceName": "email",
      "min": 1,
      "max": "*"
      },
      {
      "id": "Person.telecom:email.system",
      "path": "Person.telecom.system",
      "min": 1,
      "patternCode": "email"
      },
      {
      "id": "Person.birthDate",
      "path": "Person.birthDate",
      "min": 1
      },
      {
      "id": "Person.address.line",
      "path": "Person.address.line",
      "min": 1
      },
      {
      "id": "Person.address.city",
      "path": "Person.address.city",
      "min": 1
      },
      {
      "id": "Person.address.state",
      "path": "Person.address.state",
      "min": 1
      },
      {
      "id": "Person.address.postalCode",
      "path": "Person.address.postalCode",
      "min": 1
      }
      ]
  }
}
```

Page 4: [1] Deleted Bill Mehegan 1/25/2024 11:26:00 AM

Page 6: [2] Deleted Bill Mehegan 1/29/2024 8:38:00 AM

Page 6: [3] Deleted Bill Mehegan 1/25/2024 11:13:00 AM

Page 6: [4] Deleted Bill Mehegan 1/25/2024 11:16:00 AM

Page 6: [5] Deleted Bill Mehegan 1/29/2024 2:50:00 PM

Page 12: [6] Deleted Bill Mehegan 1/25/2024 11:22:00 AM

Page 12: [7] Deleted Bill Mehegan 1/29/2024 2:57:00 PM

Page 12: [8] Deleted Bill Mehegan 1/29/2024 3:34:00 PM

Page 12: [9] Deleted Bill Mehegan 1/29/2024 3:38:00 PM

Page 24: [10] Deleted David Pyke 11/7/2023 10:27:00 AM

Page 24: [11] Deleted David Pyke 11/7/2023 10:29:00 AM

Page 24: [12] Deleted David Pyke 11/7/2023 10:38:00 AM

Page 24: [13] Deleted David Pyke 11/7/2023 10:38:00 AM

Page 24: [14] Deleted David Pyke 11/7/2023 10:40:00 AM

Page 25: [15] Deleted David Pyke 11/7/2023 10:39:00 AM

Page 25: [16] Deleted David Pyke 11/7/2023 10:52:00 AM

Page 26: [17] Deleted David Pyke 11/7/2023 10:56:00 AM