HL7® FHIR® Security

Education Event

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

TEFCA FHIR Registration, Authentication and Authorization

FAST Security, SMART and more

David Pyke, RCE Technical SME

HL7 International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

Who am I?

- Dave Pyke, Standards Architect
- Author of the TEFCA QHIN Technical Framework and assorted SOPs
- Technical Director of the FHIR At Scale Taskforce (FAST) FHIR Accelerator
- Member of the HL7 Technical Steering Committee,
- Co-chair HL7 Community Based Care and Privacy WG
- Involved with FHIR since 2012 (part of the QA team)
  - Owner of the FHIR Consent Resource
- Author and trainer of FHIR content including FHIR Implementation Guide development
- Father of two wonderful daughters, 12 and 15 years old.

HL7 International | ASTP Assistant Secretary for Technology Policy | ONC Office of the National Coordinator for Health Information Technology

Agenda

- Introduction and History
- TEFCA FHIR Timeline
- Basic FHIR
- Basic Security
- HL7 FAST UDAP SSRAA
- HL7 SMART on FHIR
- Scope Negotiation

Introduction

- The Trusted Exchange Framework and Common Agreement (TEFCA) is an initiative of the Office of the National Coordinator for Health IT (ONC).
- TEFCA is being administrated by The Sequoia Project under the name of Recognized Coordinating Entity (RCE)
- Documentation for TEFCA is two main documents
  - Common Agreement for Nationwide Health Information Interoperability (CA): the contractual document
  - Qualified Health Information Network (QHIN) Technical Framework (QTF): the technical specification
  - There are SOPs and supplemental documents being released as they are complete
- TEFCA went live in December 2023
- All detailed information is available at https://rce.sequoiaproject.org

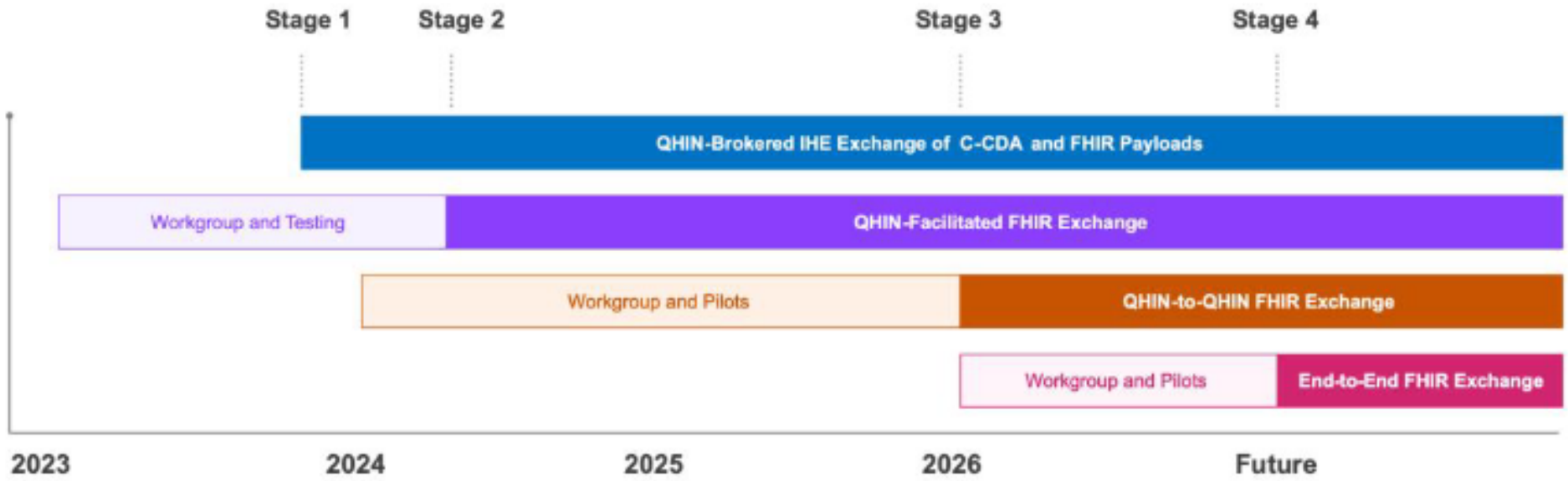
History

- ONC began the process to create TEFCA when the 21st Century Cures Act (Cures Act) was passed into law.
- The first release (TEF Draft 1) was January 2018 for comment
- The TEF Draft 2 was released April 2019 included three components:
  - the TEF Draft 2;
  - the Minimum Required Terms and Conditions (MRTCs) Draft 2; and
  - QTF Draft 1 (high level technical design).
- QTF Draft 2 was released for comment August 2020
- CA Draft was released for comment October 2021

HISTORY

- QTF V1.0 was released January 2022
- CA V1.0 was released February 2022
  - Broad ideas for design and options that might be included
- Facilitated FHIR was released for Pilot testing in December 2022
  - Based on the Carequality FHIR Implementation Guide
  - Tested at 4 Connectathons (IHE and HL7) in 2023
  - Scope Negotiation designed by a BoF meeting and subsequent discussions
- CA and QTF V2 and Facilitated FHIR SOP were released in July 2024
- Multiple SOPs including Public Health, Treatment and HCO were released in August 2024

TEFCA FHIR Roadmap (As of Jan 2024)



TEFCA Basic FHIR Requirements

- All data exchange MUST follow the USCore FHIR IG requirements (which is negotiable before Jan 1, 2026). In addition, the following FHIR Implementation Guides SHOULD be supported:
  - Bulk Data Access IG v2.0.0
  - Mobile access to Health Documents (MHD) v4.2.1 (ITI-67 AND ITI-68)
  - Da Vinci Payer Data Exchange v1.0.0
  - Da Vinci Clinical Data Exchange v2.0.0
- All requesters using a valid TEFCA certificate and Purpose of Use must be given access according to the Common Agreement
- Where data is transformed from other formats, a Provenance resource must be included to show where and how the transformation is done.

TEFCA Basic FHIR Requirements

- Endpoint and Patient discovery MUST be through a QHIN Patient Discovery Query
- Servers MUST have a CapabilityStatement and Patient resources available
- Servers MUST have a CapabilityStatement at each published endpoint
  - CapabilityStatements MUST list all FHIR IG operations supported
  - CapabilityStatements SHOULD list all FHIR IGs supported

- Servers MUST support $match
  - Servers SHOULD have the capability to return more than one potential patient match when a patient search yields more than one match.
  - Servers MUST NOT return more than one potential match when such action could be a violation of HIPAA or other Applicable Law
  - Responding Nodes MUST NOT require more than all US Core Patient Resource demographics before returning a patient list Response

FAST Auth[x] Roadmap

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

TEFCA Basic Auth[x] Requirements

- Authorization Servers SHOULD issue access tokens with a lifetime no longer than 60 minutes.
- 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”.
- All implementations MUST support RS256, and SHOULD support ES256, ES384 and RS384.

TEFCA SSRAA Requirements

- As of January 1, 2026 all auth[x] MUST use the requirements of the SSRAA FHIR IG
- 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.
  - If a new client_id has been issued for a registration modification, the responding Authorization Server MUST disable the old client_id so that it cannot be used for subsequent Queries.
  - Retired client_ids MUST be preserved so that it can be associated with log entries and the client.
- The udap_certifications_supported and udap_certifications_required metadata returned MUST include https://rce.sequoiaproject.org/udap/profiles/basic-app-certification.

TEFCA SSRAA Requirements

- The software statement MUST contain a certification_name element of “TEFCA Basic App Certification".
- The software statement MUST contain a certification_uris element which MUST be a fixed array with single string element of https://rce.sequoiaproject.org/udap/profiles/basic-app-certification

TEFCA SSRAA B2B

- The software statement extensions element MUST be present and contain a JSON B2B Authorization Extension Object
- The B2B Extension must have the following:

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

- If the request metadata is insufficient for access due to missing or insufficient ACP, the auth server MUST respond with an invalid_grant response and should respond with the following extension

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.

TEFCA SSRAA IAS

- Responders 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 consent_reference array.
- Responders MUST support the Authorization Code Grant type for IAS Queries.
- The Client and responder MUST provide the tefca_ias extension during the Authorization flow.

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

TEFCA SSRAA IAS

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

TEFCA SMART on FHIR Requirements

- The SMART capabilities MUST include “launch-standalone”, “client-public”, “context-standalone-patient”, “permission-patient”, and “permission-user”.
- The SMART grant_types_supported MUST include “authorization_code”.
- As part of the auth[x] process, the information in the tefca_smart extension MUST be collected

SMART required information

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

TEFCA SMART on FHIR Requirements

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

tefca_smart extension

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

TEFCA SMART on FHIR Requirements

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

TEFCA Scope Negotiation

- The scopes_supported metadata MUST be present in the .well-known/smart-configuration or .well-known/udap object, as applicable, and MUST list all scopes supported including all supported wildcard scopes.
  - 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.
- A client may 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 SHOULD 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”.

TEFCA Scope Negotiation

- 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.
- 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.
- The scope list as part of an access grant request MAY be the same as the list from registration or MAY be a subset.
- A grant time request to the server MAY return a full or subset of the requested scopes.

TEFCA Scope Negotiation

- 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.
- 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 and/or not part of the scopes requested during registration.

QUESTIONS?