eHealth Exchange™

Jayme Pina, Director of Governance and Onboarding

Eric Heflin, Consultant

TEFCA Policy and Technology Updates

eHealth Exchange™

Agenda

- Welcome!
  TEFCA Policy and Governance Topics
- July CMS HL7 Connectathon
- QTF v2.1 Draft
- TEFCA Government Benefits Determination SOP
- TEFCA Checklist Major Update
- 2025 Annual Meeting Invitation
- Public Comments / Open Discussion

This meeting is being recorded.

QHINs and Candidate QHINs

commonwell® HEALTH ALLIANCE

eClinicalWorks

eHealth Exchange™

Epic Nexus

HEALTH® GORILLA

Kno2®

KONZA NATIONAL NETWORK

MEDALLIES® A CENTAURI HEALTH SOLUTIONS® COMPANY

Netsmart

surescripts Health Information Network™

Candidate QHIN(s)

ORACLE Health Information Network, Inc.™

Current as of 2025-09-19

Source: https://rce.sequoiaproject.org/wp-content/uploads/2025/07/RCE-Info-Call-August-19-_Final-v2.pdf

TEFCA Policy and Governance Topics

Jayme Pina

eHealth Exchange™

Updates

- New TEFCA DRAFT Government Benefits Determination SoP and eXchange Purposes documents for feedback, which we will cover more later in this meeting
- QTF 2.1 Draft for comments released and now closed.
- QTF 2.1 is under review, and we will provide updates when the final version is released.
- New guidance from RCE on eXchange Purposes (covered next)

TEFCA eXchange Purposes (XP) Codes

Responding Nodes MUST Respond to Queries for the XP Codes that have a required Response, unless an exception applies (such as for PHAs), as set forth in the Exchange Purposes SOP

XP Codes that Require Response

- TEFCA Required Treatment
- Individual Access Services (IAS)

XP Codes that Permit a Response

- Payment
- Health Care Operations
- *Care Coordination / Case Management
- *HEDIS Reporting
- *Quality Measure Reporting
- Public Health
- Electronic Case Reporting
- Electronic Lab Reporting
- Government Benefits Determination

Source: https://rce.sequoiaproject.org/wp-content/uploads/2025/06/RCE-Info-Call-June-17-2025-to-Final.pdf p. 20

CMS Connectathon
Unified Data Access Profiles (UDAP)
Security for Scalable Registration, Authentication, and Authorization (SSRAA)

eHealth Exchange Participation
FAST Infrastructure Track
CMS FHIR Connectathon #6
July 2025

John McBride

eHealth Exchange™

CMS FHIR Connectathon – FAST Infrastructure

- eHealth Exchange participated as an active tester in the July 2025 CMS FHIR Connectation FAST Infrastructure track

- A test suite was brought to exercise UDAP DCR and SSRAA (as a client)

- The workflow tested was:

  1. Create a software statement
  2. Initiate DCR workflow, register a client, and obtain a client_id
  3. Use the client_id to obtain an access token
  4. Use the access token to retrieve from resource server

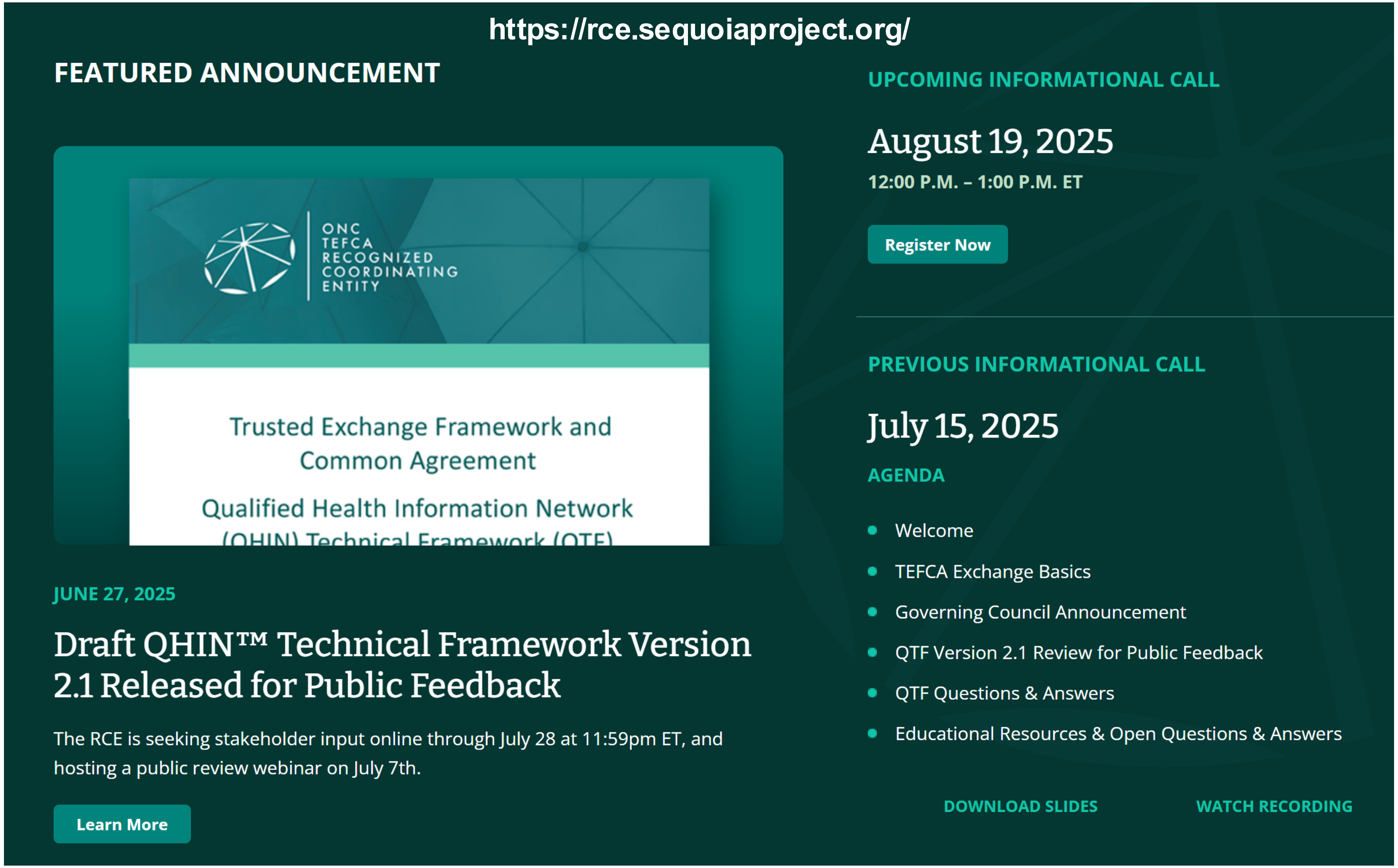
- Attended by John McBride, Tiffanie Hickman, Mike McCune, and Eric Heflin

QTF v2.1 Draft

Mike Yackanich

eHealth Exchange™

Draft QHIN™ Technical Framework Version 2.1



https://rce.sequoiaproject.org/

FEATURED ANNOUNCEMENT

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Trusted Exchange Framework and Common Agreement

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

JUNE 27, 2025

Draft QHIN™ Technical Framework Version 2.1 Released for Public Feedback

The RCE is seeking stakeholder input online through July 28 at 11:59pm ET, and hosting a public review webinar on July 7th.

Learn More

UPCOMING INFORMATIONAL CALL

August 19, 2025

12:00 P.M. – 1:00 P.M. ET

Register Now

PREVIOUS INFORMATIONAL CALL

July 15, 2025

AGENDA

- Welcome
- TEFCA Exchange Basics
- Governing Council Announcement
- QTF Version 2.1 Review for Public Feedback
- QTF Questions & Answers
- Educational Resources & Open Questions & Answers

DOWNLOAD SLIDES

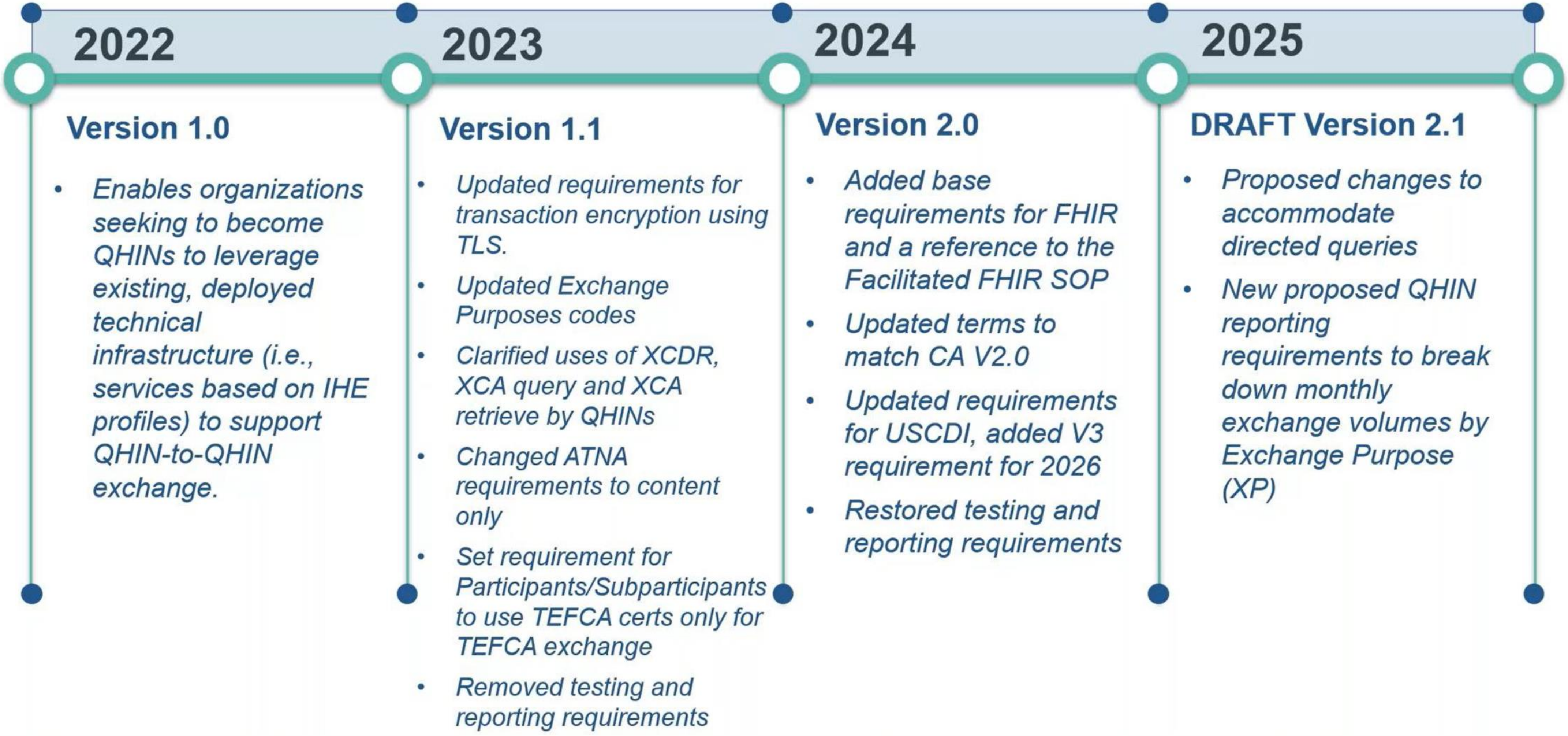
WATCH RECORDING

QHIN Technical Framework (QTF)

- What is the QTF?
  - The QHIN™ Technical Framework (QTF) describes the functional and technical requirements that a Health Information Network (HIN) must fulfill to serve as a QHIN under the Trusted Exchange Framework and Common Agreement™ (TEFCA™)
  - The QTF specifies the technical underpinnings for TEFCA Exchange, QHIN technical capabilities and services, and certain other responsibilities, some of which extend to Participants and Subparticipants
  - The TEFCA Common Agreement requires compliance with the QTF
  - The QTF focuses on technical and functional requirements for three information exchange modalities for QHINs: QHIN Query, QHIN Message Delivery, and Facilitated FHIR

See https://rce.sequoiaproject.org/tefca-and-rce-resources/ for resources such as the Common Agreement, Standard Operating Procedures (SOPs), technical documents, etc.

QTF Version History



2022

Version 1.0

- *Enables organizations seeking to become QHINs to leverage existing, deployed technical infrastructure (i.e., services based on IHE profiles) to support QHIN-to-QHIN exchange.*

2023

Version 1.1

- *Updated requirements for transaction encryption using TLS.*
- *Updated Exchange Purposes codes*
- *Clarified uses of XCDR, XCA query and XCA retrieve by QHINs*
- *Changed ATNA requirements to content only*
- *Set requirement for Participants/Subparticipants to use TEFCA certs only for TEFCA exchange*
- *Removed testing and reporting requirements*

2024

Version 2.0

- *Added base requirements for FHIR and a reference to the Facilitated FHIR SOP*
- *Updated terms to match CA V2.0*
- *Updated requirements for USCDI, added V3 requirement for 2026*
- *Restored testing and reporting requirements*

2025

DRAFT Version 2.1

- *Proposed changes to accommodate directed queries*
- *New proposed QHIN reporting requirements to break down monthly exchange volumes by Exchange Purpose (XP)*

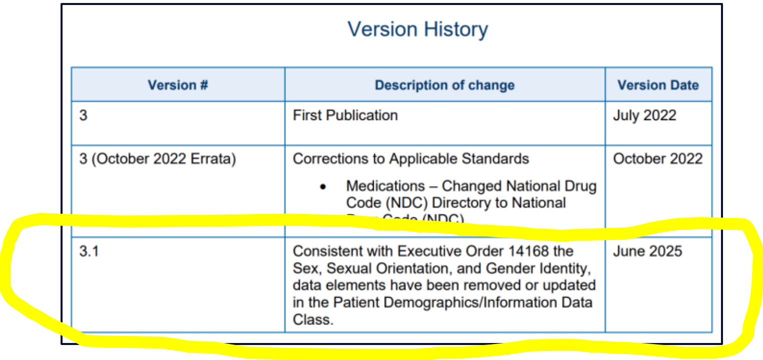
QTF v2.1 Updates

- [QTF-19]
  - Explicitly identifies the SAML attribute to be used to identify the ultimate initiator of a request (Subject Organization Id)
- [QTF-38 thru QTF-40] (added support for directed queries)
  - QHIN IGs MAY direct a query to another QHIN organization by setting the HCID of the receiver element to the targeted organization (receiver/device/asAgent/representedOrganization/id/@root)
  - QHIN RGs SHOULD only respond with information from the Responding Node corresponding to that HomeCommunityId

QTF v2.1 Updates

- [QTF-89]
  - QHINs must update the RCE Directory Service with new Participants or Subparticipant initiating nodes at least two business days prior to commencing production activity (previously was “48 hours”)

- [QTF-106]
  - As of January 1st, 2026, all information sent MUST conform to USCDI V3.1 data classes, data elements, and vocabulary requirements (previously had to conform to V3 as of Jan 2026)



Version History

Version #	Description of change	Version Date
3	First Publication	July 2022
3 (October 2022 Errata)	Corrections to Applicable Standards • Medications – Changed National Drug Code (NDC) Directory to National Drug Code (NDC)	October 2022
3.1	Consistent with Executive Order 14168 the Sex, Sexual Orientation, and Gender Identity, data elements have been removed or updated in the Patient Demographics/Information Data Class.	June 2025

QTF v2.1 Updates

- [QTF-135]
  - Monthly transaction volume for document retrieval and submission to be broken down by Exchange Purpose (XP)

TEFCA Government Benefits Determination SOP

New TEFCA Standard Operating Procedure

Mike McCune

eHealth Exchange™

Purpose of the SOP

Streamline Benefit Determinations:

- The primary goal is to allow government agencies to more efficiently receive health information needed to determine eligibility for benefits like Social Security disability.

Expand Interoperability:

- It expands the uses of the TEFCA network beyond clinical care and public health to include the critical function of government benefits determination.

Support Individuals:

- For individuals, this means potentially faster responses from government agencies and quicker access to benefits they are entitled to.

Key Components

Authorized Exchange Purposes:

- Government Benefits Determination (TEFCA code **T-GOVDTRM**) is one of the authorized “eXchange Purposes" under the TEFCA framework. TEFCA exchange for this purpose is a "SHOULD" and not a "MUST".

- Sub-exchange purposes for Social Security Determination (SSD) consists of a code of **T-GOVDTRM-SSD** and **T-GOVDTRM-ACP** for related consent assertions.

- For QHIN queries: Only Initiating Nodes controlled by the Social Security Administration (SSA) or their Delegates may initiate Queries under the XP Code **T-GOVDTRM-SSD**, in accordance with the Framework Agreements, applicable SOPs, and Applicable Law. Reference the SOP for specific citations of the Code of Federal Regulations.

Key Components

Exchange Purposes SOP Draft 4.1

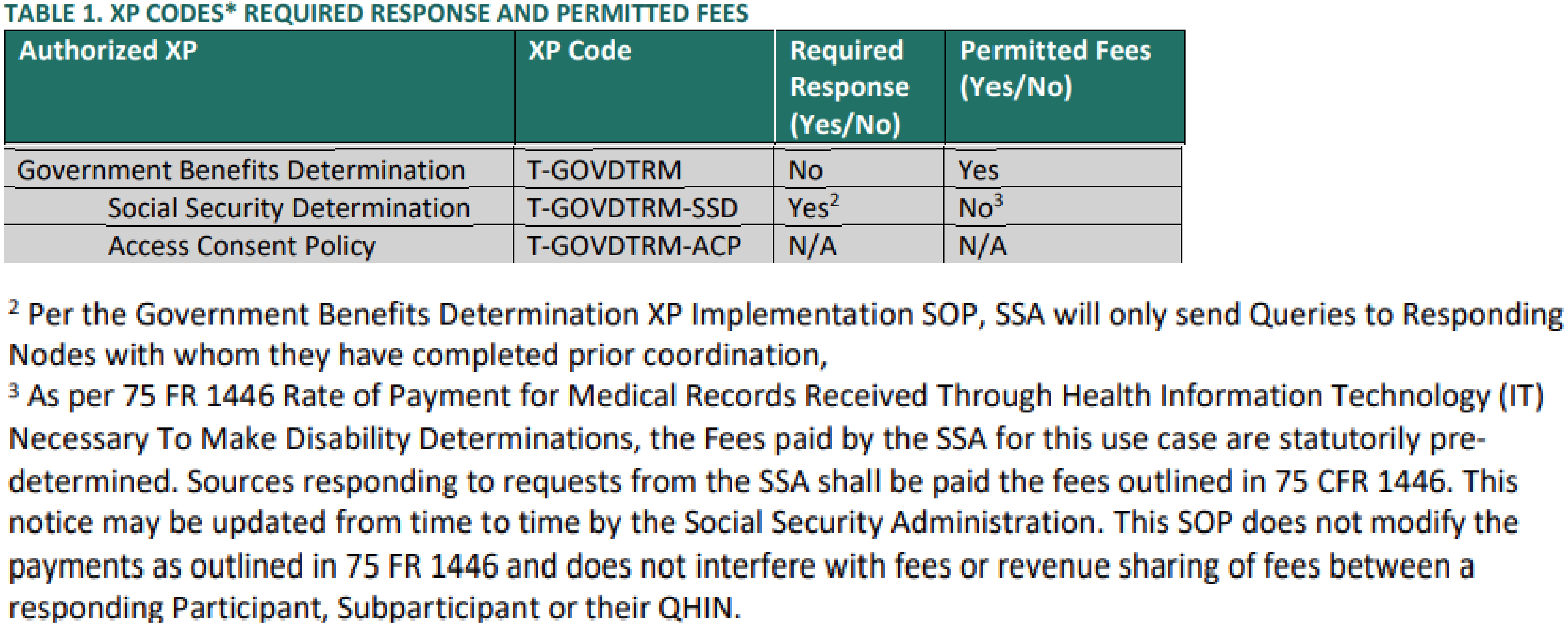


TABLE 1. XP CODES* REQUIRED RESPONSE AND PERMITTED FEES

Authorized XP	XP Code	Required Response (Yes/No)	Permitted Fees (Yes/No)
Government Benefits Determination	T-GOVDTRM	No	Yes
Social Security Determination	T-GOVDTRM-SSD	Yes[2]	No[3]
Access Consent Policy	T-GOVDTRM-ACP	N/A	N/A

[2] Per the Government Benefits Determination XP Implementation SOP, SSA will only send Queries to Responding Nodes with whom they have completed prior coordination,

[3] As per 75 FR 1446 Rate of Payment for Medical Records Received Through Health Information Technology (IT) Necessary To Make Disability Determinations, the Fees paid by the SSA for this use case are statutorily pre-determined. Sources responding to requests from the SSA shall be paid the fees outlined in 75 CFR 1446. This notice may be updated from time to time by the Social Security Administration. This SOP does not modify the payments as outlined in 75 FR 1446 and does not interfere with fees or revenue sharing of fees between a responding Participant, Subparticipant or their QHIN.

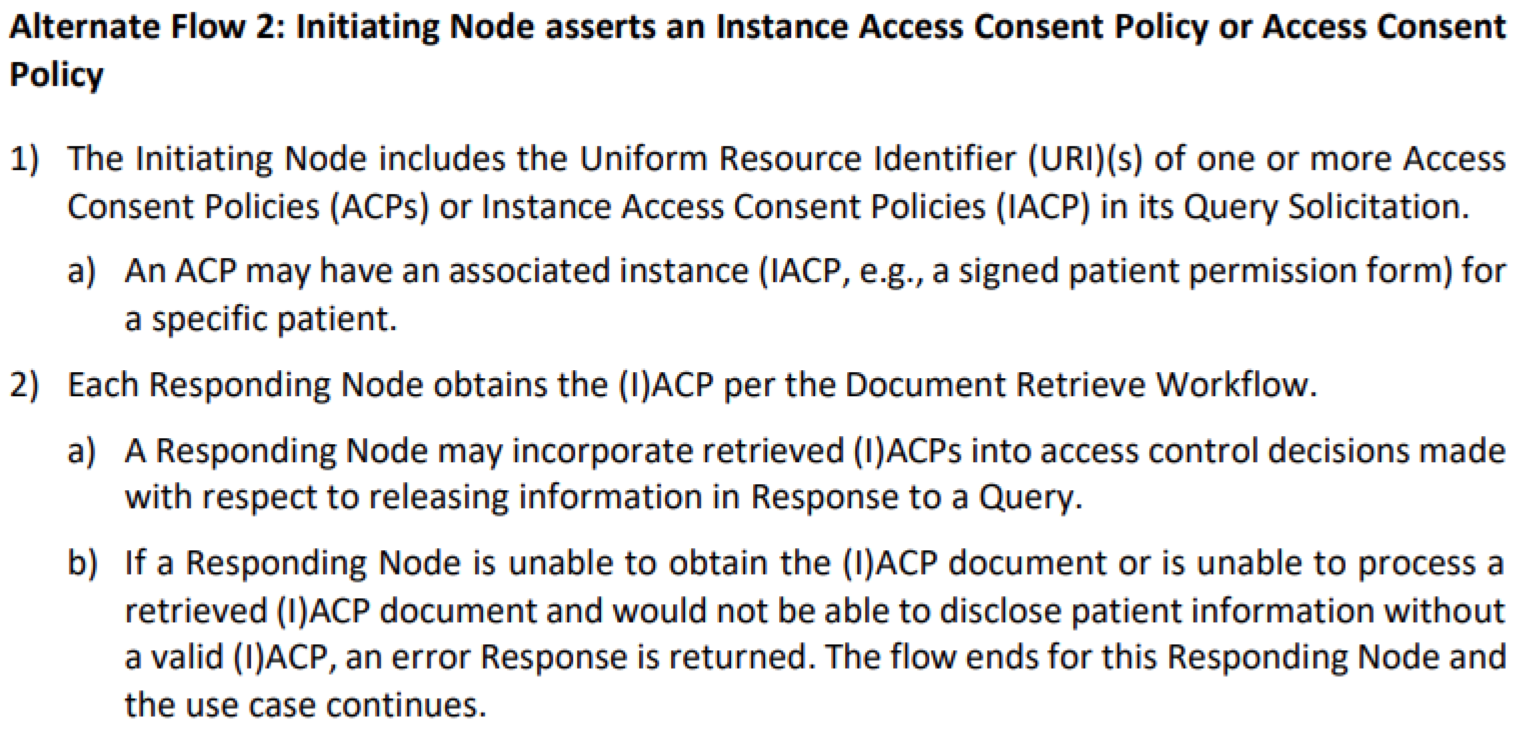
https://www.federalregister.gov/documents/2010/01/11/2010-225/rate-of-payment-for-medical-records-received-through-health-information-technology-it-necessary-to

Key Components

Access Consent Policy:

- Nodes responding to the SSA **must** retrieve and store the asserted Access Consent Policy using the flow described in QTF Patient Discovery Alternate Flow 2: Initiating Node asserts an Instance Access Consent Policy or Access Consent Policy.
- Responding Nodes MUST retrieve the patient's authorization/consent using the XP Code T-GOVDTRM-ACP.

QTF 2.1 Draft



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

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

Key Components

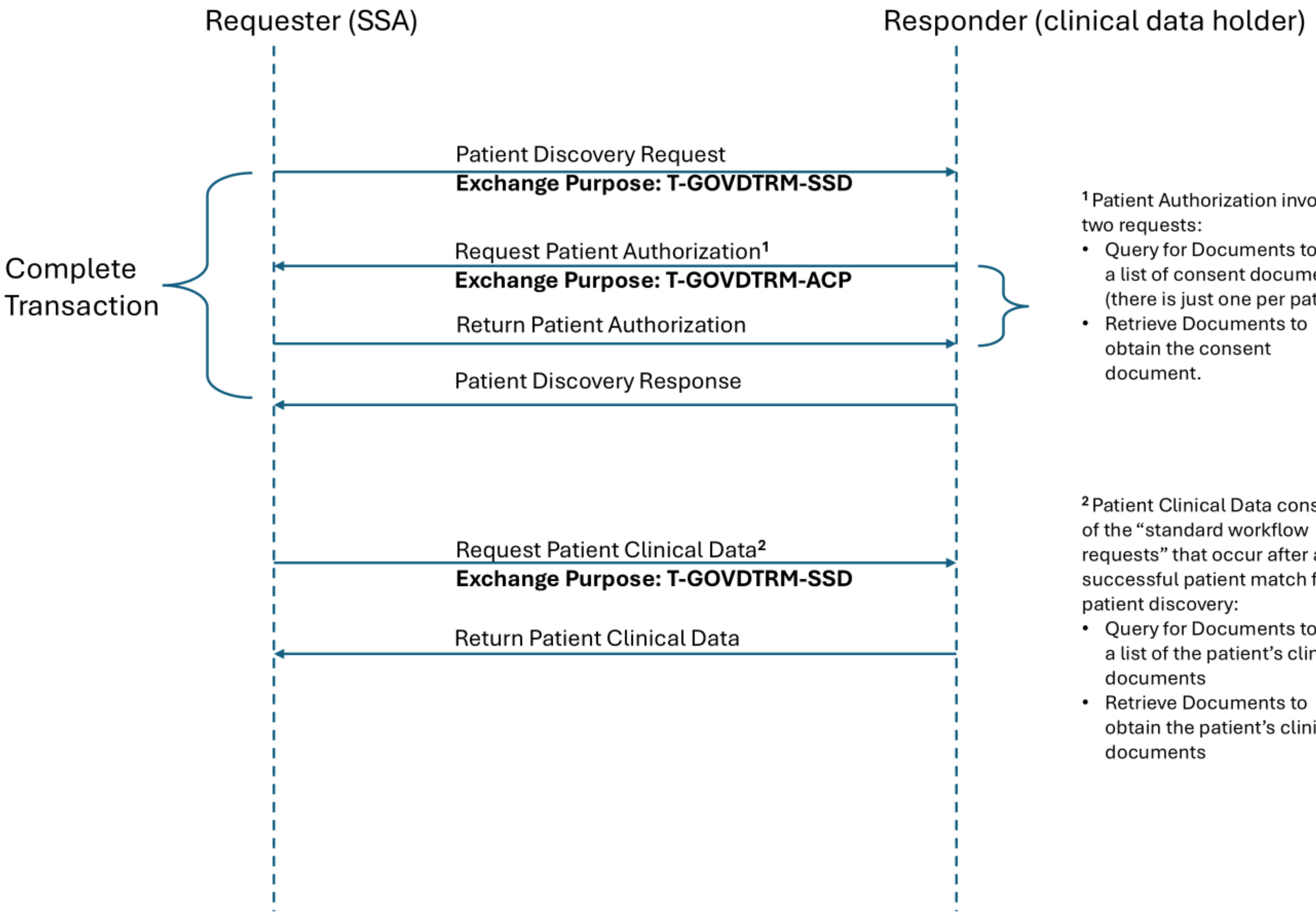
Responding Node Clinical Content:

- When responding to the SSA, the SSA has guidance on clinical content as per the referenced Implementation Guide.

The Government Benefits Determination SOP References the QTF 2.1 Draft

- QTF 2.1 draft added support for **directed query** which is a key feature required by the SSA.
- The SSA wants to limit queries flowing through nodes that don't have a need to process the request messages. On the responding side, the goal is to limit the message "exposure" to just the receiving QHIN and the ultimate responder.
- For patient discovery, the initiating node/QHIN should specify the responding node using the "receiver" element in the body of the SOAP message. This is the ultimate receiver of the message. The receiving QHIN should process the "receiver" element and direct the query to the responding node specified by the "receiver".
- Further changes are under consideration to support directed query for Query for Documents requests.

Workflow indicating exchange purpose



Requester (SSA)

Responder (clinical data holder)

Complete Transaction

Patient Discovery Request
Exchange Purpose: T-GOVDTRM-SSD

Request Patient Authorization[1]
Exchange Purpose: T-GOVDTRM-ACP

Return Patient Authorization

Patient Discovery Response

Request Patient Clinical Data[2]
Exchange Purpose: T-GOVDTRM-SSD

Return Patient Clinical Data

[1] Patient Authorization involves two requests:

- Query for Documents to get a list of consent documents (there is just one per patient)
- Retrieve Documents to obtain the consent document.

[2] Patient Clinical Data consists of the "standard workflow requests" that occur after a successful patient match for patient discovery:

- Query for Documents to get a list of the patient's clinical documents
- Retrieve Documents to obtain the patient's clinical documents

Status and Artifacts

- Two documents released for feedback on August 18, 2025:
  - Draft Government Benefits Determination Exchange Purpose Standard Operating Procedure (SOP)
  - https://rce.sequoiaproject.org/wp-content/uploads/2025/08/Draft-SOP-Gov-Benefits-Determination_5081.pdf
  - Draft Exchange Purposes SOP v4.1
  - https://rce.sequoiaproject.org/wp-content/uploads/2025/08/SOP-Exchange-Purposes_GBD-Updates_508.pdf
  - Feedback was closed on September 18, 2025
- GBD SOP references QTF 2.1 Draft
  - https://rce.sequoiaproject.org/wp-content/uploads/2025/06/QTF-2.1-Draft-for-Comment-clean.pdf

TEFCA Checklist Major Update

New Category: Facilitated FHIR
Ads 88 New Requirements for FF Transactions

Eric Heflin

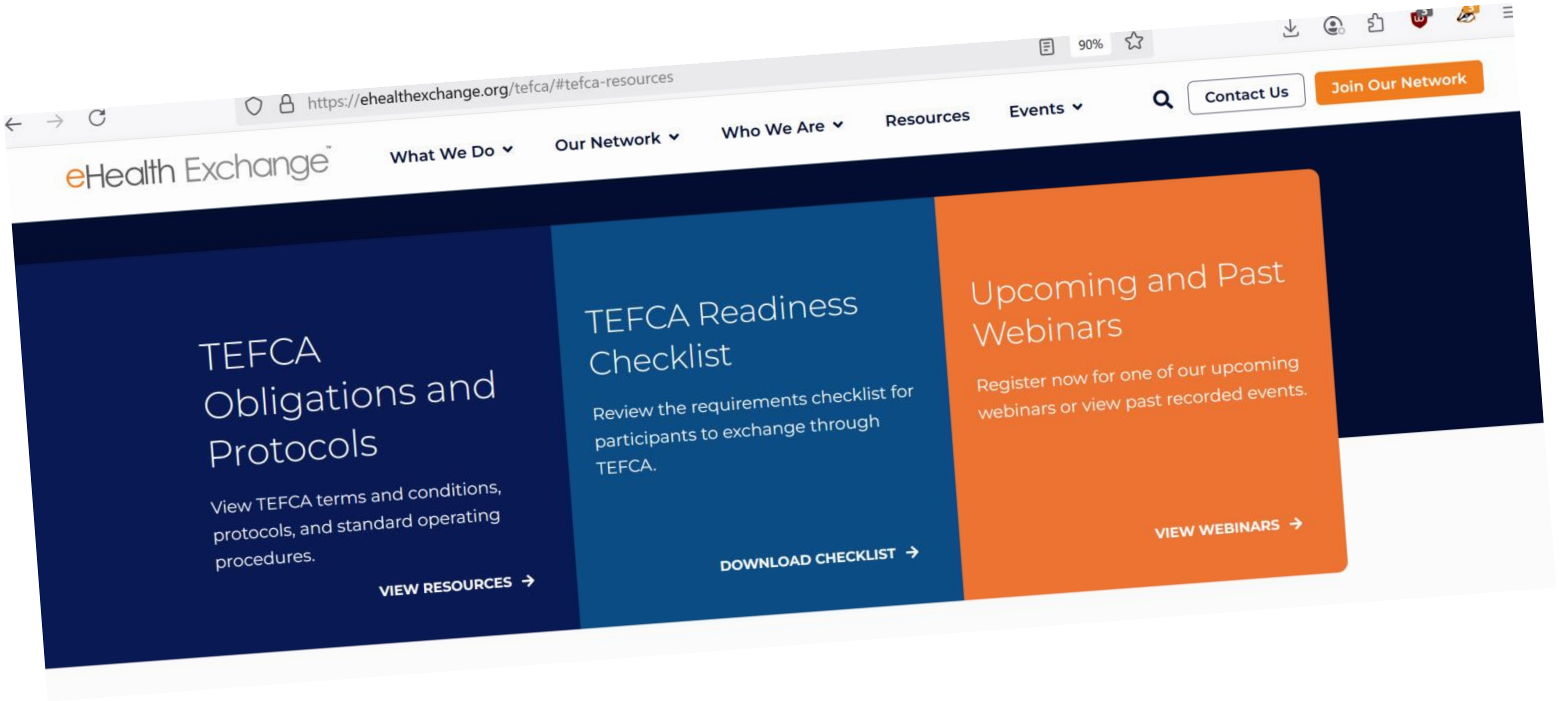
eHealth Exchange™

TEFCA Readiness Checklist Updates

- Added new tab for Facilitated FHIR
- Substantial new group of requirements, approximately 88 new flow-down requirements
- A dedicated webinar is being scheduled
- Groups of new requirements:
  - SSRAA security
  - US CORE v3.11
  - Capability statements
  - $match constraints
  - Project US@ support
  - Provance required for transformed data
  - Basic app certification

- Source: https://rce.sequoiaproject.org/wp-content/uploads/2024/07/SOP-Facilitated-FHIR-Implementation_508-1.pdf

TEFCA Readiness Checklist Updates (Contd.)



TEFCA Obligations and Protocols

View TEFCA terms and conditions, protocols, and standard operating procedures.

VIEW RESOURCES →

TEFCA Readiness Checklist

Review the requirements checklist for participants to exchange through TEFCA.

DOWNLOAD CHECKLIST →

Upcoming and Past Webinars

Register now for one of our upcoming webinars or view past recorded events.

VIEW WEBINARS →

- New requirement categories:
  - HL7 b2b extension
  - Patient consent
  - IAS extension
  - SMART application launch
  - Many constraints and processing requirements related to scopes
- View updated checklist on the eHealth Exchange website here

Changes Are Expected

- Please note that a number of these requirements could change and are under active discussion
- We will provide more information as any decisions are made and published by the RCE and ASTP
- The TEFCA Checklist documents topics under discussion

- The next group of slides paraphrase the new checklist items, organized by an eHealth Exchange taxonomy

TEFCA Facilitated FHIR Categories*

1. Security and Trust Foundations
2. Directory and Endpoint Management
3. Registration Processes
4. Authentication and Authorization Flows
5. FHIR Resources and Operations
6. Error and Response Handling

* These are eHealth Exchange determined categories

1. Security and Trust Foundations

These requirements establish baseline trust mechanisms, including certificates and metadata for secure exchanges.

- Certificates and Trust Requirements
- Metadata and Extensions

Certificates and Trust Requirements

- FF-001: Certificate use for authentication MUST conform to TEFCA certificate requirements as outlined in the Technical Trust Requirements document.
- FF-049: The udap_certifications_supported metadata MUST include the TEFCA certification URI.
- FF-050: The udap_certifications_required metadata MUST include the TEFCA certification URI.
- FF-051: The software statement MUST include the certification_name "TEFCA Basic App Certification".
- FF-052: The software statement MUST contain a certification_uris element as a fixed array with the TEFCA certification URI.

Metadata and Extensions

- FF-056: The software statement extensions element MUST include the “hl7-b2b” key with a B2B Authorization Extension Object.
- FF-057: Use of the hl7-b2b extension MUST include organization_id, organization_name, subject_id (conditional), and purpose_of_use.

2. Directory and Endpoint Management

These requirements cover indications in directories, endpoint discovery, and capability declarations.

- Directory Entries and Support Indications
- Endpoint Discovery
- Capability Statements

Directory Entries and Support Indications

- FF-002: All FHIR Adopters MUST indicate in their Directory Entry the supported registration and authentication/authorization standards.
- FF-003: The FHIR Endpoint to be used for TEFCA FHIR exchange.
- FF-004: Indicate support for the HL7 SSRAA FHIR IG 1.0.0 STU 1 – US Dynamic Registration (True/False).
- FF-005: Indicate support for one or more of the specified authentication/authorization frameworks.
- FF-006: HL7 SSRAA FHIR IG 1.0.0 – STU 1 US, Sections 4 and 5.
- FF-007: SMART Backend Services or Application Launch Implementation Guide Release (SMART) 1.0.0 and Framework.
- FF-008: Some other authentication and authorization framework that adheres to the QTF, based on out-of-band agreements.

Endpoint Discovery

- FF-020: All discovery of endpoints by Participants and Subparticipants MUST be executed by a Query to the QHIN Directory using the HCID from a Patient Discovery Query.
- FF-021: Responding Nodes with FHIR capabilities in the RCE Directory MUST provide access to the Patient Resource and at least one additional patient compartment Resource.

Capability Statements

- FF-022: All Responding Nodes MUST supply a CapabilityStatement resource to describe their FHIR capabilities.
- FF-023: Responding Nodes MUST use the FHIR CapabilityStatement resource to define server capabilities.
- FF-024: FHIR-capable Responding Nodes MUST provide at least one publicly discoverable CapabilityStatement.kind="instance".
- FF-025: Each FHIR endpoint of Responding Nodes listed in the RCE Directory MUST have a CapabilityStatement defining its capabilities.
- FF-026: CapabilityStatement MUST include all FHIR Implementation Guide operations supported by the Responding Node.

3. Registration Processes

These requirements detail client registration, modifications, and related timelines.

- General Registration Requirements
- Authentication and Authorization Framework Selection
- Client Modifications and Management

General Registration Requirements

- FF-009: Requirements surrounding the registration, authentication, and authorization of a FHIR client to a Responding Node MUST follow these requirements.
- FF-010: Prior to January 1, 2026 (subcategory header).
- FF-011: All FHIR Adopters MAY follow the requirements of HL7 SSRAA FHIR IG 1.0.0 STU 1 US Section 3 Registration.
- FF-012: Manual registration requests for client_id MUST be resolved within 5 business days where sufficient information has been provided, not exceeding specified requirements.
- FF-017: Beginning January 1, 2026, all FHIR Adopters MUST follow the requirements in HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Sections 2, 3, 4, and 5.
- FF-068: Each QHIN, Participant, or Subparticipant MUST establish a process for client registration, collecting specified information (client_name, redirect_uris, etc.).
- FF-069: Authorization Servers MUST assign a unique client_id to each registered client.

Authentication and Authorization Framework Selection

- FF-013: All FHIR adopters MUST use one of the specified frameworks (HL7 SSRAA, SMART, or other QTF-adherent).
- FF-014: HL7 SSRAA FHIR IG 1.0.0 – STU 1 US Sections 4 and 5.
- FF-015: SMART Release 1.0.0.
- FF-016: Some other authentication and authorization framework that adheres to the QTF, based on out-of-band agreements.

Client Modifications and Management

- FF-048: Clients MUST use the new client_id provided in a registration modification Response for all subsequent transactions.
- FF-053: Authorization Servers MUST disable old client_ids after issuing a new one in registration modification.
- FF-054: Retired client_ids MUST be preserved by the Authorization Server for association with log entries.

4. Authentication and Authorization Flows

These requirements govern auth/authz processes, including grants, extensions, and IAS/SMART specifics.

- General Auth/Authz Requirements
- Exchange Purposes
- IAS (Individual Access Services) Specific
- SMART Specific

General Auth/Authz Requirements

- FF-055: Servers MUST respond with "invalid scope" if a client requests a user scope without specifying a user during registration for certain grant types.
- FF-070: Responders MUST support Authorization Code Grant type for requests.

Exchange Purposes

- FF-018: All transactions MUST utilize the Exchange Purpose code system OID as defined in the Exchange Purposes SOP.

IAS (Individual Access Services) Specific

- FF-059: Responders supporting use cases that require transmission of consent information MUST support consent_policy and consent_reference claims.
- FF-060: Responders MUST support Authorization Code Grant type for IAS Queries.
- FF-061: Initiating Nodes MUST provide the tefca_ias extension during the IAS Authorization Flow.
- FF-063: A client application requesting a token for patient requests MUST include the TEFCA IAS Authorization Extension Object in its token request.
- FF-064: The user metadata in the patient_information element MUST correspond to the verified identity attributes of the permitted user.
- FF-065: If submitted user information does not match a person, return invalid_grant error.
- FF-075: When issuing an access token for an Individual, include the FHIR Patient Resource ID in the SMART launch context.

SMART Specific

- FF-066: SMART capabilities MUST include specified values (“launch-standalone”, etc.).
- FF-067: SMART grant_types_supported MUST include "authorization_code".
- FF-071: Initiating Nodes MUST provide the tefca_smart extension when requesting an authorization code.
- FF-072: The responder MUST support the TEFCA User Authorization Extension object "tefca_smart" as detailed more in the specification.
- FF-073: A client application requesting a token for patient requests MUST include the TEFCA SMART Authorization Extension Object.
- FF-074: If id_token does not match or is invalid, return invalid_grant error.

5. FHIR Resources and Operations

These requirements address resource availability, queries, and data handling.

- Resource Availability
- Patient Matching and Queries
- Provenance Requirements

Resource Availability

- FF-019: FHIR Adopters MUST make available all US Core V3.1.1 or higher Resources where such data exists.

Patient Matching and Queries

- FF-027: $match operations MUST be executed using demographics from the Patient Discovery Query.
- FF-028: Responding Nodes SHOULD return more than one potential patient match when applicable.
- FF-029: Responding Nodes MUST NOT return more than one potential match if it violates HIPAA or Applicable Law.
- FF-030: When "onlyCertainMatches"=true, return only one match if unique.
- FF-031: MUST NOT return more than 100 potential matches when “onlyCertainMatches”=false.
- FF-032: Initiating Nodes MUST include all available US Core Patient demographics in $match Query, excluding optional SSN.
- FF-033: Responding Nodes MAY request user-specified credentials if demographic matching fails, per the IAS XP Implementation SOP.
- FF-034: Initiating Nodes MUST populate Query elements per US Core vocabulary bindings.
- FF-035: Initiating Nodes MUST normalize addresses to Project US@, recommending preservation of non-street details.
- FF-036: Demographics in Queries and Responses MUST adhere to all US Core Patient Resource elements.
- FF-037: Responding Nodes MUST not require demographics beyond US Core for patient list Response.

Provenance Requirements

- FF-038: A US Core Provenance Resource MUST be available for Query for data transformed from another standard.
- FF-039: Responding Nodes MUST use US Core Provenance to record data source and transformations.
- FF-040: Provenance.target MUST reference all FHIR resources extracted from the cited document.
- FF-041: Provenance.policy MUST contain a specific static URI.
- FF-042: Provenance agent MUST include an entry for the extracting system.
- FF-043: Provenance.agent.type MUST use "assembler" code.
- FF-044: Provenance.agent.who SHOULD be a Device Resource; otherwise, use Organization.
- FF-045: Provenance entity MUST describe the source document.
- FF-046: Provenance.entity.role MUST be "source".
- FF-047: Provenance.entity.what MUST reference a DocumentReference to the original document.

6. Error and Response Handling

These requirements specify error responses and negotiation behaviors.

- Error Responses
- Scope Negotiation

Error Responses

- FF-058: When B2B Authorization Extension is insufficient, return invalid_grant with TEFCA-specific error extension (consent_required, consent_form optional).
- FF-080: If wildcard scopes not supported, respond with “invalid scope”.
- FF-083: Respond with “invalid scope” only if wildcard unsupported or no requested scopes supported.
- FF-088: Return “invalid scope” only if none of the scopes requested are available or not part of registration.

Scope Negotiation

- FF-076: Note on mandatory negotiation behavior for clients and servers.
- FF-077: scopes_supported metadata MUST list all supported scopes, including wildcards.
- FF-078: Client MAY request wildcard only if supported in metadata.
- FF-079: If wildcard supported, server SHOULD respond with wildcard or exploded list.
- FF-081: For OIDC/SMART scopes, SHOULD include a list of specific supported scopes in metadata.
- FF-082: Server MAY respond with fewer scopes than requested.
- FF-084: Server MAY respond with scopes not in requested set based on registration policies.
- FF-085: Scope list in grant request MAY match or subset registration.
- FF-086: Grant request MAY return full or subset of scopes.
- FF-087: Client application SHOULD handle superset of requested scopes.

Annual Meeting Reminder

2025 Annual Meeting Registration Open Now!

Eric Heflin

eHealth Exchange™

Keynote Speaker

We are honored to welcome CMS Deputy Administrator and COO, Kim Brandt, as the keynote speaker for the 2025 eHealth Exchange Annual Meeting.

Ms. Brandt will share insights on CMS's recently announced Make Health Tech Great Again initiative, including the CMS Interoperability Framework, strategies to advance payer–provider data exchange through new rules, efforts to align priorities across HHS, and the responsible use of AI in healthcare.

FEATURED SPEAKERS

We're proud to showcase an exceptional lineup of thought leaders and innovators who are shaping the future of health information exchange, interoperability, and public health.

ERICA OLENSKI

VP at Finn Partners

Founder & Executive Director of August's Artists

ABDEL MAHMOUD, MD

Founder & CEO

Anterior

KIM BRANDT

Deputy Administrator and COO

Centers of Medicare & Medicaid Services

RYAN HOWELLS

Principal

Leavitt Partners

KAT MCDAVITT

President & Founding Partner, Innsena

Host & Founder, Health Tech Talk Show

Press release dropped today.

Full Agenda available here.

Full Speaker list available here.

2025 Annual Meeting

- Back to Nashville, TN
- November 18, 2025
- Co-located again with The Sequoia Project and Carequality following November 19-20, 2025
- Embassy Suites by Hilton Downtown Nashville

Registration and Hotel Booking
2025 Annual Meeting - eHealth Exchange

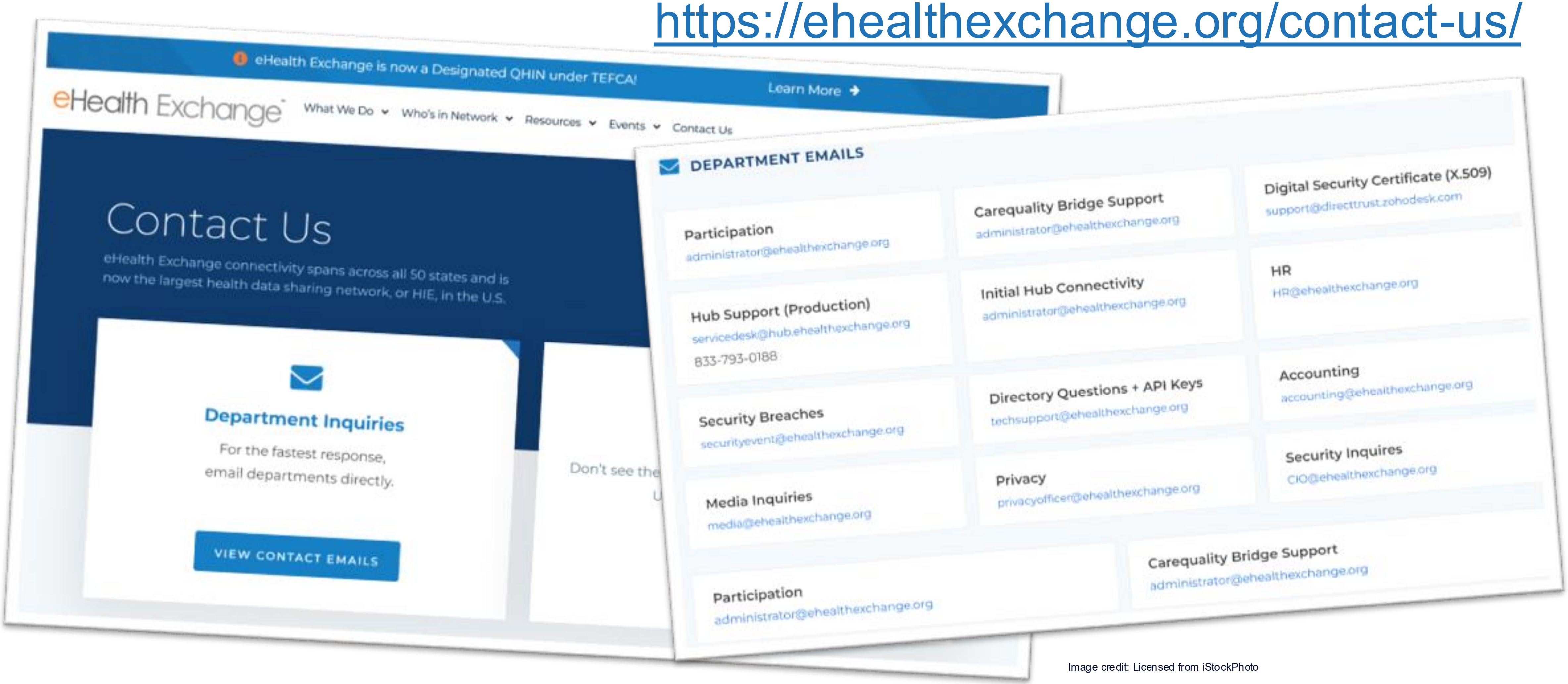
Public Feedback

Discussion

Questions

To Contact eHealth Exchange:

https://ehealthexchange.org/contact-us/



eHealth Exchange is now a Designated QHIN under TEFCA! Learn More

Contact Us

eHealth Exchange connectivity spans across all 50 states and is now the largest health data sharing network, or HIE, in the U.S.

Department Inquiries

For the fastest response, email departments directly.

VIEW CONTACT EMAILS

Don't see the

DEPARTMENT EMAILS

Participation
administrator@ehealthexchange.org

Carequality Bridge Support
administrator@ehealthexchange.org

Digital Security Certificate (X.509)
support@directtrust.zohodesk.com

Hub Support (Production)
servicedesk@hub.ehealthexchange.org
833-793-0188

Initial Hub Connectivity
administrator@ehealthexchange.org

HR
HR@ehealthexchange.org

Security Breaches
securityevent@ehealthexchange.org

Directory Questions + API Keys
techsupport@ehealthexchange.org

Accounting
accounting@ehealthexchange.org

Media Inquiries
media@ehealthexchange.org

Privacy
privacyofficer@ehealthexchange.org

Security Inquires
CIO@ehealthexchange.org

Participation
administrator@ehealthexchange.org

Carequality Bridge Support
administrator@ehealthexchange.org

Image credit: Licensed from iStockPhoto

Monthly Technical Work Group

Every 1st Thursday 4-5pm Eastern: email administrator@ehealthexchange.org for an invite

Typical Topics:

1. Technical Specifications
2. Testing
3. Hub Updates
4. Capacity planning

Request an invite: https://ehealthexchange.org/technical-workgroup-form/

How might I obtain assistance?

What	Who	How
Certificates	DirectTrust Support	support@directtrust.zohodesk.com
Hub and Hub Dashboard Assistance	Hub Service Desk	servicedesk@hub.ehealthexchange.org
Testing Questions	Testing Team	testing@ehealthexchange.org
Questions about the DURSA, policy, or anything else!	Administrator	administrator@ehealthexchange.org

Visit: https://ehealthexchange.org/contact-us/

eHealth Exchange™

ehealthexchange.org