ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

February 2, 2024

TEFCA Webinar 3:

New and Revised Standard Operating Procedures (SOPs), including Exchange Purpose (XP) Implementation SOPs

Zoe Barber, RCE Policy Director
Johnathan Coleman, RCE CISO
Didi Davis, RCE Conformance Testing
Lindsey Elkind, RCE Legal SME
Kathryn Lucia, RCE Policy Analyst
Dave Pyke, RCE Technical SME
Steve “Sully” Sullivan, RCE Program Operations
Alan Swenson, RCE Program Operations Lead
Erin Whaley, RCE Legal SME
Chantal Worzala, RCE Stakeholder Engagement
Mariann Yeager, RCE Lead

TEFCA Webinar 3: Agenda

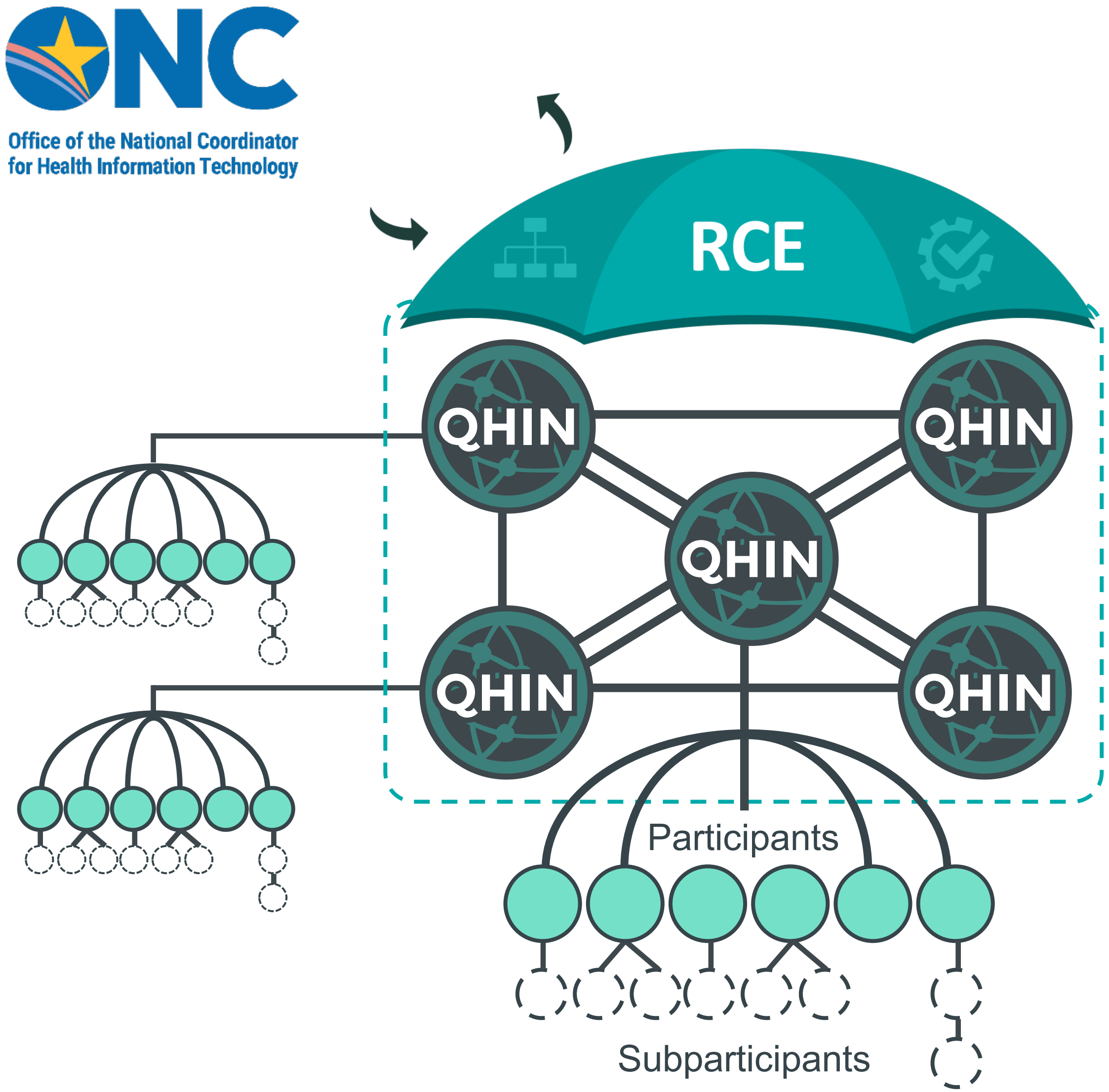
ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

- Review TEFCA℠ Exchange and Evolution
- Overview of Feedback Period and Process
- Overview of Documents Released for Feedback
- **Deep dive on:**
  - **Exchange Purposes (XPs) Standard Operating Procedure (SOP)**
  - **XP Implementation SOPs**
    - **XP Implementation SOP: Public Health SubXP-1**
    - **XP Implementation SOP: Health Care Operations SubXP-1**
- **Individual Access Services (IAS) SOPs**

TEFCA℠ is Live and Looking to the Future with FHIR®!

TEFCA Exchange

How Does Exchange Work Under TEFCA?


ONC
Office of the National Coordinator for Health Information Technology
RCE
QHIN
QHIN
QHIN
QHIN
QHIN
Participants
Subparticipants

ONC defines overall policy and certain governance requirements.

RCE^{TM} provides oversight and governing approach for QHINs.

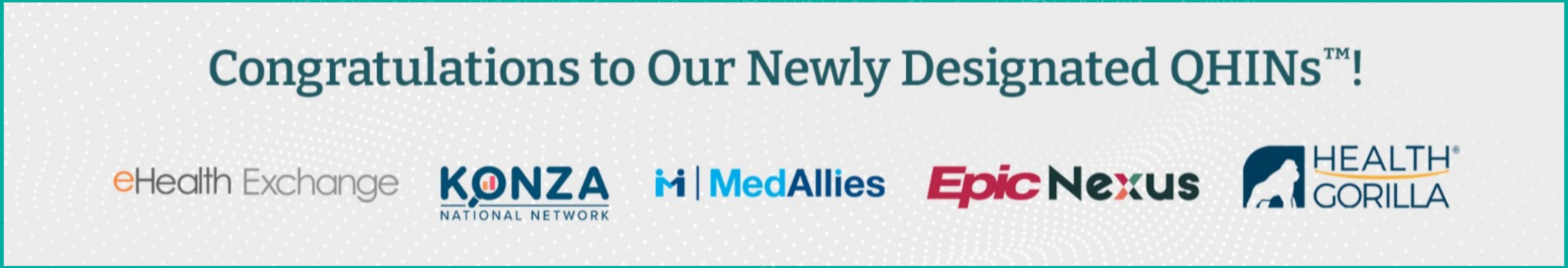
Qualified Health Information Networks^{TM} (QHINs^{TM}) connect directly to each other to facilitate nationwide interoperability.

Each QHIN connects Participants, which connect Subparticipants.

TEFCA Components

- Trusted Exchange Framework
- Framework Agreements
- Standard Operating Procedures
- QHIN Technical Framework
- QHIN Onboarding
- Metrics
- Governing Approach

TEFCA is Live!



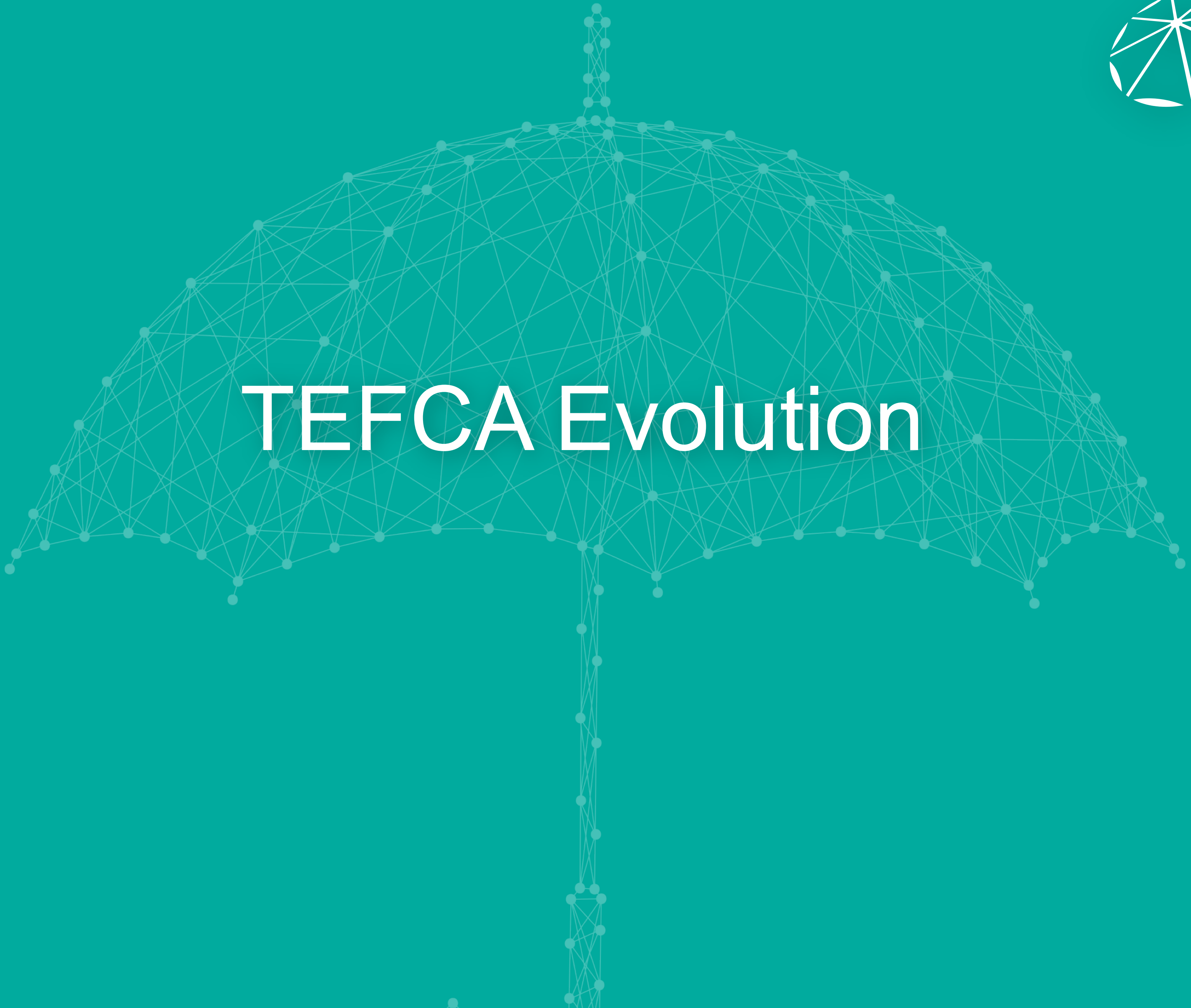
Congratulations to Our Newly Designated QHINs™!

Applicant QHINs include CommonWell Health Alliance, eClinicalWorks, Kno2, and Surescripts Health Information Network.

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

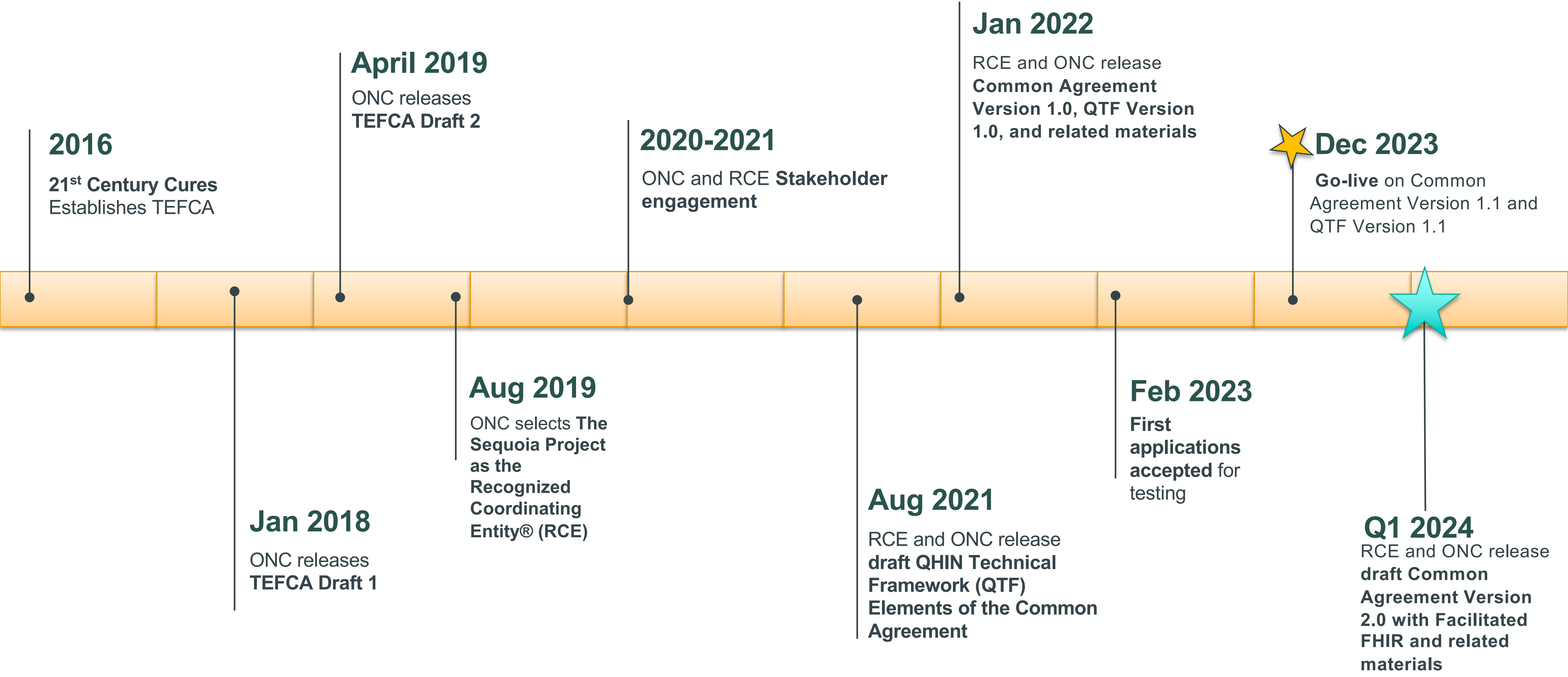
TEFCA is Looking to the Future

- Updates to technical and policy documents to support greater use of FHIR
- Better support for use cases beyond Treatment
- Stand-alone and static Terms of Participation to ease onboarding
- Ability to participate with multiple QHINs
- Restructuring to create flexibility for future change management



TEFCA Evolution

TEFCA Evolution



2016

21st Century Cures Establishes TEFCA

Jan 2018

ONC releases **TEFCA Draft 1**

April 2019

ONC releases **TEFCA Draft 2**

Aug 2019

ONC selects **The Sequoia Project as the Recognized Coordinating Entity® (RCE)**

2020-2021

ONC and RCE **Stakeholder engagement**

Aug 2021

RCE and ONC release **draft QHIN Technical Framework (QTF) Elements of the Common Agreement**

Jan 2022

RCE and ONC release **Common Agreement Version 1.0, QTF Version 1.0, and related materials**

Feb 2023

First applications accepted for testing

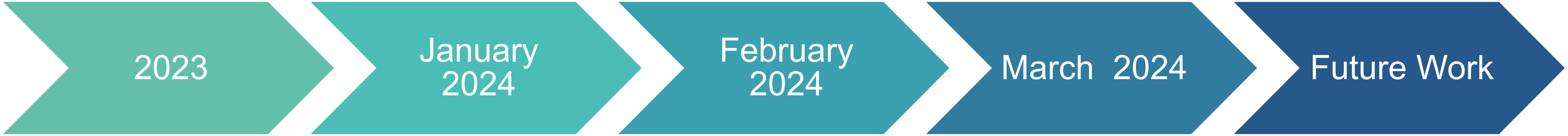
Dec 2023

Go-live on Common Agreement Version 1.1 and QTF Version 1.1

Q1 2024

RCE and ONC release **draft Common Agreement Version 2.0 with Facilitated FHIR and related materials**

Common Agreement and QTF Version 2.0 Evolution



2023

- Drafting Common Agreement Version 2.0 and related materials with RCE, ONC, TEFCA Task Team (Applicant QHINs), and Stakeholders

January 2024

- Documents for Stakeholder feedback released on 1/19/2024
- Public webinars:
  - 1/23/2024
  - 1/30/2024
  - 2/2/2024

February 2024

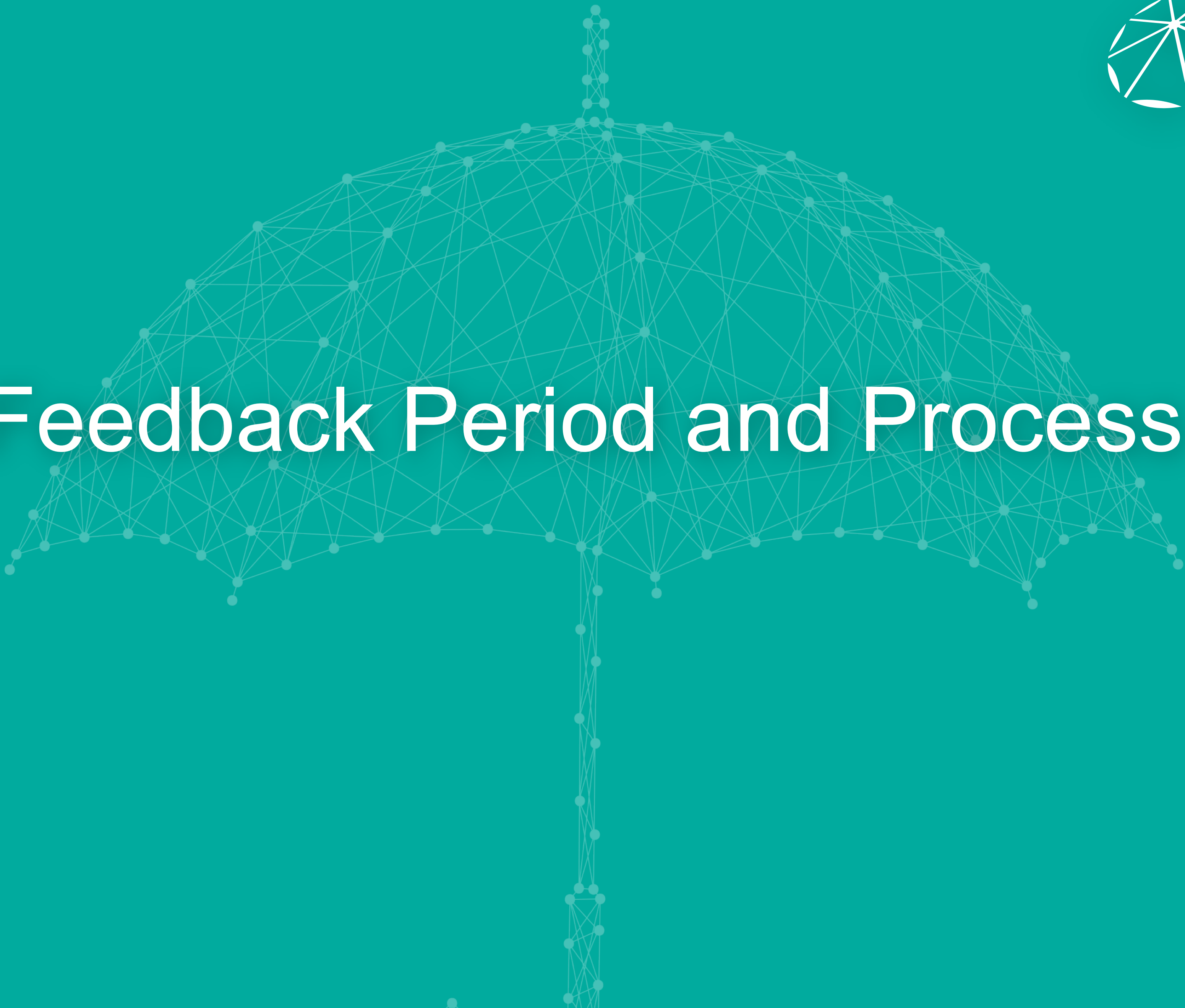
- Stakeholder feedback period ends 2/5/2024
- Ongoing targeted stakeholder input
- Transitional Council convenes 2/2/2024

March 2024

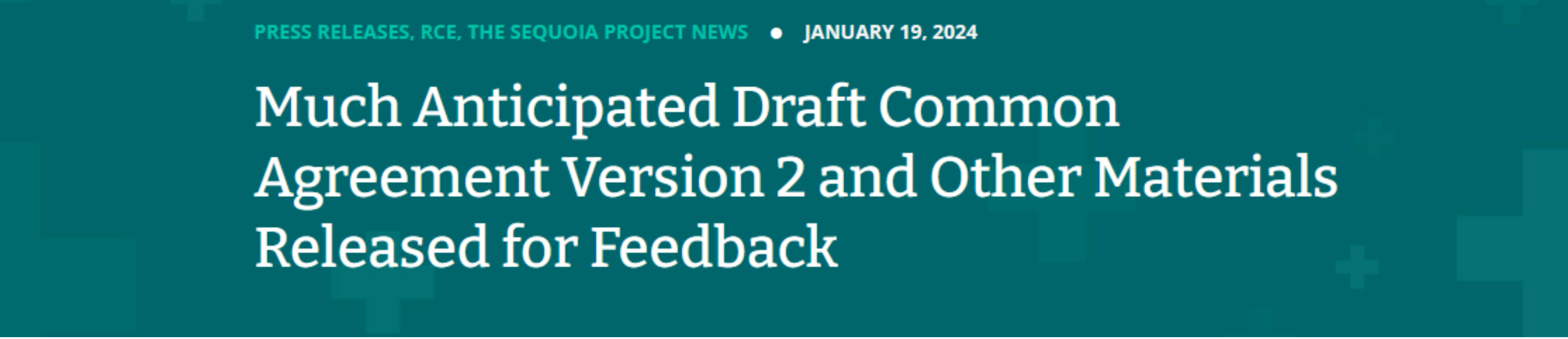
- Anticipated release of final Common Agreement Version 2.0, QTF Version 2.0, and SOPs end of Q1 2024

Future Work

- Additional Exchange Purpose (XP) Implementation SOPs
- Ongoing operations and change management



Feedback Period and Process



PRESS RELEASES, RCE, THE SEQUOIA PROJECT NEWS • JANUARY 19, 2024

Much Anticipated Draft Common Agreement Version 2 and Other Materials Released for Feedback

https://rce.sequoiaproject.org/rce-draft-documents-for-feedback/

- The RCE is seeking stakeholder input online through **Monday, February 5**. Stakeholders can submit input via the **feedback form on our website**, **email feedback to** rce@sequoiaproject.org,
  - The deadline for the XP Implementation SOP: Public Health SubXP-1 and the Public Health Educational Guidance Document has been extended to **Monday, February 12**
- The RCE will thoroughly review all feedback received via the webinars and online feedback forms for each document.
- The community is encouraged to submit comments all year long on the RCE website’s general feedback form.

Documents for Feedback

The RCE has released a set of draft materials in support of FHIR adoption and other advancements. These build from the existing framework and include:

Common Agreement Version 2.0

QHIN Technical Framework Version 2.0

Participant/Subparticipant Terms of Participation (ToP)

New Standard Operating Procedures (SOPs)

- Expectations for Cooperation
- Delegation of Authority
- Governance Approach
- XP Implementation SOP: Public Health (PH) SubXP-1
- RCE Directory Service Requirements Policy

Updated SOPs

- Exchange Purposes (XPs)
- XP Implementation SOP: Individual Access Services (IAS) Demographic Matched – *Updated from IAS Exchange Purpose Implementation*
- IAS Provider Requirements – *Updated from IAS Provider Privacy and Security Notice and Practices*
- XP Implementation SOP: Health Care Operations (HCO) SubXP-1 – *Updated from previously released draft*

New Explanatory Resources

- TEFCA Glossary
- TEFCA Cross Reference Resource

Common Agreement Versions At-a-Glance

ONC TEFCA RECOGNIZED COORDINATING ENTITY

January 2022

Common Agreement v1

The Common Agreement version 1 was the initial version of the Common Agreement and reflected policies developed with extensive public input.

Related QTF Version: 1
Related FHIR Roadmap Version: 1

December 2023

Common Agreement v1.1

The Common Agreement version 1.1 included changes required by HHS prior to TEFCA exchange going live. *This is the version in operation as of the official launch of TEFCA exchange.*

Related QTF Version: 1.1
Related FHIR Roadmap Version: 2

Common Agreement v2

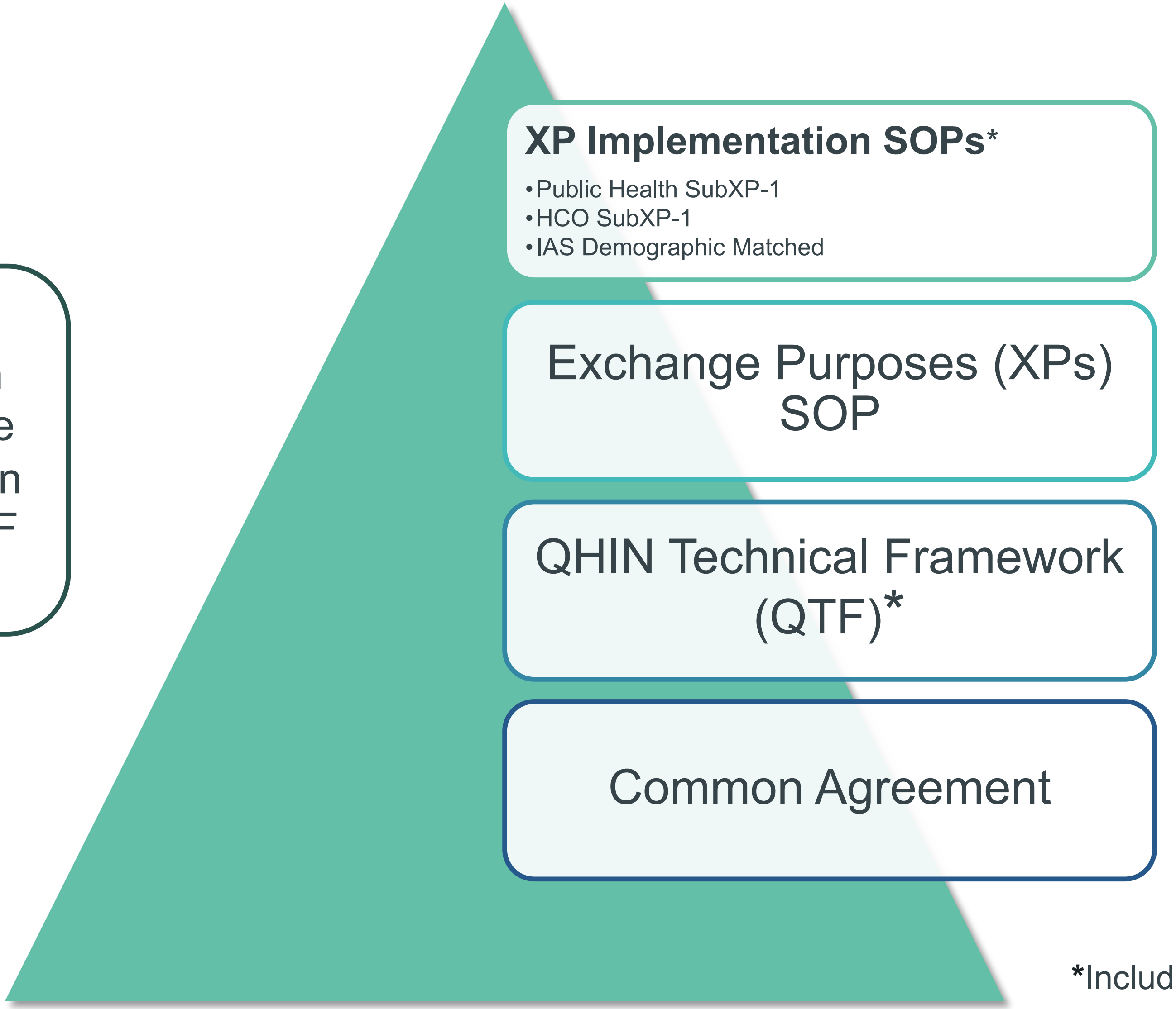
The Common Agreement version 2 will include enhancements and updates to require support of HL7 FHIR® based transactions.

Related QTF Version: 2 – DRAFT
Related FHIR Roadmap Version: 2

Exchange Purpose(s) or XP(s)

XP Implementation SOPs Foundation

XP Implementation SOPs build from the base of the Common Agreement and QTF



XP Implementation SOPs*

- Public Health SubXP-1
- HCO SubXP-1
- IAS Demographic Matched

Exchange Purposes (XPs) SOP

QHIN Technical Framework (QTF)*

Common Agreement

*Includes references to industry standards

Exchange Purpose(s) or XP(s)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Table 1 TEFCA XP Codes

Display Value	Code
Treatment	T-TRTMNT
Payment	T-PYMNT
Health Care Operations	T-HCO
Health Care Operations SubXP-1	T-HCO1
Public Health	T-PH
Public Health SubXP-1	
Electronic Case Reporting	T-PH-ECR
Electronic Lab Reporting	T-PH-ELR
Other Electronic Disease/ Condition Reporting	T-PH-EDR
Electronic Case Investigation	T-PH-ECI
Individual Access Services	T-IAS
Government Benefits Determination	T-GOVDTRM

Treatment

Payment

Health Care Operations

- Health Care Operations SubXP-1

Individual Access Services

Public Health

- Public Health SubXP-1

Government Benefits Determination

XP Implementation SOPs: Overview

New XP Implementation: Health Care Operations SubXP-1

- SubXP-1 definition mirrors that in 45 CFR 164.501 Health Care Operations definition section (1)
- Responding Nodes with a FHIR Endpoint MUST Respond to FHIR Queries for HCO SubXP-1

New XP Implementation: Public Health SubXP-1

- Electronic Case Investigation and Electronic Disease/Condition Reporting (e.g., Electronic Case Reporting and Electronic Lab Reporting)
- Responding Nodes SHOULD respond to Requests for Case Investigation, in accordance with the Common Agreement and Applicable Law

Updated XP Implementation SOP: Individual Access Services (IAS): Demographic Matched

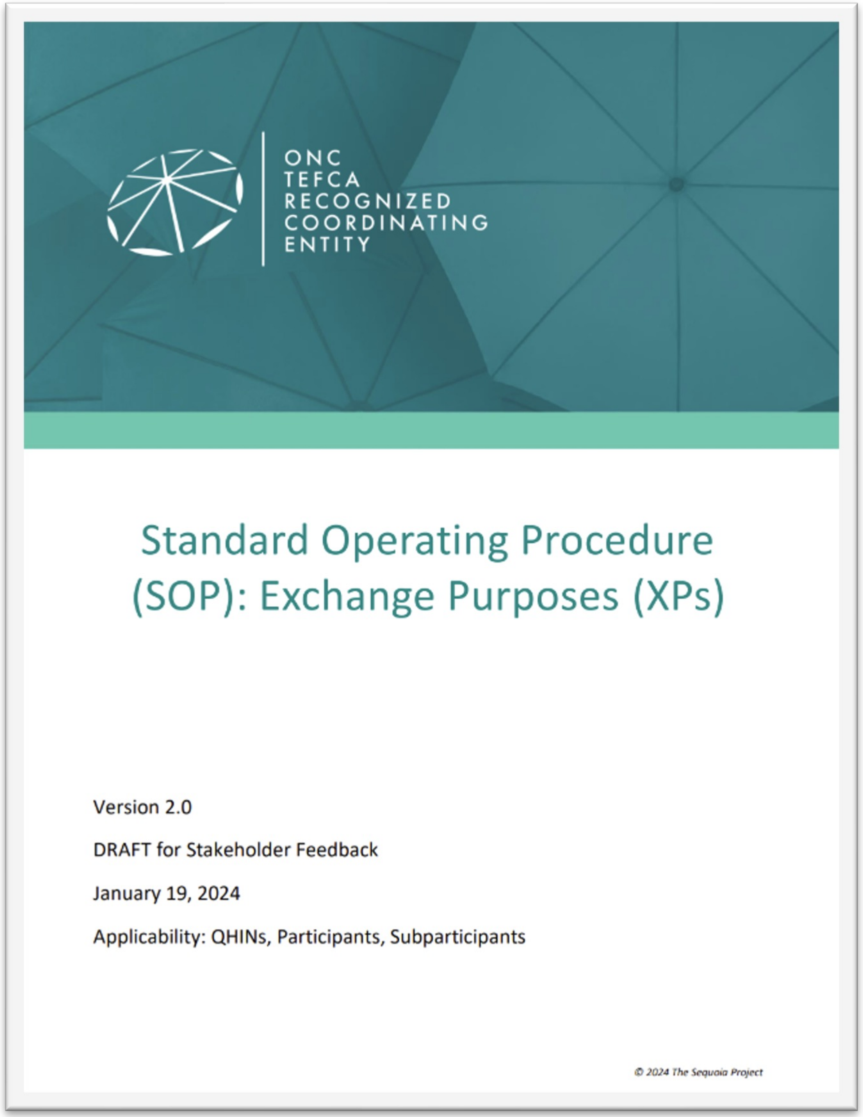
- Any Responding Node that receives a Request from an IAS Provider that includes the appropriate IAL2 Claims Token, and that achieves an acceptable demographics-based match based on responder policy MUST Respond
- Requirements for IAS Requests made using FHIR/OAuth with responder-issued credentials are out of scope for this SOP

Updated from IAS Exchange Purpose Implementation

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Exchange Purposes (XPs) SOP

Exchange Purposes (XPs) SOP Overview


ONC TEFCA RECOGNIZED COORDINATING ENTITY

Standard Operating Procedure (SOP): Exchange Purposes (XPs)

Version 2.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability: QHINs, Participants, Subparticipants

© 2024 The Sequoia Project

Purpose:

This Exchange Purposes (XPs) SOP defines the XPs and sets forth any limitations on the types of Participants or Subparticipants that can utilize such XP. It also identifies any XPs for which a Response is required pursuant to the Common Agreement.

SOP Sections:

1. Common Agreement References
2. SOP Definitions
3. Purpose
4. Procedure
   - 4.1 Authorized Exchange Purposes
   - 4.2 Exchange Purpose Codes
   - 4.3 Limitations on Types of Participants/Subparticipants
   - 4.4 Required Support
   - 4.5 Required Responses
   - 4.6 Exceptions to Required Responses

Exchange Purposes (XPs) SOP Relevant Definitions (1)

- **Government Benefits Determination**: a determination made by any federal, State, local, or tribal agency, instrumentality, or other unit of government as to whether an Individual qualifies for government benefits for any purpose other than health care (for example, Social Security disability benefits) to the extent permitted by Applicable Law. Disclosure of TI for this purpose may require an authorization that complies with Applicable Law.

- **Health Care Operations:** has the meaning assigned to such term at 45 CFR § 164.501, except that this term shall apply to the applicable activities of a Health Care Provider regardless of whether the Health Care Provider is a Covered Entity.

- **Individual Access Services (IAS):** the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant, or Subparticipant, as applicable, agrees to satisfy that Individual's ability to use TEFCA Exchange to access, inspect, obtain, or transmit a copy of that Individual's Required Information.

Exchange Purposes (XPs) SOP Relevant Definitions (2)

- **Payment:** has the meaning assigned to such term at 45 CFR § 164.501.
- **Public Health:** with respect to the definition of Exchange Purposes (XPs), a Request, Use, Disclosure, or Response permitted under the HIPAA Rules and other Applicable Law for public health activities and purposes involving a Public Health Authority, where such public health activities and purposes are permitted by Applicable Law, including a Use or Disclosure permitted under 45 CFR § 164.512(b) and 45 CFR § 164.514. For the avoidance of doubt, a Public Health Authority may Request, Use, and Disclose TEFCA Information (TI) hereunder for Public Health to the extent permitted by Applicable Law and the Framework Agreements.
- **Treatment:** has the meaning assigned to such term at 45 CFR § 164.501.

Exchange Purposes (XPs) SOP Procedure

4.1 Authorized Exchange Purposes (XPs)

- The authorized XPs are:
  - Treatment
  - Payment
  - Health Care Operations (including HCO SubXP-1)
  - Public Health (including PH SubXP-1)
  - Government Benefits Determination
  - Individual Access Services

4.2 Exchange Purpose Codes (XP Codes)

- Each transaction MUST be accompanied by the appropriate TEFCA XP Code in the table below

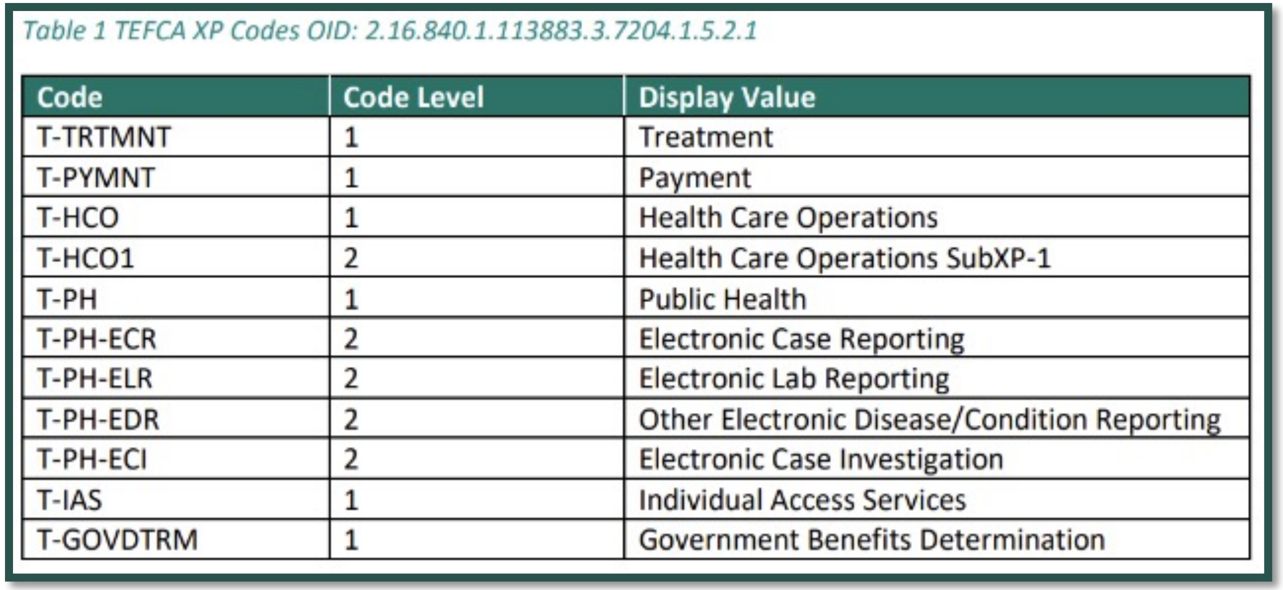


Table 1 TEFCA XP Codes OID: 2.16.840.1.113883.3.7204.1.5.2.1

Code	Code Level	Display Value
T-TRTMNT	1	Treatment
T-PYMNT	1	Payment
T-HCO	1	Health Care Operations
T-HCO1	2	Health Care Operations SubXP-1
T-PH	1	Public Health
T-PH-ECR	2	Electronic Case Reporting
T-PH-ELR	2	Electronic Lab Reporting
T-PH-EDR	2	Other Electronic Disease/Condition Reporting
T-PH-ECI	2	Electronic Case Investigation
T-IAS	1	Individual Access Services
T-GOVDTRM	1	Government Benefits Determination

Exchange Purposes (XPs) SOP Procedure

4.3 Limitations on Types of Participants/Subparticipants

a. Initiating Nodes may only Request information for a specific XP if the Initiating Node is controlled by a QHIN, Participant, or Subparticipant that is the type of entity or person that is authorized by Applicable Law to assert Requests for the applicable XP. For example:

   i. Only Health Care Providers may assert Treatment for a Request

   ii. Only a federal, state, local, or tribal agency, instrumentality, or other unit of government may assert Government Benefits Determination for a Request

b. Notwithstanding the foregoing, a Principal may use a Delegate to make such Request or transact for the applicable XP, provided that the Principal has in place a written agreement with the Delegate that authorizes the Delegate to make such Request or transact for the applicable XP.

Exchange Purposes (XPs) SOP Procedure

4.4 Required Support

a. For purposes of this SOP, “support” means the technical capability to:

   i. Receive and respond to transactions from QHINs, Participants, and Subparticipants via TEFCA Exchange, including transmitting all information that a QHIN, Participant, or Subparticipant may send via TEFCA Exchange related to any XP (e.g., the content of the packet itself, if any)

b. QHIN MUST support all the XPs.

c. Responding Nodes MUST support any XP that they are required to Respond to per Section 4.5 of the SOP, and they may support any that are authorized per Section 4.1 of the SOP.

Exchange Purposes (XPs) SOP Procedure

4.5 Required Responses

a. Responding Nodes of Principals MUST Respond to Requests for the XPs listed in Section 4.5c of this SOP, except to the extent that one or more of the exceptions applies as set forth in Section 4.6 of this SOP.

b. Responding Nodes of Delegates MUST Respond to Requests for the XPs listed in Section 4.5(c) below, if authorized by the written agreement authorizing the Delegate to conduct TEFCA Exchange for the Principal, except to the extent that one or more of the exceptions applies as set forth in Section 4.6 of this SOP.

c. The XPs that require a Response to a Request are as follows:

   i. Treatment
   ii. Individual Access Services
   iii. Healthcare Operations SubXP-1 if the Request is received via FHIR Query

d. Responding Nodes are permitted to Respond to all authorized XPs in Section 4.1 and not listed in 4.5(c).

Exchange Purposes (XPs) SOP Procedure

4.6 Exceptions to Required Responses

i. The Response is prohibited by Applicable Law; is inconsistent with Signatory’s Privacy and Security Notice, if applicable; or is not in accordance with the Common Agreement;

ii. If the Responding Node is controlled by a Public Health Authority;

iii. If the Responding Node is controlled by a federal, state, local, or tribal agency, instrumentality, or other unit of government, including such government agency’s agent(s) and contractor(s), using TEFCA Exchange solely for purposes of Requesting information for Government Benefits Determination;

iv. If the reason asserted for the Request is Individual Access Services and the information would not be required to be provided to an Individual pursuant to 45 CFR § 164.524(a)(2), regardless of whether the Responding Node is controlled by a Non-HIPAA Entity or a Covered Entity or a Business Associate;

Exchange Purposes (XPs) SOP Procedure

4.6 Exceptions to Required Responses

v. If the Requested information is not Required Information, provided such Response would not otherwise violate the terms of this Common Agreement;

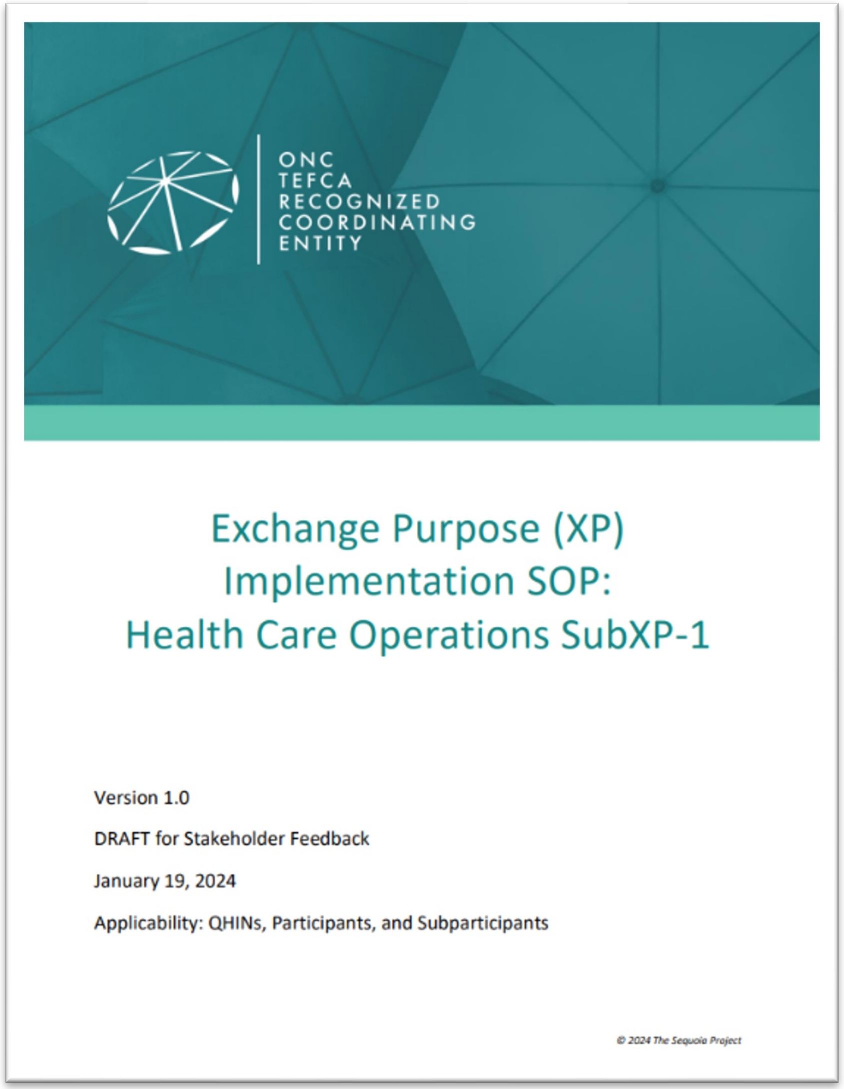
vi. If the Responding Node is controlled by a federal agency, to the extent that the Requested Disclosure of Required Information is not permitted under Applicable Law (e.g., it is Controlled Unclassified Information as defined at 32 CFR Part 2002, and the party requesting it does not comply with the applicable policies and controls that the federal agency adopted to satisfy its requirements);

vii. If the XP is authorized but not required at the time of the Request, either under this SOP or the Common Agreement; or

viii. An applicable SOP exempts the Response.

XP Implementation SOP: Health Care Operations (HCO) SubXP-1

XP Implementation SOP: Health Care Operations (HCO) SubXP-1 Overview



ONC TEFCA RECOGNIZED COORDINATING ENTITY

Exchange Purpose (XP)
Implementation SOP:
Health Care Operations SubXP-1

Version 1.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability: QHINs, Participants, and Subparticipants

© 2024 The Sequoia Project

Purpose

This SOP defines the Health Care Operations (HCO) SubXP-1, which is a subset of Health Care Operations, as defined in the Exchange Purposes (XPs) SOP. In addition to the Common Agreement, QTF, and applicable SOPs, this SOP identifies specific requirements that QHINs, Participants, and Subparticipants must follow when asserting HCO SubXP-1 for TEFCA Exchange.

SOP Sections:

1. Common Agreement References
2. SOP Definitions
3. Purpose
4. Procedure
   - 4.1 Exchange Purpose (XP)
   - 4.2 QHIN Technical Framework (QTF)
   - 4.3 QHIN Message Delivery
   - 4.4 QHIN Query
   - 4.5 Facilitated FHIR
   - 4.6 RCE Directory Services

XP Implementation SOP: HCO SubXP-1 SOP Relevant Definitions

- **Health Plan:** has the meaning assigned to such term at 45 CFR § 164.501.
- **Health Plan Parent:** the QHIN, Participant, or Subparticipant of which the Health Plan(s) is a part.
- **Health Care Operations (HCO) SubXP-1**: means transactions for any of the following activities, under TEFCA Exchange, to the extent permitted by Applicable Law and the Common Agreement:

  Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment. [1]

[1] This language mirrors that in 45 CFR 164.501 Health Care Operations definition section (1).

4.6 RCE Directory Service

- A Health Plan Parent listed in the RCE Directory Service MUST publish all of its participating Health Plans to the RCE Directory in order to identify the source of a Request as required in Section 4.4.1 and Section 4.5.1 of this SOP.

XP Implementation SOP: HCO SubXP-1 SOP Procedure

4.1 Exchange Purpose Code (XP Code)

- All TEFCA Exchange under HCO SubXP-1 MUST use the XP Code T-HCO1. For HCO purposes that are not covered by this or a subsequent XP Implementation SOP, TEFCA Exchange MUST use the more general T-HCO code, as defined in the Exchange Purposes (XPs) SOP.

4.2 QHIN Technical Framework

- All TEFCA Exchange under HCO SubXP-1 MUST follow technical requirements as specified in the QTF.

XP Implementation SOP: Health Care Operations SubXP-1
Transaction Types and Permitted Users

ONC TEFCA RECOGNIZED COORDINATING ENTITY

This SOP supports TEFCA Exchange in the form of a QHIN Message Delivery, QHIN Query, or Facilitated FHIR Query/Push between Nodes published in the RCE Directory Service, in accordance with Applicable Law and the Common Agreement.

- **Section 4.3 QHIN Message Delivery**
  - Any Initiating Node → Any Responding Node, in accordance with Applicable Law and the Common Agreement.
- **Section 4.4 QHIN Query**
  - Only Initiating Nodes of Health Plans and Health Care Providers that are Covered Entities or their Delegates may Request Required Information under HCO SubXP-1, in accordance with Applicable Law and the Common Agreement.
- **Section 4.5 Facilitated FHIR**
  - FHIR Query
    - Only Initiating Nodes of Health Plans and Health Care Providers that are Covered Entities or their Delegates may Request Required Information under HCO SubXP-1, in accordance with Applicable Law and the Common Agreement.
  - FHIR Push
    - Any Initiating Node → Any Responding Node, in accordance with Applicable Law and the Common Agreement.

XP Implementation SOP: HCO SubXP-1 SOP Procedure

4.4.1 QHIN Query Request

a) Requestors MUST specify the date range for the requested data.

b) Requestor Identifying Information
   (i) If the Request is originating from a Health Care Provider, it MUST include:
      a. the Health Care Provider's individual or organizational National Provider Identifier (NPI) and/or Tax Identification Number (TIN), as applicable; and
         1. The NPI Attribute MUST be encoded in the SAML attributes with a FriendlyName of NPI and MUST be NameFormat urn:oasis:names:tc:xspa:2.0:subject:npi.
         2. The TIN attribute MUST be encoded in the SAML attributes with a FriendlyName of TIN and MUST be NameFormat urn:nhin:names:saml:tin.
   (ii) If the Request is originating from a Health Plan, it MUST include:
      a. the Health Plan's National Association of Insurance Commissioners (NAIC) Code, if available;
         1. the NAIC code MUST be encoded in the SAML attributes with a FriendlyName of NAIC and MUST be NameFormat .urn:nhin:names:saml:naic.
      b. the RCE Directory Organization.ID of the Health Plan or of the Health Plan Parent.
         1. This <Attribute> element shall have the Name attribute set to urn:oasis:names:tc:xspa:1.0:subject:organization-id with FriendlyName set to FHIRInitiating. The value shall be the Resource ID of the Organization entry in the RCE Directory for the entity that is initiating the Request.

c) Patient Identifying Information
   (i) Requestors MUST include the Individual's Member ID and/or Subscriber ID, if known, as additional patient identifiers in the Request. See the Health Insurance Information data class in USCDI v3 available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#uscdi-v3

XP Implementation SOP: HCO SubXP-1 SOP Procedure

4.4.2 QHIN Query Response

a) All Responding Nodes SHOULD respond to QHIN Query Requests for HCO SubXP-1 that contain the information specified in this SOP, in accordance with the Common Agreement and Applicable Law.

b) If a Responding Node responds to a Request for HCO SubXP-1, then it MUST respond with all Required Information that it maintains, that are within the parameters of the Request, in accordance with Applicable Law, including, but not limited to:

   (i) The data classes and data elements, as identified in USCDI v1
   (ii) Adjudicated claims

a) For any Social Determinants of Health (SDOH) data elements, Responding Node MUST include the SDOH Z ICD-10-CM SDOH encounter reason codes ("Z-Codes"), if available, in addition to any other codes, as appropriate.

Data classes and data elements available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#uscdi-v1.

XP Implementation SOP: HCO SubXP-1 SOP Procedure

ONC TEFCA RECOGNIZED COORDINATING ENTITY

4.5.1 Facilitated FHIR Query

a) If the Request is originating from a Health Care Provider, it MUST include, as part of the United Data Access Profiles (UDAP) authorization and authentication flow in the FHIR Security IG OAuth hl7-b2b extension:

b) the Health Care Provider's individual or organizational NPI and/or TIN, as applicable, appended to the Human readable name within organization_name; and

    (i) the ResourceID of the Organization entry in the RCE Directory of the Health Care Provider as organization_id

c) If the Request is originating from a Health Plan, it MUST include:

    a. the Health Plan's NAIC Code, if available, appended to the Human readable name within organization_name

        a. If no NAIC is available, 000000 MUST be appended.

    b. the ResourceID of the Organization entry in the RCE Directory of the Health Plan or of the Health Plan Parent, as organization_id

d) The Individual's Member ID and/or Subscriber ID, if known, as additional patient identifiers in the Request Patient resource. The member ID/subscriber ID Patient.identifier code MUST be of system http://hl7.org/fhir/us/davinci-hrex/CodeSystem/hrex-temp and code umb.

Implementation Guide available at https://hl7.org/fhir/us/udap-security/.

4.5.2 Facilitated FHIR Response

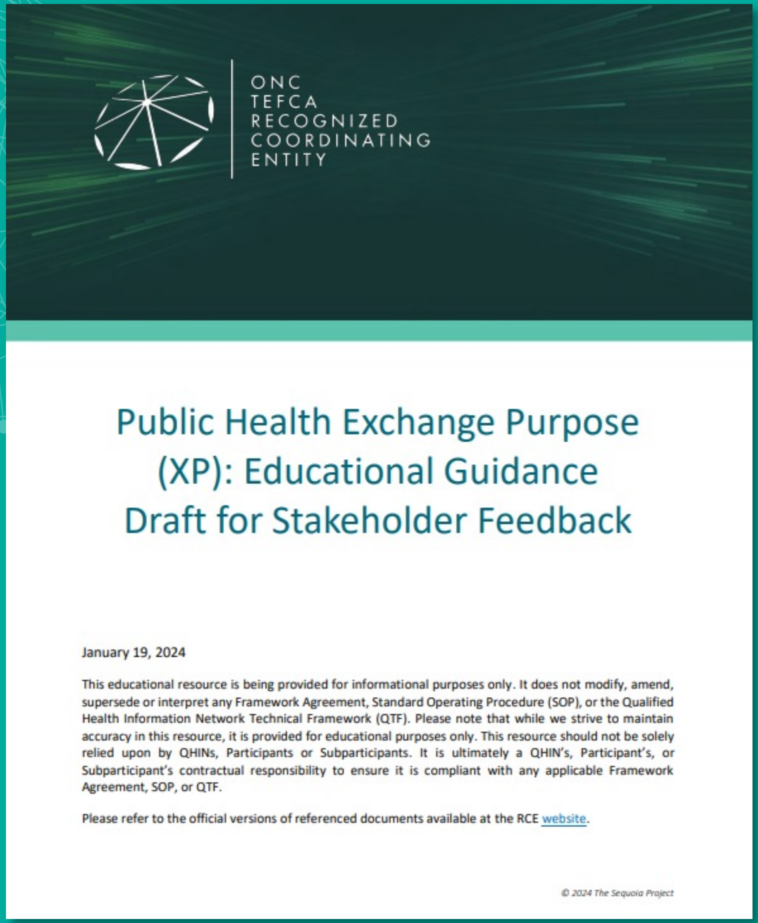
a) All Responding Nodes with a FHIR Endpoint in the RCE Directory Service MUST use that FHIR Endpoint to Respond to Facilitated FHIR Queries for HCO SubXP-1 that contain the information in Section 4.5.1 of this SOP.

b) All Responding Nodes with a FHIR Endpoint in the RCE Directory Service MUST Respond with all Required Information it maintains that are within the parameters of the Request, in accordance with Applicable Law, including but not limited to:
   (i) The data classes and data elements, as identified in USCDI v1
   (ii) Adjudicated claims

c) Responses containing adjudicated claims data SHOULD abide by the requirements in the following implementation guides:
   (i) CARIN for Blue Button IG Version 2.0.0
   (ii) HL7 Da Vinci Payer Data Exchange FHIR Implementation Guide Version 1.0.0
   (iii) HL7 Da Vinci Payer Data Exchange FHIR U.S. Drug Formulary Implementation Guide Version 2.0.0

Data classes and data elements available at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi#uscdi-v1.
Implementation Guide available at https://hl7.org/fhir/us/carin-bb/.
Implementation Guide available at https://hl7.org/fhir/us/davinci-pdex/index.html.
Implementation Guide available at https://hl7.org/fhir/us/davinci-drug-formulary/.

XP Implementation SOP: Public Health SubXP-1



ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Public Health Exchange Purpose
(XP): Educational Guidance
Draft for Stakeholder Feedback

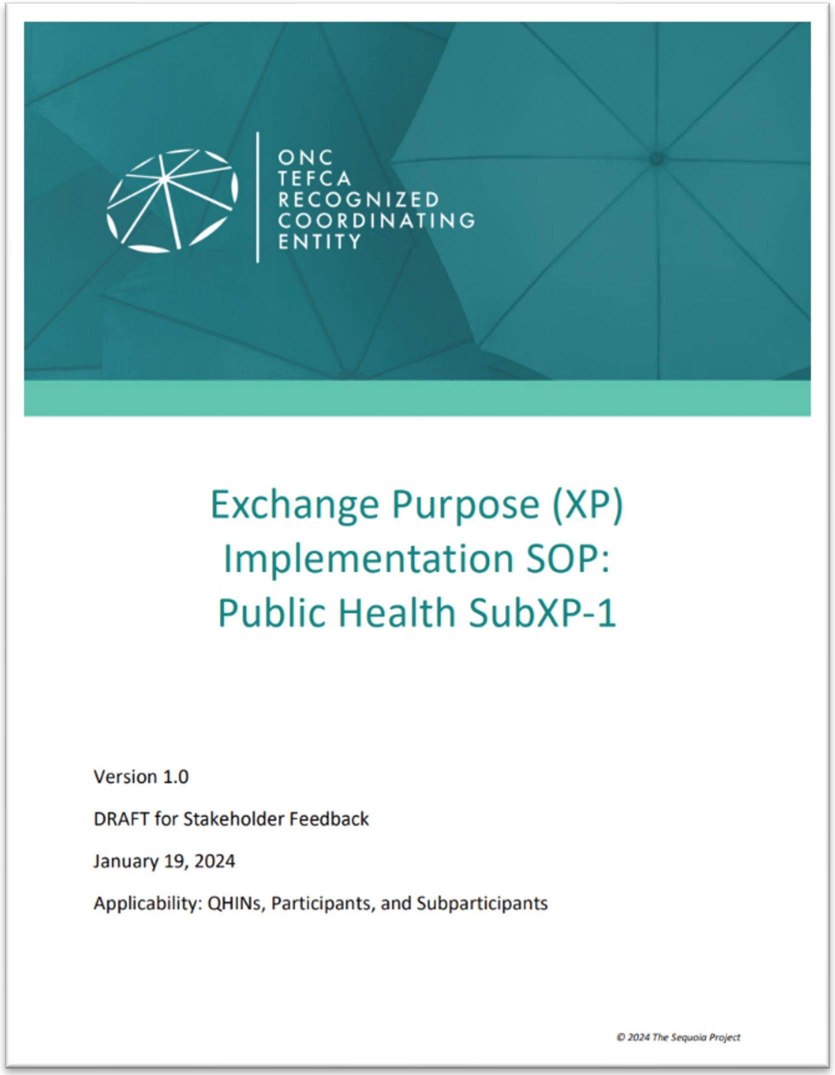
January 19, 2024

This educational resource is being provided for informational purposes only. It does not modify, amend, supersede or interpret any Framework Agreement, Standard Operating Procedure (SOP), or the Qualified Health Information Network Technical Framework (QTF). Please note that while we strive to maintain accuracy in this resource, it is provided for educational purposes only. This resource should not be solely relied upon by QHINs, Participants or Subparticipants. It is ultimately a QHIN's, Participant's, or Subparticipant's contractual responsibility to ensure it is compliant with any applicable Framework Agreement, SOP, or QTF.

Please refer to the official versions of referenced documents available at the RCE website.

© 2024 The Sequoia Project

Public Health SubXP-1 SOP Overview



ONC TEFCA RECOGNIZED COORDINATING ENTITY

Exchange Purpose (XP) Implementation SOP: Public Health SubXP-1

Version 1.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability: QHINs, Participants, and Subparticipants

Purpose

This SOP defines the Public Health SubXP-1, which is a subset of Public Health, as defined in the Exchange Purposes (XPs) SOP. In addition to the Common Agreement and QTF, this SOP identifies requirements that QHINs, Participants, and Subparticipants are required to follow when asserting the Public Health SubXP-1 described herein for TEFCA Exchange transactions.

SOP Sections:

1. Common Agreement References
2. SOP Definitions
3. Purpose
4. Procedure
   - 4.1 Exchange Purpose (XP)
   - 4.2 QHIN Technical Framework (QTF)
   - 4.3 Alternative Uses
   - 4.4 QHIN Message Delivery
   - 4.5 QHIN Query
   - 4.6 Facilitated FHIR

Public Health SubXP-1 SOP Relevant Definitions

Public Health SubXP-1 includes transactions for any of the following Public Health activities via TEFCA Exchange, to the extent permitted by Applicable Law and the Common Agreement.

- **Electronic Disease Reporting:** (e.g., Electronic Case Reporting and Electronic Lab Reporting): Public Health Authorities (PHAs) are generally required by Applicable Law to monitor, investigate, mitigate, and otherwise act to prevent the introduction or spread of diseases and conditions that endanger the public health in their jurisdictions. To facilitate this duty, physicians, clinical laboratories, and other healthcare organizations are often mandated by Applicable Law to report certain diseases and conditions and/or certain indicators thereof. The use of electronic case and lab reporting streamlines this mandated reporting process for healthcare providers and PHAs alike.

- **Electronic Case Investigation:** is a public health tool that involves a PHA gathering additional information in response to a disease or condition that has already been reported under Applicable Law. This often includes collecting information about the individual's symptoms, their clinical characteristics/history, how/where they may have contracted or acquired the disease/condition, and the overall course of their illness, including clinical interventions received. These investigations help PHAs understand and mitigate the extent to which other people or groups may be at risk. The ability to gather information for case investigation electronically vastly improves the efficacy of these investigations. This includes the ability of a PHA to query healthcare providers and others for additional information for case investigation in follow-up to a PHA's receipt of an electronic disease report.

Definitions derived from those included in: https://www.crisphealth.org/wp-content/uploads/2022/01/Approved_Use-Case-Disease-Investigation-Updated_2021.pdf.

Public Health SubXP-1 SOP Procedure

4.1 Exchange Purpose Codes (XP Codes)

- All TEFCA Exchange under Public Health SubXP-1 MUST use the appropriate XP Code matching the use case for exchange, as specified in Table 1. For Public Health purposes that are not covered by this or a subsequent XP Implementation SOP, TEFCA Exchange MUST use the more general T-PH code, as defined in the Exchange Purposes (XPs) SOP.

Table 1 Public Health Sub Exchange Purpose Codes (XP Codes)

Use Case	XP Code
Electronic Case Reporting	T-PH-ECR
Electronic Lab Reporting	T-PH-ELR
Other Electronic Disease/Condition Reporting	T-PH-DR
Electronic Case Investigation	T-PH-CI

4.2 QHIN Technical Framework

- All transactions under Public Health SubXP-1 MUST follow technical requirements as specified in the QTF.

Public Health SubXP-1 SOP Procedure

4.3 Alternate Uses

a) Information transacted for purposes under Public Health SubXP-1 MUST NOT be persisted by any Node along the transaction chain that is not the addressed recipient, unless agreed to by the data source or recipient through a specific written agreement.

b) Information transacted for purposes of Public Health SubXP-1 MUST NOT be used for any other purpose beyond that of required audit by any Node along the transaction chain that is not the addressed recipient, unless agreed to by the data source or recipient through a specific written agreement.

Public Health SubXP-1 SOP
Transaction Types and Permitted Users

This SOP supports TEFCA Exchange in the form of a QHIN Message Delivery, QHIN Query, or Facilitated FHIR Query/Push between Nodes published in the RCE Directory Service, in accordance with Applicable Law and the Common Agreement.

- **Section 4.4 QHIN Message Delivery**
  - Any Initiating Node → a Responding Node of a Public Health Authority (PHA) or its Delegate, in accordance with Applicable Law and the Common Agreement.
- **Section 4.5 QHIN Query**
  - Only Initiating Nodes of a PHA or its Delegate may Request Required Information for PH SubXP-1, in accordance with Applicable Law and the Common Agreement.
- **Section 4.6 Facilitated FHIR**
  - FHIR Query
    - Only Initiating Nodes of a PHA or its Delegate with a FHIR Endpoint may Request Required Information for PH SubXP-1, in accordance with Applicable Law and the Common Agreement.
  - FHIR Push
    - Any Initiating Node with a FHIR Endpoint → a Responding Node of a Public Health Authority (PHA) or its Delegate, in accordance with Applicable Law and the Common Agreement.

Public Health SubXP-1 SOP Procedure

ONC TEFCA RECOGNIZED COORDINATING ENTITY

4.4 QHIN Message Delivery

a) An Initiating Node MUST only send Message Deliveries to a PHA or its Delegate, or other Responding Node, that is listed in the RCE Directory Service as capable of receiving Message Deliveries.

b) All Initiating Nodes MUST include its OrganizationID in addition to its HomeCommunityID within the SAML information.

```
<saml:Attribute FriendlyName="RCEDirectoryID"
Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
<saml:AttributeValue>https://directory.prod.rce.sequoiaproject.org/Organiz
ation/f40f2693-6b8e-4691-ae1d-47c63c88c486</saml:AttributeValue>
</saml:Attribute>
```

c) If an Initiating Node sends a Message Delivery for a use case that requires or includes Reportability Response, the Initiating Node MUST support the required Reportability Response standards, as specified in Table 2

d) For each of the specified SubXP Codes in Section 4.1 of the SOP, Initiating Nodes MUST use the appropriate, corresponding content standards, as specified below for Integrating the Healthcare Enterprise (IHE) standards-based transactions

Table 2 QHIN Message Delivery Use Case Document Standards

Use Case	Document Standard
Electronic Case Reporting	**Health Care Providers:** HL7 CDA® R2 Implementation Guide: Public Health Case Report - the Electronic Initial Case Report (eICR) Release 2, STU Release 3.1 **Public Health Authorities and Delegates:** HL7 CDA® R2 Implementation Guide: Reportability Response, Release 1, STU Release 1.1 - US Realm
Electronic Lab Reporting	HL7 Version 2.5.1 Implementation Guide: Electronic Laboratory Reporting to Public Health, Release 1 (US Realm)
Other Electronic Disease/Condition Reporting	As required by PHA policy

Public Health SubXP-1 SOP Procedure

4.5 QHIN Query

- Only Initiating Nodes of a PHA or its Delegate may initiate a QHIN Query for the purposes listed under Section 4.1 of the SOP, in accordance with Applicable Law and the Common Agreement.

4.5.1 QHIN Query Request

a. The Query MUST include the jurisdiction the PHA represents

```
<saml:Attribute FriendlyName="PHAJurisdiction" Name="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
<saml:AttributeValue>HazzardCounty</saml:AttributeValue>
</saml:Attribute>
```

b. Queries SHOULD include a date range for a period of no more than 5 years in the QHIN Query metadata. If omitted, a period of 5 years SHOULD be assumed

c. Queries MUST include the Public Health Authority Organization.ID as follows:

```
<saml:Attribute FriendlyName="RCEDirectoryID" Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
<saml:AttributeValue>https://directory.prod.rce.sequoiaproject.org/Organization/f40f2693-6b8e-4691-ae1d-47c63c88c486</saml:AttributeValue>
</saml:Attribute>
```

Public Health SubXP-1 SOP Procedure

4.5.2 QHIN Query Response

a) All Responding Nodes SHOULD respond to Requests for Case Investigation, in accordance with the Common Agreement and Applicable Law.

b) If a Responding Node responds to a Request for Case Investigation, then it MUST return all Required Information as requested by the Initiating Node, in accordance with Applicable Law.

Public Health SubXP-1 SOP Procedure

4.6.1 FHIR Push

a) Initiating Nodes MUST only send FHIR Pushes to a PHA or its Delegate who have a FHIR Endpoint listed in their RCE Directory Entry.

b) Initiating Nodes MUST include their Resource ID of the Organization entry in the RCE Directory Service within the OAuth information.

c) If an Initiating Node sends a FHIR Push for a use case that requires or includes Reportability Response, the Initiating Node MUST support the required Reportability Response standards, as specified in Table 3.

d) For each of the specified SubXP Codes in Section 4.1 of the SOP, Initiating Nodes MUST, at least, use the appropriate, corresponding content standards, as specified below for FHIR-based exchange.

Table 3 FHIR Use Case FHIR Implementation Guide

Use Case	Document Standard or FHIR Implementation Guide
Electronic Case Reporting	HL7 FHIR® Implementation Guide: Electronic Case Reporting (eCR) - US Realm 2.1.1 - STU 2
Electronic Lab Reporting	US Core Laboratory Result Observation Profile
Other Electronic Disease/Condition Reporting	US Core Observation Clinical Result Profile

Public Health SubXP-1 SOP Procedure

4.6.2 FHIR Query

a) FHIR Requests MUST include the jurisdiction the PHA represents within the OAuth flow using the extension defined in Table 4 TEFCA Public Health Jurisdiction Extension Object.

b) FHIR Requests SHOULD include a date range for a period of no more than 5 years in the FHIR metadata. If omitted, a period of 5 years SHOULD be assumed.

Table 4 TEFCA Public Health Jurisdiction Extension Object

Extension Name: “tefca_phj”		
Element	Optionality	Requirement
Version	Required	Fixed string value: "1"
Jurisdiction	Required	A string value representing the public health jurisdiction as assigned by the federal, state, tribal, local, or territorial government public health oversight authority

Public Health SubXP-1 SOP Procedure

4.6.3 FHIR Query Response

a) All Responding Nodes SHOULD respond to Requests for Case Investigation, in accordance with the Common Agreement and Applicable Law.

a) If a Responding Node responds to a Request for Case Investigation, then it MUST return all Required Information as requested by the Initiating Node, in accordance with Applicable Law.

Individual Access Services (IAS)

IAS Relevant Definitions (1)

- **Individual**: has the meaning assigned to such term at 45 CFR § 171.202(a)(2).
- **Individual Access Services (IAS)**: the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant, or Subparticipant, as applicable, agrees to satisfy that Individual’s ability to use TEFCA Exchange to access, inspect, obtain, or transmit a copy of that Individual’s Required Information.
- **Individual Access Services Provider (IAS Provider)**: each QHIN, Participant, and Subparticipant that offers Individual Access Services (IAS).
- **Individual Access Services (IAS) Incident**: means a TEFCA Security Incident or a Breach of Unencrypted Individually Identifiable Information maintained by the IAS Provider.

IAS Relevant Definitions (2)

- **Individually Identifiable:** information that identifies an Individual or with respect to which there is a reasonable basis to believe that the information could be used to identify an Individual.
- **Breach of Unencrypted Individually Identifiable Information**: the acquisition, access, or Disclosure of unencrypted Individually Identifiable information maintained by an Individual Access Services (IAS) Provider that compromises the security or privacy of the unencrypted Individually Identifiable information.
- **TEFCA Information (TI)**: any information that is transacted through TEFCA Exchange except to the extent that such information is received by a QHIN, Participant, or Subparticipant that is a Covered Entity, Business Associate, or Non-HIPPA Entity (NHE) that is exempt from compliance with the Privacy section of the applicable Framework Agreement and is incorporated into such recipient’s system of records, at which point the information is no longer TI with respect to such recipient and is governed by the HIPAA Rules and other Applicable Law.

IAS Provider Privacy/Security Requirements

IAS Provider Privacy/Security Requirements: Highlights from the Common Agreement

- **Common Agreement Version 2.0 Section 10**
  - Individuals must complete the IAS Provider's own supplied form for obtaining express written consent from the Individual (IAS Consent).
  - Requirements for IAS Providers shall survive for so long as the IAS Provider maintains the Individually Identifiable information.
- **Common Agreement Version 2.0 Section 11**
  - IAS Providers that are Non-HIPAA Entities must comply with the provisions of the HIPAA Privacy Rule listed in Section 11 with respect to all Individually Identifiable information.
- **Common Agreement Version 2.0 Section 12**
  - IAS Providers that are Non-HIPAA Entities must encrypt all Individually Identifiable information they maintain, both in transit and at rest.
  - IAS Providers that are Non-HIPAA Entities must comply with the HIPAA Security Rule with respect to all Individually Identifiable information.

Note: Minimal substantive changes were made to the IAS Provider Privacy and Security requirements in the Common Agreement

IAS Provider Requirements SOP

IAS Provider Requirements SOP: Highlights

- IAS Providers are required to have publicly available, written Privacy and Security Notice that explains the privacy and security practices of the IAS Provider with respect to Individually Identifiable information and the Individual's rights with respect to their Individually Identifiable information maintained by the IAS Provider in connection with the Individual Access Services. (Section 4.1)
- IAS Providers must obtain the Individual's prior, express, written consent if a provider intends to sell or otherwise receive renumeration in exchange for Individually Identifiable Information. (Section 4.2)
- If an IAS Incident occurs, an IAS provider must inform affected Individuals about the incident, any steps Individuals should take to protect themselves and the actions being taken to address the situation. (Section 4.3)

Note: Minimal substantive changes were made to the IAS Provider Requirements SOP from the previously published IAS Provider Privacy and Security Notice and Practices SOP

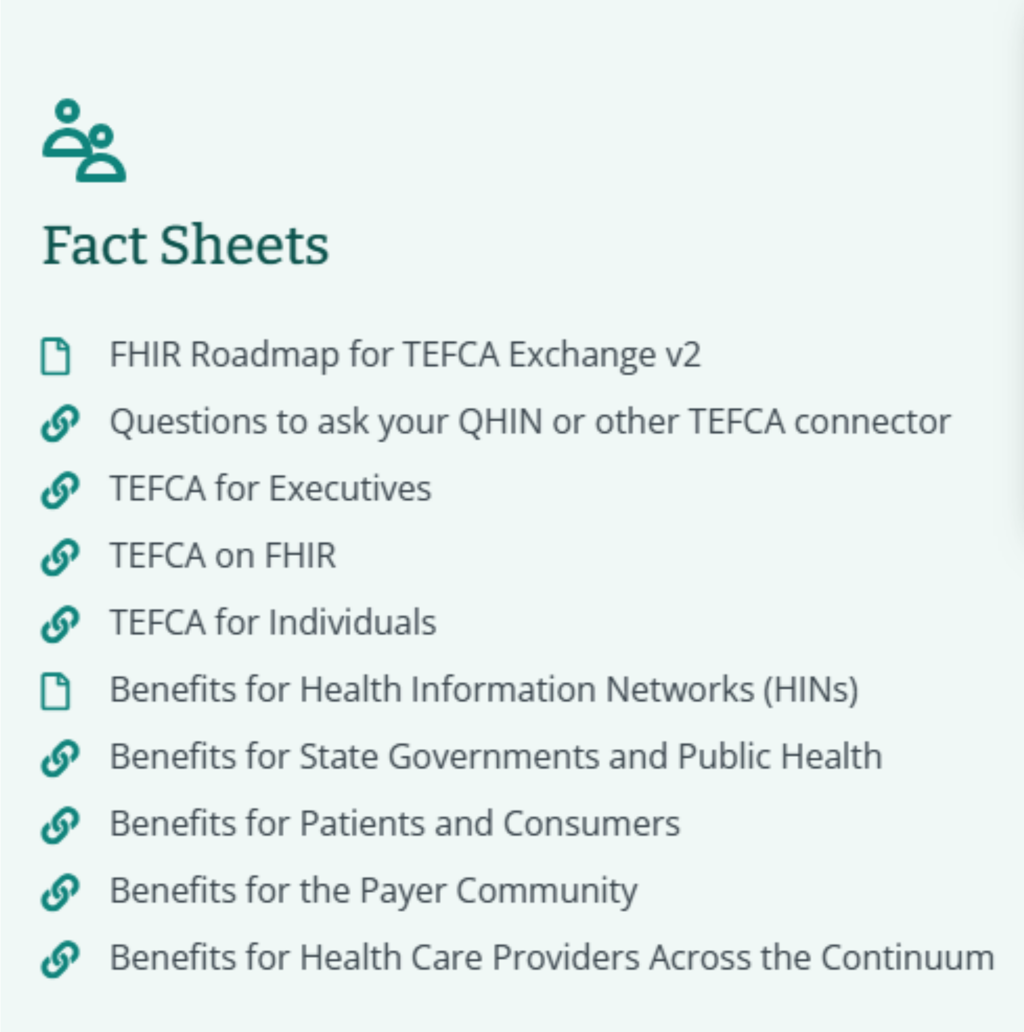
IAS Exchange Purpose (XP) and IAS Implementation SOP

Highlights

- IAS is a required Exchange Purpose
- The IAS XP Implementation SOP: Demographic Matched, focuses on IAS Requests made using *demographics matched*
  - The QTF includes specifications for IAS Requests made using issued credentials
- The IAS XP Implementation SOP: Demographic Matched, requires that IAS Providers:
  - Have an agreement with an approved credential service provider (CSP)
  - Authenticate individuals using processes set to at least Authenticator Assurance Level 2 (AAL2)
  - Verify the identities of Individuals to at least Identity Assurance Level 2 (IAL2) via a CSP prior to the Individual’s first use of TEFCA Exchange, and then again after credentials expire

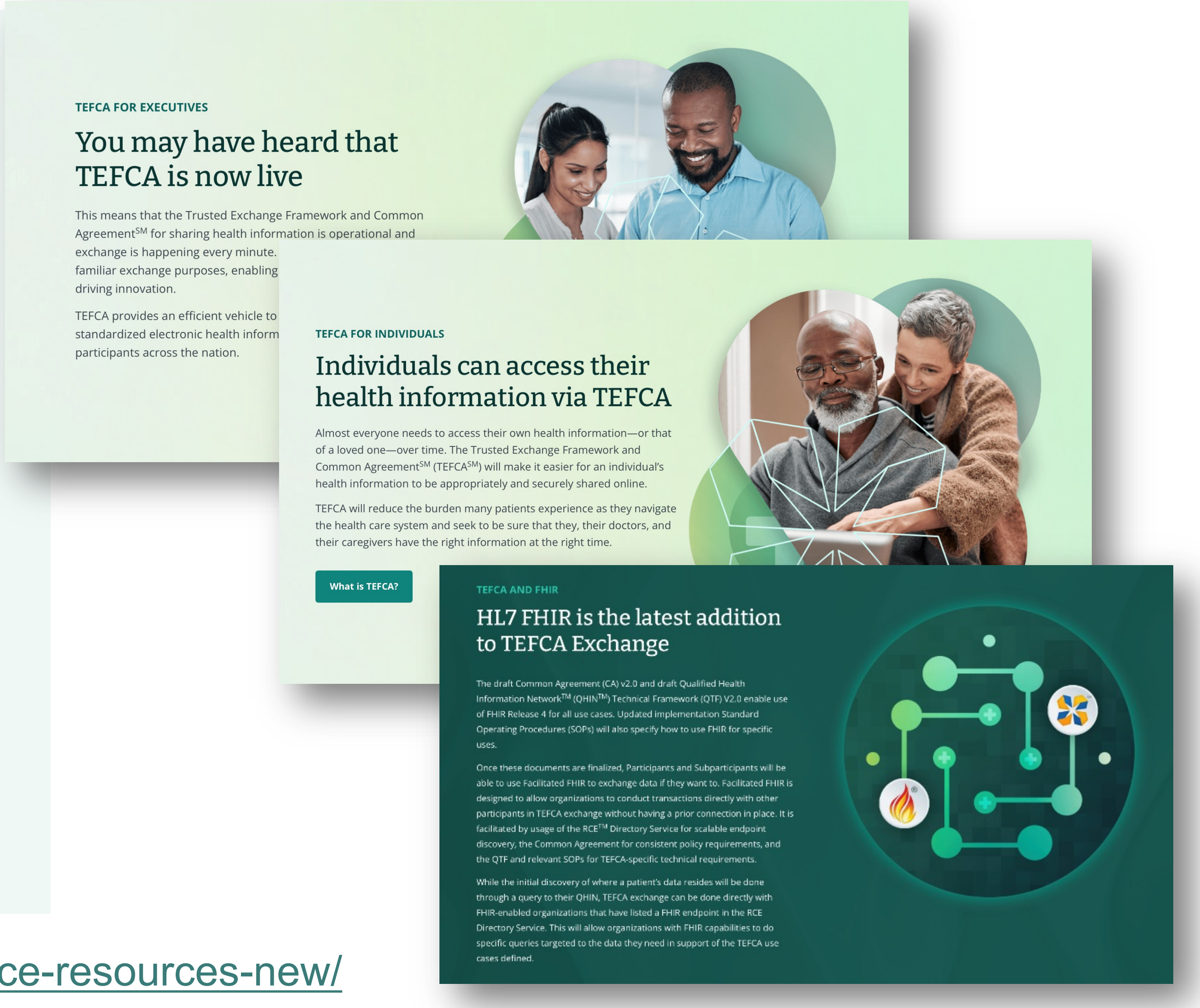
Educational Resources and Upcoming Events

New Fact Sheets



Fact Sheets

- FHIR Roadmap for TEFCA Exchange v2
- Questions to ask your QHIN or other TEFCA connector
- TEFCA for Executives
- TEFCA on FHIR
- TEFCA for Individuals
- Benefits for Health Information Networks (HINs)
- Benefits for State Governments and Public Health
- Benefits for Patients and Consumers
- Benefits for the Payer Community
- Benefits for Health Care Providers Across the Continuum



TEFCA FOR EXECUTIVES

You may have heard that TEFCA is now live

This means that the Trusted Exchange Framework and Common Agreement^{SM} for sharing health information is operational and
exchange is happening every minute.
familiar exchange purposes, enabling
driving innovation.

TEFCA provides an efficient vehicle to
standardized electronic health inform
participants across the nation.

TEFCA FOR INDIVIDUALS

Individuals can access their health information via TEFCA

Almost everyone needs to access their own health information—or that of a loved one—over time. The Trusted Exchange Framework and Common Agreement^{SM} (TEFCA^{SM}) will make it easier for an individual's health information to be appropriately and securely shared online.

TEFCA will reduce the burden many patients experience as they navigate the health care system and seek to be sure that they, their doctors, and their caregivers have the right information at the right time.

TEFCA AND FHIR

HL7 FHIR is the latest addition to TEFCA Exchange

The draft Common Agreement (CA) v2.0 and draft Qualified Health Information Network^{TM} (QHIN^{TM}) Technical Framework (QTF) V2.0 enable use of FHIR Release 4 for all use cases. Updated implementation Standard Operating Procedures (SOPs) will also specify how to use FHIR for specific uses.

Once these documents are finalized, Participants and Subparticipants will be able to use Facilitated FHIR to exchange data if they want to. Facilitated FHIR is designed to allow organizations to conduct transactions directly with other participants in TEFCA exchange without having a prior connection in place. It is facilitated by usage of the RCE^{TM} Directory Service for scalable endpoint discovery, the Common Agreement for consistent policy requirements, and the QTF and relevant SOPs for TEFCA-specific technical requirements.

While the initial discovery of where a patient's data resides will be done through a query to their QHIN, TEFCA exchange can be done directly with FHIR-enabled organizations that have listed a FHIR endpoint in the RCE Directory Service. This will allow organizations with FHIR capabilities to do specific queries targeted to the data they need in support of the TEFCA use cases defined.

https://rce.sequoiaproject.org/rce-resources-new/

New Fact Sheet

THINKING ABOUT JOINING TEFCA?

Questions to ask your QHIN or other TEFCA connector

Nationwide sharing of health information is now possible under the Trusted Exchange Framework and Common Agreement^{SM} (TEFCA^{SM}). The federally endorsed framework provides access to clinical data when and where it is needed for informed decisions, efficient care, and better outcomes.

In order to assist providers, payers, health information networks, public health agencies, app developers, and others that want to participate in TEFCA exchange choose the best QHIN, health information network, or other technology partner for connecting, the RCE has assembled a list of important questions to ask potential QHIN vendors or intermediary connectors.

RCE Resource Library

TEFCA is a multifaceted, living framework that enables seamless and secure nationwide exchange of health information.

Below is a guide to the Common Agreement, Standard Operating Procedures (SOPs), technical documents, and other resources that make up TEFCA's rules of the road. Start your journey to next generation interoperability here.

https://rce.sequoiaproject.org/rce-resources-new/

Additional Resources:
https://www.healthit.gov/tefca

All Events Registration and Recordings:
https://rce.sequoiaproject.org/community-engagement/

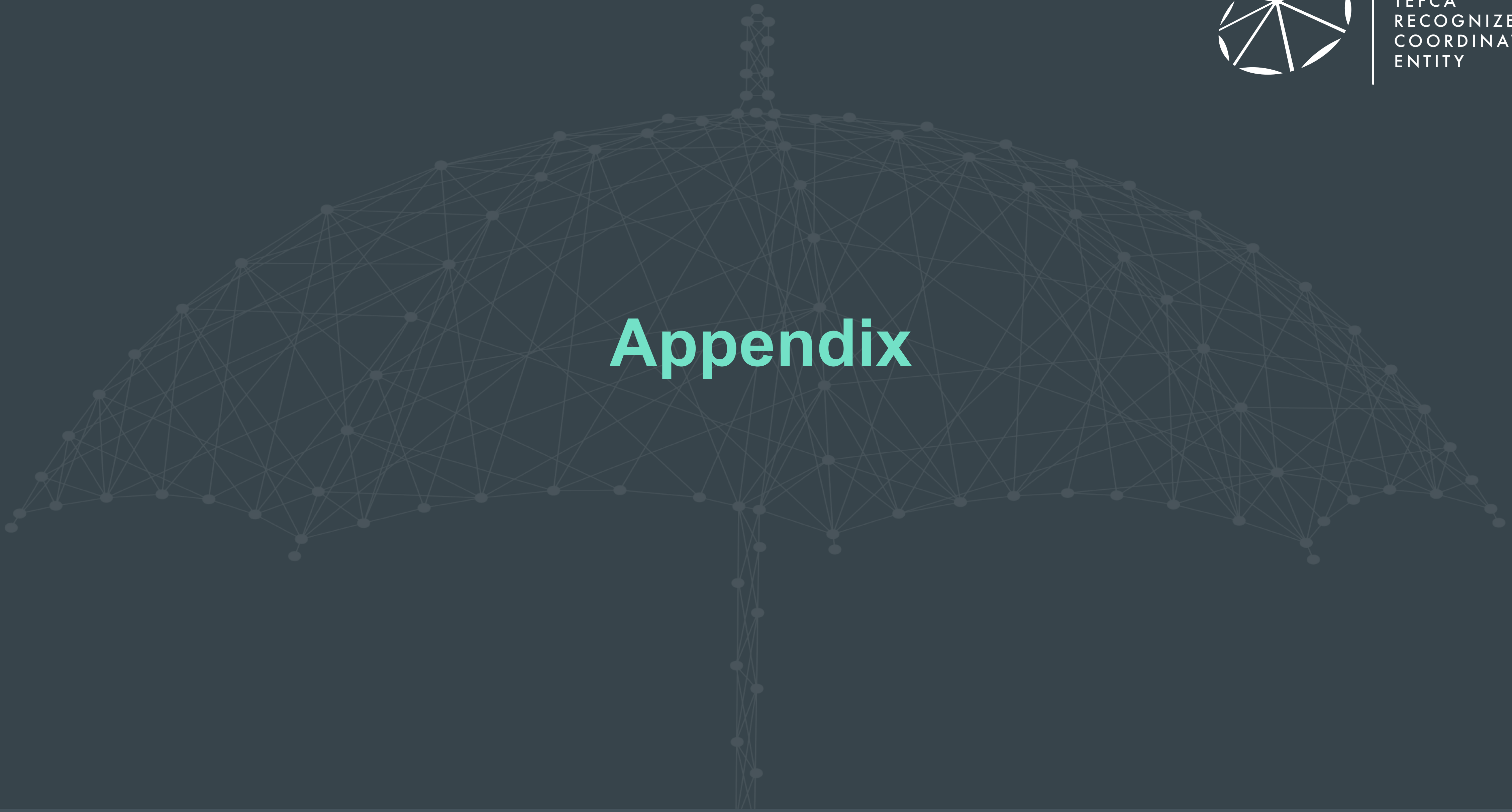
The RCE is seeking stakeholder input online through **Monday, February 5**. Stakeholders can submit input via the feedback form on our website, email feedback to **rce@sequoiaproject.org**,

The deadline for the XP Implementation SOP: Public Health SubXP-1 and the Public Health Educational Guidance Document has been extended to **Monday, February 12**

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Questions & Answers

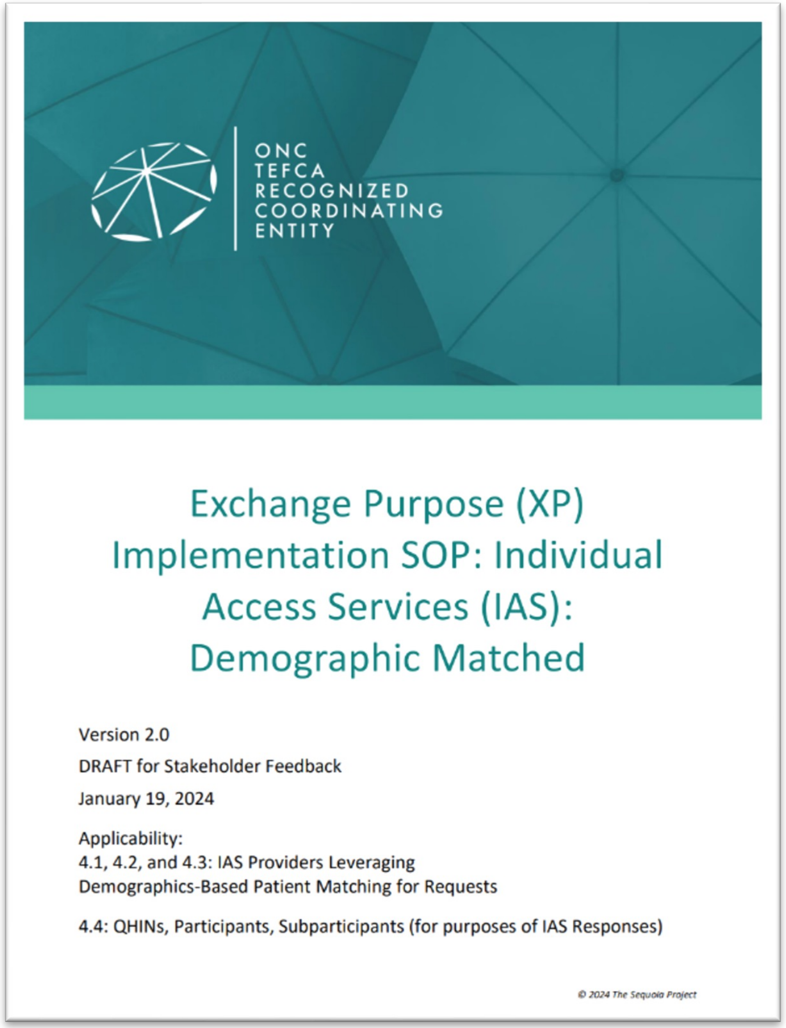
For more information:
rce.sequoiaproject.org



Appendix

XP Implementation SOP: Individual Access Services (IAS): Demographic Matched

XP SOP: IAS Demographic Matched Overview



ONC TEFCA RECOGNIZED COORDINATING ENTITY

Exchange Purpose (XP) Implementation SOP: Individual Access Services (IAS): Demographic Matched

Version 2.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability:
4.1, 4.2, and 4.3: IAS Providers Leveraging Demographics-Based Patient Matching for Requests

4.4: QHINs, Participants, Subparticipants (for purposes of IAS Responses)

© 2024 The Sequoia Project

Purpose

This SOP identifies specific requirements that Individual Access Services (IAS) Providers are required to follow for Individual identity verification for IAS demographics-based matching. This SOP also identifies when a QHIN, Participant, or Subparticipant is required to Respond to an IAS Request made using demographics-based matching[1]. Requirements for IAS Requests made using Health Level 7® (HL7®) Fast Healthcare Interoperability Resources® (FHIR®) and OAuth with responder-issued credentials are out of scope for this SOP and are in the QTF.

SOP Sections:

1. Common Agreement References
2. SOP Definitions
3. Purpose
4. Procedure
   - 4.1 Credential Service Provider
   - 4.2 Authentication
   - 4.3 Identity Verification Requirement
   - 4.4 Response Requirement

[1] Nothing in this SOP alters a Covered Entity's obligations under the HIPAA Rules.

XP SOP: IAS Demographic Matched Procedure

4.1 Credential Service Provider (CSP)

- IAS Providers MUST have an agreement with a credential service provider (CSP) who has been approved by an RCE-selected CSP approval organization.2 The CSP approval organization must maintain a published list of CSPs who conduct identity proofing to at least Identity Assurance Level 2 (IAL2) as defined by the then latest version of the National Institute of Standards and Technology Special Publication 63A Digital Identity Guidelines (NIST SP800-63A). The CSP approval organization MUST require approved CSPs to be assessed for conformance to the minimum appropriate identity proofing and credential management standards, and to publish and maintain the standards to which the CSPs are assessed.

4.2 Authentication

- IAS Providers MUST authenticate Individuals using processes set to at least Authenticator Assurance Level 2 (AAL2) as defined by the then latest version of the NIST SP800-63A requirements.

XP SOP: IAS Demographic Matched Procedure

4.3 Identity Verification Requirement

- IAS Providers MUST verify the identities of Individuals to at least IAL2 via a CSP prior to the Individual's first use of TEFCA Exchange, and then again after credentials expire.

  a. Verification MUST include, at a minimum, the following demographics: First Name, Last Name, Date of Birth, Address, City, State, ZIP.

  b. Verification SHOULD also include, but does not require, Sex, Middle Name, Middle Initial, Suffix, Email Address, Mobile Phone Number, Social Security Number (SSN), SSN last 4 digits, ZIP+4, and other verifiable identifiers (e.g., Medical Record Number, Passport Number, Driver's License, State ID).

  c. IAS Providers MUST demonstrate that all Individuals that elect to use their IAS offering have proven their identities consistent with achieving IAL2. This evidence MUST be included within the Request as an IAL2 Claims Token using the OpenID Connect token format as further specified in Appendix A of the SOP.

  d. Requests initiated by an IAS Provider MUST include only the demographics as provided to the CSP and as part of the Individual's identity verified to IAL2.

  e. Historical name and/or address information MAY be included only if validated by the CSP for identity proofing for that Individual.

  f. An IAS Provider MUST ensure that all updates to demographic information used for TEFCA Exchange for IAS have the demographics validated to IAL2 by the CSP prior to the Individual's first use.

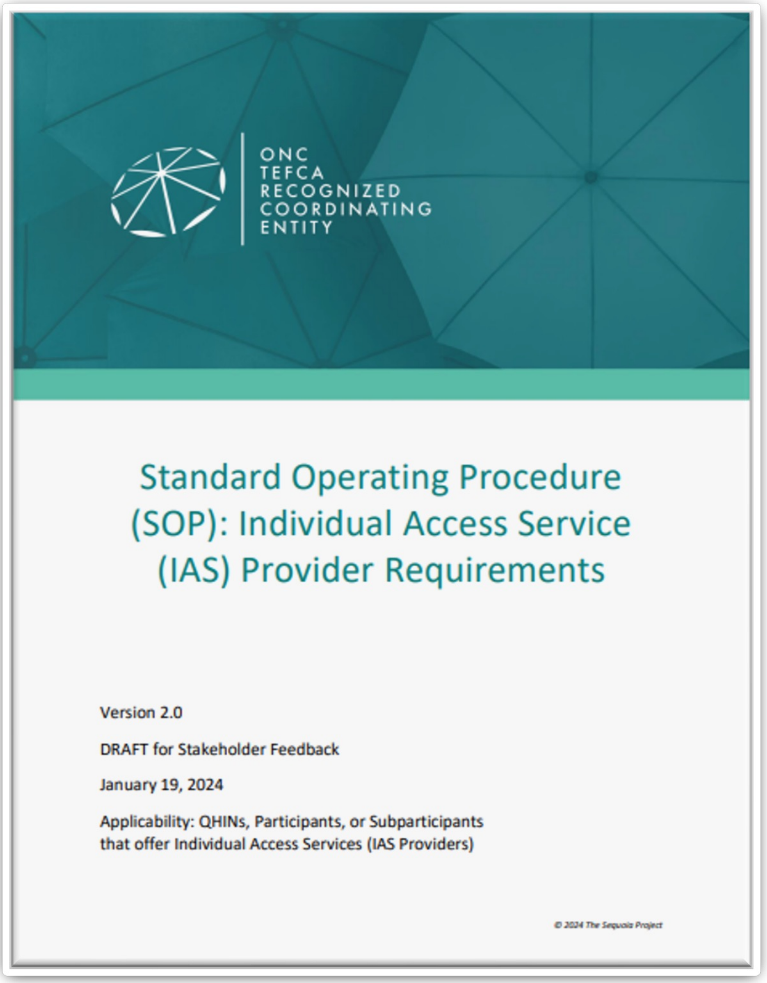
XP SOP: IAS Demographic Matched Procedure

4.4 Response Requirement

- Any Responding Node that receives a Request from an IAS Provider that includes the appropriate IAL2 Claims Token, as specified in 4.3(c), and that achieves an acceptable demographics-based match based on responder policy is required to Respond with the Required Information per the Common Agreement, the QHIN Technical Framework, and the Exchange Purposes (XPs) SOP.

Individual Access Services (IAS) Provider Requirements

IAS Provider Requirements SOP Overview



ONC TEFCA RECOGNIZED COORDINATING ENTITY

Standard Operating Procedure (SOP): Individual Access Service (IAS) Provider Requirements

Version 2.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability: QHINs, Participants, or Subparticipants that offer Individual Access Services (IAS Providers)

Purpose

Section 10 of the Common Agreement outlines terms and conditions that IAS Providers must follow to offer IAS. Among other things, IAS Providers are required to obtain the Individual's express written consent in connection with IAS, including acknowledgment of and agreement to the IAS Provider's written Privacy and Security Notice that describes the privacy and security practices used to safeguard Individually Identifiable information.

SOP Sections:

1. Common Agreement References
2. SOP Definitions
3. Purpose
4. Procedure
   - 4.1 Written Privacy and Security Notice and Individual Consent
   - 4.2 Consent to Sale
   - 4.3 Content of Notice to Individual of TEFCA Security Incident or Breach of Unencrypted Information (IAS Incident)

IAS Provider Requirements SOP Procedure

4.1 Written Privacy and Security Notice and Individual Consent

- IAS Providers are required to have a publicly available, written Privacy and Security Notice (for purposes of this SOP “Notice”) that provides an explanation, as described below, of the privacy and security practices of the IAS Provider with respect to Individually Identifiable information and the Individual’s rights with respect to their Individually Identifiable information maintained by the IAS Provider in connection with the Individual Access Services.

IAS Provider Requirements SOP Procedure

ONC TEFCA RECOGNIZED COORDINATING ENTITY

4.1 Written Privacy and Security Notice and Individual Consent (1)

a) IAS Providers must implement the Notice using the following standards. The Notice must meet each of the following requirements:

1. Be publicly accessible and kept current at all times, including updated versions.
2. Be shared with an Individual prior to the Individual's use/receipt of IAS from the IAS Provider.
3. Be written in plain language and in a manner calculated to inform the Individual of such privacy practices.
4. Include a statement regarding whether and how Individually Identifiable information may be accessed, exchanged, Used, and/or Disclosed by IAS Provider or by other persons or entities to whom/which IAS Provider Discloses or provides access to the information, including whether the Individually Identifiable information may be sold at any time (including the future).
5. Include a statement that the IAS Provider is required to act in conformance with the Privacy and Security Notice and must protect the security of the information it holds in accordance with the applicable Framework Agreement.
6. Include information regarding whom the Individual may contact within IAS Provider for further information regarding the Privacy and Security Notice and/or with privacy-related complaints.

IAS Provider Requirements SOP Procedure

4.1 Written Privacy and Security Notice and Individual Consent (2)

7. Include a requirement by IAS Provider to obtain express written consent to the terms of the Privacy and Security Notice from the Individual prior to the access, exchange, Use, or Disclosure of the Individually Identifiable information, other than Disclosures that are required by Applicable Law.
8. Include information on how the Individual may revoke consent.
9. Include an explanation of the Individual’s rights with respect to Individually Identifiable information, including, at a minimum the right of an Individual to:
    - i. Require that all of their Individually Identifiable information maintained by the IAS Provider in connection with the IAS be deleted unless such deletion is prohibited by Applicable Law; provided, however, that the foregoing shall not apply to Individually Identifiable information contained in audit logs;
    - ii. Access their Individually Identifiable information maintained by the IAS Provider in connection with the IAS;
    - iii. Obtain an export of their Individually Identifiable information in a machine-readable format, including the means to interpret such machine-readable format; and
    - iv. Be notified in the event their Individually Identifiable information is reasonably believed to have been affected by an IAS Incident.
10. Notice to the Individual must include the information in Section 3.C of this SOP.
11. Include a disclosure of any applicable fees or costs related to IAS including the exercise of any Individual rights.
12. Include an effective date of the written Notice and an effective date of any subsequent material changes to such Notice.

IAS Provider Requirements SOP Procedure

4.2 Consent to Sale

- Notwithstanding anything to the contrary in the Notice, if an IAS Provider intends to sell, or otherwise receive renumeration in exchange for Individually Identifiable information, the IAS Provider must obtain the Individual’s prior, express, written consent ("Consent to Sale"). While the IAS Provider may obtain the Consent to Sale contemporaneously with the Individual’s consent to the Notice, the Consent to Sale must be conspicuously labeled as such and separate from the consent to the Notice.

4.3 Content of Notice to Individual of TEFCA Security Incident or Breach of Unencrypted Information (IAS Incident)

Notice to an Individual of an IAS Incident in which the Individual's Individually Identifiable information is reasonably believed to have been affected must include, to the extent possible, the following information:

a. A brief description of what happened, including the date of the IAS Incident and the date of its Discovery, if known;

b. A description of the type(s) of Individually Identifiable involved in the IAS Incident (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

c. Any steps Individuals should take to protect themselves from potential harm resulting from the IAS Incident;

d. A brief description of what the IAS Provider involved is doing to investigate the IAS Incident, to mitigate harm to Individuals, and to protect against any further IAS Incidents; and

e. Contact procedures for Individuals to ask questions or learn additional information related to the IAS Incident, which shall include a telephone number (toll-free), e-mail address, and website with contact information and/or a contact form for the IAS Provider.