FAST Response to Draft TEFCA Facilitated FHIR Implementation Guide

2.2 Responding Actor

An Actor with the declared role of a Responding Actor provides information in response to queries by an Actor in the FHIR Query Initiator role. An Actor with the declared role of a Responding Actor shall support the technical requirements throughout this Guide that are specifically described as applying to the Responding Actor role. The Responding Actor is associated with one or more FHIR servers. Each FHIR server is associated with an Authorization Server.

Comment: Many of the FHIR endpoints will be FHIR Facades and not FHIR services – need to clarify the difference and the implications.

3.1 Provenance

QHINS, Participants, and Subparticipants SHALL use the Provenance Resource [1] 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 Use of Provenance to record Import and Transform. The US Core v4.0 Provenance profile SHALL be included in any response where data has been transformed.

Comment: US Core v4.0 only requires support for the Author Organization and the Transmitter. There is no requirement to indicate the transformation and, in general, the value sets are not sufficient to describe the transformation in an unambiguous manner.

General: Please use the standard conformance verbs (SHALL, SHALL NOT, SHOULD, SHOULD NOT, MAY, MAY NOT) for describing FHIR standards – the use of other conformance verbs (e.g., MUST) should be avoided.

3.3 Error Responses

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, such as via a retry operation due to the resource being busy, or a fatal error. QHINs, Participants and Subparticipants MAY choose to obscure some of these details for security reasons. Any such choice SHOULD be linked to identified security concerns.

Comment:

1) Conformance to the use of OperationOutcome should be a SHALL to promote interoperability in error conditions.

2) OperationOutcome resource specifies a value set for OperationOutcome.details with Example binding. If the use of operation outcome is to be of value in automating the handling of errors, a well-defined value set is necessary with a binding of at least Extensible.

3.6 Endpoint Lifetime

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.

Comment: why 48 hours?

4.1.2 Nominal Flow:

2. The FHIR Query Initiator discovers the endpoints associated with each Responding Actor it wants to transact with using FHIR.
    a. This IG does not define the mechanism a FHIR Query Initiator uses to discover the endpoints. A QHIN, for example, might provide direct access to its QHIN Directory. However, queries for Patient Discovery SHALL be done via the QHIN Directory.

Comment: This IG should define the minimum query requirements that SHALL be supported by all QHINs for any query. Anything less will compromise the ability of Query Initiators to discover endpoints.

5.1 FHIR Endpoints & Endpoint Discovery

QHINs, Participants, and Subparticipants SHALL use the FHIR CapabilityStatement resource to define FHIR server capabilities. Implementers SHALL provide at least one publicly discoverable CapabilityStatement where CapabilityStatement.kind=”instance”. Implementers SHALL provide a

CapabilityStatement for each endpoint associated with a FHIR server, defining the capabilities available at that endpoint. Each endpoint SHALL provide access to at least one FHIR resource. Discovery of Endpoints shall be executed by a query to the QHIN Directory service which will have the FHIR endpoint(s) for the Participant and Subparticipant.

This CapabilityStatement will only be made available by the server and will not be copied into the RCE/QHIN 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 RCE Directory, but that will be addressed later based on implementation feedback.

Comment: The requirement to access the capability statement for all FHIR endpoints makes determining the correct endpoint for a specific use overly complex. The FAST solution document and the National Directory IG effort have defined specific elements (e.g., FHIR version supported) that SHOULD be part of any compliant directory. We encourage TEFCA to require that QHINs adopt a compatible directory endpoint model.

Links to the FAST National Healthcare Directors IGs are below:

- National Healthcare Directory Exchange
- National Healthcare Directory Query
- National Healthcare Directory Attestation and Verification

5.2 Authentication/Trust

X.509 certificates establish the authenticity of Actors implementing this IG. The RCE will issue one "Intermediate" certificate to each QHIN to seed the QHIN's Certificate Authority. A QHIN's Certificate Authority issues certificates to downstream Actors. Certificates used by any Actor SHALL be chained to the RCE "root" certificate.

Comment: This comment's context is in light that QHINs, participant, and subparticipants must be viewed through a lens where Healthcare is a Critical Infrastructure Sector. QHINs and related participants will be best served through accredited CAs whose security, operations, and procedures are audited. CAs will play a critical role in upholding trustworthiness of TEFCA as it matures, and whose networks will undoubtably become of focal point of adversarial actors.

5.2.1.2 Issuance

QHINs SHALL issue certificates to each Operator of a FHIR client or server. If multiple instances of a client or server are maintained by different Operators, then each Operator SHALL be issued a separate certificate. An Operator MAY group various client and/or server functions together as a single application with a single certificate, or divide them into separate applications with 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).

Comment: We strongly encourage TEFCA to require that all QHINs utilize an accredited Certificate Authority (CA) to issue all certificates. Any CA must support the ability to provide certificate status information to relying parties so a relying party can determine whether a certificate has been revoked and the guaranteed response time to revoke certificates must meet Federal standards.

TLS certificates used for transactions within a QHIN’s network environment SHALL NOT be used by FHIR transactions between Participants and Subparticipants across QHIN networks.

Comment: The above paragraph as written is likely to lead to confusion. Consider the following when revising.

- TLS certificate typically implies a x.509 that is used for host identification in the context of the TLS handshake such as in https. Is that the precise context of ***TLS certificates*** this paragraph? If not, the term X.509 should be used in place of “TLS”. If the intent is that TLS certificates should not be used to sign UDAP assertions, that should be stated.
- The term “used” leaves too much room for interpretation. Is the term “used” meant to imply some or all of the following?
    - Used for host identification as in the TLS handshake employed by https
    - Used for digital signatures of JWT claims of any token type specified by the HL7 Security IG

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

Comment: In reference to page 19 – Table 4. The element named “organization” element should be “organization_name” to be consistent with 5.2.1.1 of the FHIR/Security IG: http://hl7.org/fhir/us/udap-security/b2b.html#b2b-authorization-extension-object

5.3.1 FHIR Version and FHIR Implementation Guide Support Requirements

Implementers SHALL support FHIR US Core Implementation Guide V4.0.0 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 SHOULD support version 5.0.1. In addition, the following FHIR Implementation Guides SHOULD be supported:

- Bulk Data Access IG v2.0.0
- Mobile access to Health Documents (MHD) v4.1.0
- Da Vinci Payer Data Exchange v2.0.0 when released

Other FHIR Implementation Guides MAY be supported as appropriate. Actors SHOULD list all IGs supported in their FHIR server CapabilityStatement.

Comment: Support should be as follows (in addition to the three bullets above

1) SHALL support FHIR release 4.0.1 (as specified in the 21st Century Cures Act Final regulation)
2) SHALL support US Core 3.1.1 (as specified in the 21st Century Cures Act Final regulation)
3) SHOULD support US Core 4.0.0 and/or 5.0.1 (as specified in 2022 SVAP)
4) SHOULD support SMART Application Launch Framework IG V2.2.0
5) SHOULD support FHIR Version awareness as specified by 2.1.7.0.7 Extensions for converting between versions. FHIR Clients should be required to self-identify where possible to avoid version incompatibility.

5.2.4.2 Obtaining an Access Token

Comment: Referenced link at the bottom of pg. 17 (also #4 reference page footer pg. 8) is broken: should be https://rce.sequoiaproject.org/tefca-and-rce-resources/