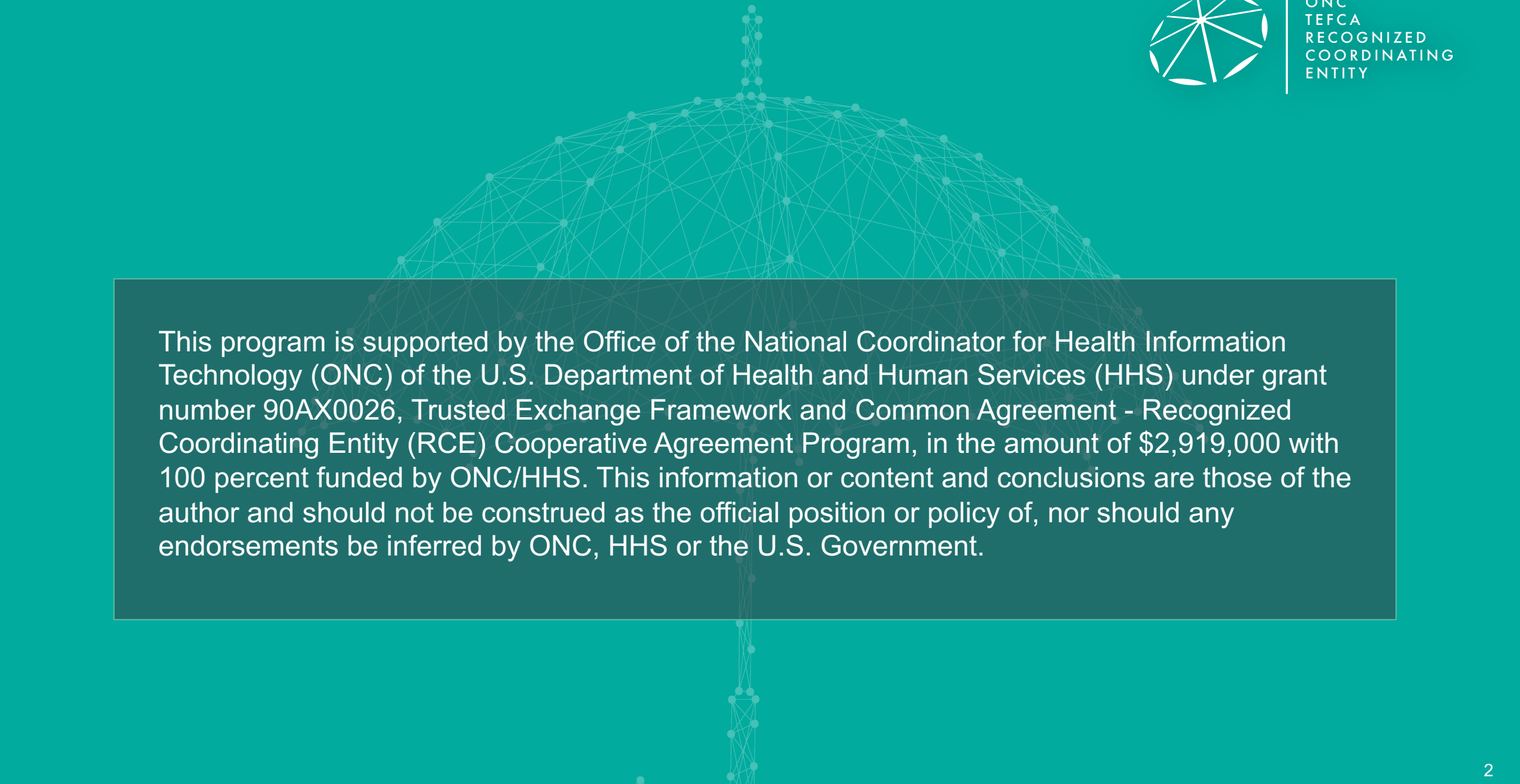
ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

April 19, 2022

RCE Monthly Informational Call

Mariann Yeager, CEO, The Sequoia Project; RCE Lead
Didi Davis, VP, Interoperability, The Sequoia Project
Zoe Barber, Director, Policy, The Sequoia Project
Johnathan Coleman, RCE CISO
Alan Swenson, Executive Director, Carequality



ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

This program is supported by the Office of the National Coordinator for Health Information Technology (ONC) of the U.S. Department of Health and Human Services (HHS) under grant number 90AX0026, Trusted Exchange Framework and Common Agreement - Recognized Coordinating Entity (RCE) Cooperative Agreement Program, in the amount of $2,919,000 with 100 percent funded by ONC/HHS. This information or content and conclusions are those of the author and should not be construed as the official position or policy of, nor should any endorsements be inferred by ONC, HHS or the U.S. Government.

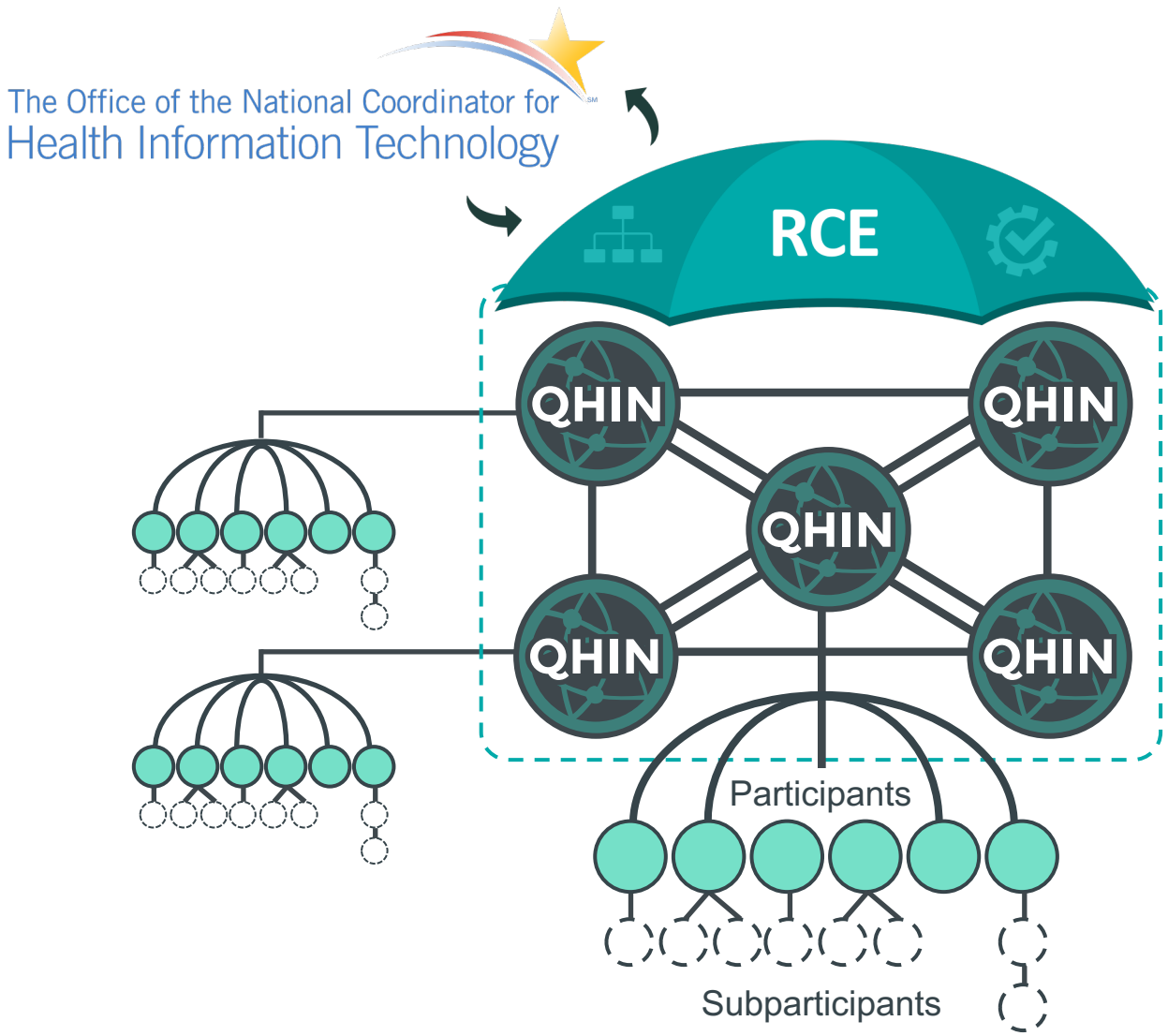
Agenda

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- How will TEFCA work?
- What are TEFCA components?
- How will TEFCA be operationalized?
- Transition of legal counsel
- Status of SOPs
- Exchange Purposes SOP
- Testing Approach
- Security of TEFCA Information – Security Certification
- Questions & Answers

How will exchange work under TEFCA?

ONC TEFCA RECOGNIZED COORDINATING ENTITY



ONC defines overall policy and certain governance requirements.

RCE provides oversight and governing approach for QHINs.

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

Each QHIN connects Participants, which connect Subparticipants.

TEFCA Components

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Trusted Exchange Framework

Common Agreement

Standard Operating Procedures

QHIN Technical Framework

QHIN Onboarding

Metrics

Governing Approach

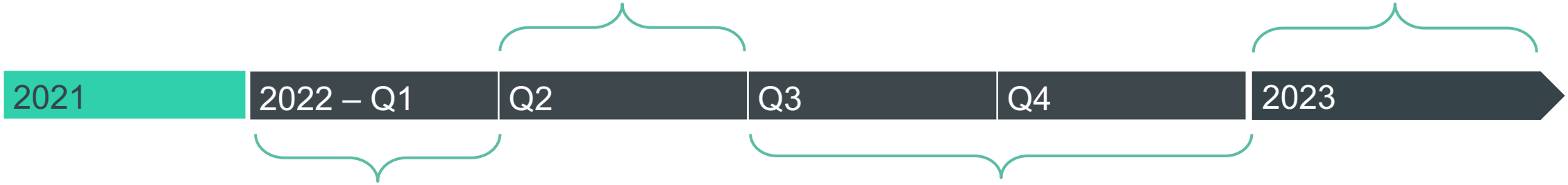
Timeline to Operationalize TEFCA

ONC TEFCA RECOGNIZED COORDINATING ENTITY

2021
- Public engagement
- Common Agreement Work Group sessions
- RCE and ONC use feedback to finalize TEFCA

Q2 of 2022
- QHINs begin signing Common Agreement and applying for designation

2023
- Establish Governing Council
- Follow change management process to iterate Common Agreement, SOPs, and QTF, including to support FHIR-based exchange



Q1 of 2022
- Publish Common Agreement Version 1
- Publish QHIN Technical Framework (QTF) Version 1 and FHIR Roadmap
- Initiate work to enable FHIR-based exchange
- Public education and engagement

Q3 and Q4 of 2022
- Onboarding of initial QHINs
- Additional QHIN applications processed
- RCE establishes Transitional Council
- RCE begins designating QHINs to share data
- Prepare for TEFCA FHIR exchange pilots

Transition of Legal Counsel

Steve Gravely
Founder & CEO
Gravely Group

Cait Riccobono
Attorney
Gravely Group

Erin Whaley
Partner
Troutman Pepper

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

SOP Status

SOP Status

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Completed

- Governing Council
- Transitional Council
- Advisory Groups
- Conflicts of Interest
- Dispute Resolution
- QHIN Security of TEFCA Information (TI)
- Cyber Security Insurance

Future

- QHIN Eligibility & Designation SOP and QHIN Application
- Foreign Ownership SOP
- Update Security of TI SOP: Certification Process and Security Certification List
- IAS Implementation SOP
- Exchange Purposes SOP
- Participant Subparticipant Definition SOP
- Participant Subparticipant Security SOP
- IAS Provider Privacy and Security Notice SOP
- Payment and Healthcare Operations Implementation SOP
- Public Health Implementation SOP
- Government Benefits Determination Implementation SOP
- Other Security Incidents and Reportable Events SOP
- Suspensions Process SOP
- Successor RCE & Transition SOP

Exchange Purposes SOP (under development)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- **Authorized Exchange Purposes**
  - Treatment
  - Payment
  - Healthcare Operations
  - Individual Access Services
  - Public Health
  - Government Benefits Determination

- **Required Responses** — QHINs, Participants, and Subparticipants are required to Respond to Requests for:
  - Treatment
  - Individual Access Services — Required six (6) months following publication date of the Individual Access Services Implementation SOP

- **Permitted Responses** — QHINs, Participants, and Subparticipants are permitted to Respond to Requests for any/all authorized Exchange Purposes

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Testing Approach

Testing Approach

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- **Pre-Production Testing** – Prospective QHIN will be required to complete within 12 months of approval of its application by the RCE
  - » Conformance Testing Process – Self-Service Automated Transaction & Security against the Sequoia Interoperability Testing Platform
  - » Non-Production Partner Testing – non-production transaction testing against test instances of other QHIN gateways (“Test Ecosystem”) that must be maintained by all QHINs ongoing
- **Production Connectivity Validation** – After RCE Designation and within 30 calendar days of having entry added to RCE Production Directory
  - » All QHINs must complete testing with all other in-Production QHINs
  - » All QHINs must support new QHINs Production Testing

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Security of TEFCA Information: Security Certification

SOP – QHIN Security Requirements for the Protection of TEFCA Information

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- **Purpose:** This SOP identifies specific requirements that QHINs must follow to protect the security of TI. It also provides specific information about the Cybersecurity Council.

- **Procedure:**
  1. Third-Party Cybersecurity Certification
  2. Annual Technical Audits
  3. Reports or Summaries of Certification Assessments & Annual Technical Audits
  4. Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation
  5. Cybersecurity Council

The Cybersecurity & Infrastructure Security Agency (CISA) has identified the healthcare and public health sector as part of the nation's critical infrastructure, stating: The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health critical infrastructure

https://www.cisa.gov/healthcare-and-public-health-sector#:~:text=The%20Healthcare%20and%20Public%20Health,disease%20outbreaks%2C%20and%20natural%20disasters

QHIN Certification Requirements (under development)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- **QHIN Security Certification Considerations:**
  - Every QHIN would be certified under a nationally recognized security framework from a list of pre-approved certifications/certifying bodies developed by the RCE.
  - The RCE would maintain and publish a list of certifying bodies which meet the RCE's security certification requirements as outlined in the SOP. Any third-party accreditation or certification body that can demonstrate adherence to the requirements listed in the SOP may be considered for inclusion in the RCE's list of certification bodies.
  - The RCE's list would include certifying bodies which have been used successfully by QHINs to obtain certification during their onboarding/designation process.
  - Certification bodies providing services which meet these requirements would also be able to request pre-approval to be included in the list.

**This SOP is under development and considers feedback received from RCE outreach sessions*

QHIN Certification Requirements (under development)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

(a) As part of a QHIN's third-party Security Certification process, the certification body would:

- (i) Utilize the NIST Cyber Security Framework (CSF) as the basis for its certification program.
- (ii) Review the QHIN's HIPAA Security Analysis (consistent with §164.308(a)(1)(ii)(A)).
- (iii) Verify Common Agreement requirements for technical audits and assessments are met. This includes making sure they are conducted at least annually, include the necessary scope for security assessments (see below), and include mitigation planning activities.

(b) A QHIN's annual third-party security audit would, at a minimum, include the following within scope:

- (i) Adoption of the NIST CSF.
- (ii) Requirements of the HIPAA Security Rule, including Security Risk Analysis.
- (iii) Include a review of security requirements from the CA, Security SOPs, QTF, and other Security Requirements as incorporated by TEFCA at time of assessment.
- (iv) Utilize methodologies and security controls consistent with Recognized Security Practices** (e.g. NIST Special Publications, CMS Guidelines, ONC HIPAA Security Risk Assessment (SRA) Tool, etc.)

**This SOP is under review and considers feedback received from RCE outreach sessions*

***https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf*

QHIN Certification Requirements (under development)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

(c) Certification bodies and third-party assessment organizations would be qualified, independent third parties:

(i) Organizations conducting assessments would attest (in the assessment report) to having no organizational COI with the certification body or the organization being assessed.

(ii) Assessors would be security professionals with active/current security certifications and ongoing credential maintenance requirements (e.g., security assessment credentials with CPE requirements. Examples include certifications recognized by Federal Agencies as minimum requirements for conducting certain security roles).

(d) Quality review:

(i) Third party assessments and certification activities would be subject to quality review/sampling by the certification body to ensure consistency and quality.

**This SOP is under development and considers feedback received from RCE outreach sessions*

IAS SOP, Identity Proofing Section (Under Development)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- The RCE will publish a list of selected Credential Service Provider (CSP) Approval Organizations on the RCE website. These approval organizations will maintain a published list of their approved CSPs.
- The **Individual Access Services SOP** (under development) identifies specific requirements that IAS Providers would follow for Individual identity verification. These requirement may include:
  - IAS Providers would have an agreement with a credentialing service provider (CSP) who has been approved by an RCE selected Credential Service Provider Approval Organization.
  - The Credential Service Provider (CSP) Approval Organization would maintain a published list of CSPs who conduct Identity Proofing to IAL2 as defined by NIST SP800-63A (r3 or later).
  - The CSP Approval Body would require approved CSPs to be assessed for conformance to the appropriate identity proofing and credential management standards, and to publish and maintain the standards to which they are assessed.

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

QHIN Technical Framework (QTF) Security Requirements

QTF Security

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- Protecting the privacy and security of health information is essential for building trust among participating entities. As such, QHINs must provide a secure channel to ensure transport-level security for all transactions under their domain

- Public key infrastructure (PKI) often serves as the basis for securing electronic communications over the internet. PKI involves the use of digital certificates to assert and authenticate identities, encrypt data, and sign communications.

- Maintaining records of activities and transactions supported by the Connectivity Services can assist with troubleshooting and help facilitate monitoring for improper use. Moreover, audit records support a QHIN's ability to maintain and produce an accounting of disclosures, where required by Applicable Law and/or the Common Agreement.

User Authentication Requirements

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- For QHIN Query or QHIN Message Delivery, a QHIN MUST transmit an IHE XUA SAML assertion identifying the user or staff member at the QHIN, Participant, or Subparticipant or identifying the Individual who requested use of the QHIN's Connectivity Services.

- When a QHIN rewrites the SAML information, the new SAML assertion MUST persist the originating user and, as applicable, organization information.

- Following the IHE XUA requirements, the SAML assertion MUST include:
  - User information including name, UserID, Subject-Role, and, if appropriate, NPI;
  - The Organization name and HomeCommunityID of the Query or Message Source; and
  - Patient Identifier including Assigning Authority, if known.

User Authentication Requirements (Cont'd)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- The SAML assertion MAY include the IHE XUA Authz-Consent Option.
- QHINs MUST be capable of receiving authentication information from Participants, including the authenticated identity of any Subparticipants and/or Individuals and/or users requesting the use of Connectivity Services.
- QHINs MUST specify the mechanism(s) (i.e., format and content) by which Participants transmit authentication information to the QHIN.

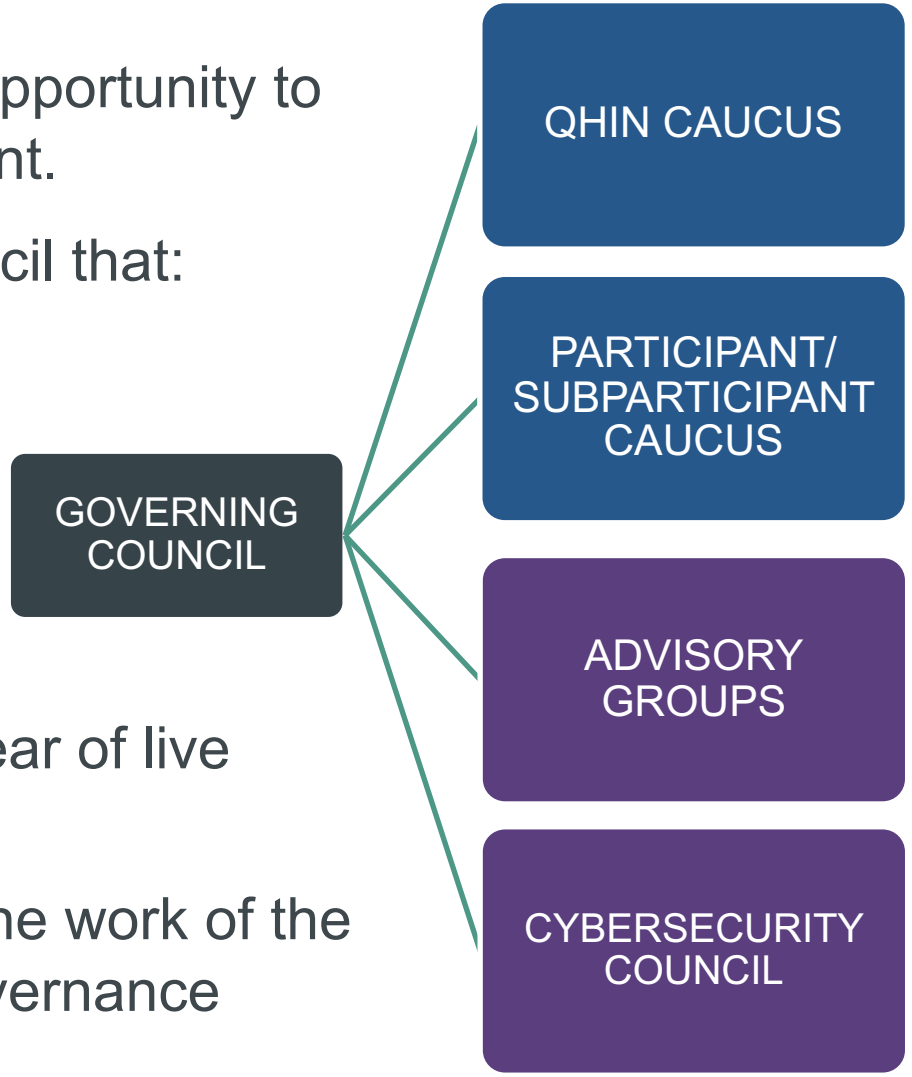
ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Security Management: Metrics and Governance

Governing Approach Overview

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- QHINs, Participants, and Subparticipants have the opportunity to engage in governance under the Common Agreement.
- The Common Agreement creates a Governing Council that:
  - Reviews amendments to the Common Agreement, QTF, and SOPs.
  - Serves as a resource to the RCE and forum for discussion.
  - Provides oversight for resolution of disputes.
- A Transitional Council serves during TEFCA's first year of live exchange.
- Under the Cooperative Agreement, ONC oversees the work of the RCE, which has specific obligations to follow the governance procedures set forth in the Common Agreement.



Security Governance

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- **Cybersecurity Council**
  - Cybersecurity Council – The RCE shall establish a Cybersecurity Council, which shall evaluate the cybersecurity risks to the activities conducted under the Framework Agreements and advise the RCE on ways to remediate these risks that are commensurate with such risks.
  - The RCE Chief Information Security Officer (CISO) shall serve as the Chairperson of the Cybersecurity Council and shall be a voting member of the Cybersecurity Council. The QHIN Caucus shall select five CISOs from among the QHINs to serve as voting members of the Cybersecurity Council.
  - The Participant/Subparticipant Caucus shall select five CISOs from among the Participants and Subparticipants to serve as non-voting members of the Cybersecurity Council. The Cybersecurity Council shall meet at the request of the RCE CISO, but no less than on a quarterly basis. The Cybersecurity Council may invite subject-matter experts to participate in meetings to provide input on specific issues.

Educational Resources

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Resources

- Common Agreement v. 1
- QHIN Technical Framework
- FHIR® Roadmap for TEFCA
- Standard Operating Procedures
- User's Guide
- Benefits of TEFCA by Stakeholder Factsheets
- FAQs

https://rce.sequoiaproject.org/tefca-and-rce-resources/

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

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

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Questions & Answers

For more information:
rce.sequoiaproject.org