ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

May 18, 2022

ONC Health Information Technology Advisory Committee (HITAC) — Trusted Exchange Framework and Common Agreement (TEFCA) Update

Mariann Yeager, CEO, The Sequoia Project; TEFCA Recognized Coordinating Entity (RCE) Lead
Zoe Barber, Policy Director, The Sequoia Project
Chantal Worzala, Principal, Alazro Consulting

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.

General Disclaimers

- The information in this presentation is based on the Common Agreement Version 1, the Qualified Health Information Network (QHIN) Technical Framework Version 1, and the Standard Operating Procedures as of January 18, 2022.
- While every effort has been made to ensure accuracy, this presentation is not a legal document.
- Examples are merely illustrative and may be simplified for ease of discussion.
- Readers should consult the latest versions of the Common Agreement, the QHIN Technical Framework, and Standard Operating Procedures for the definitive requirements.
- This communication is produced and disseminated at U.S. taxpayer expense.

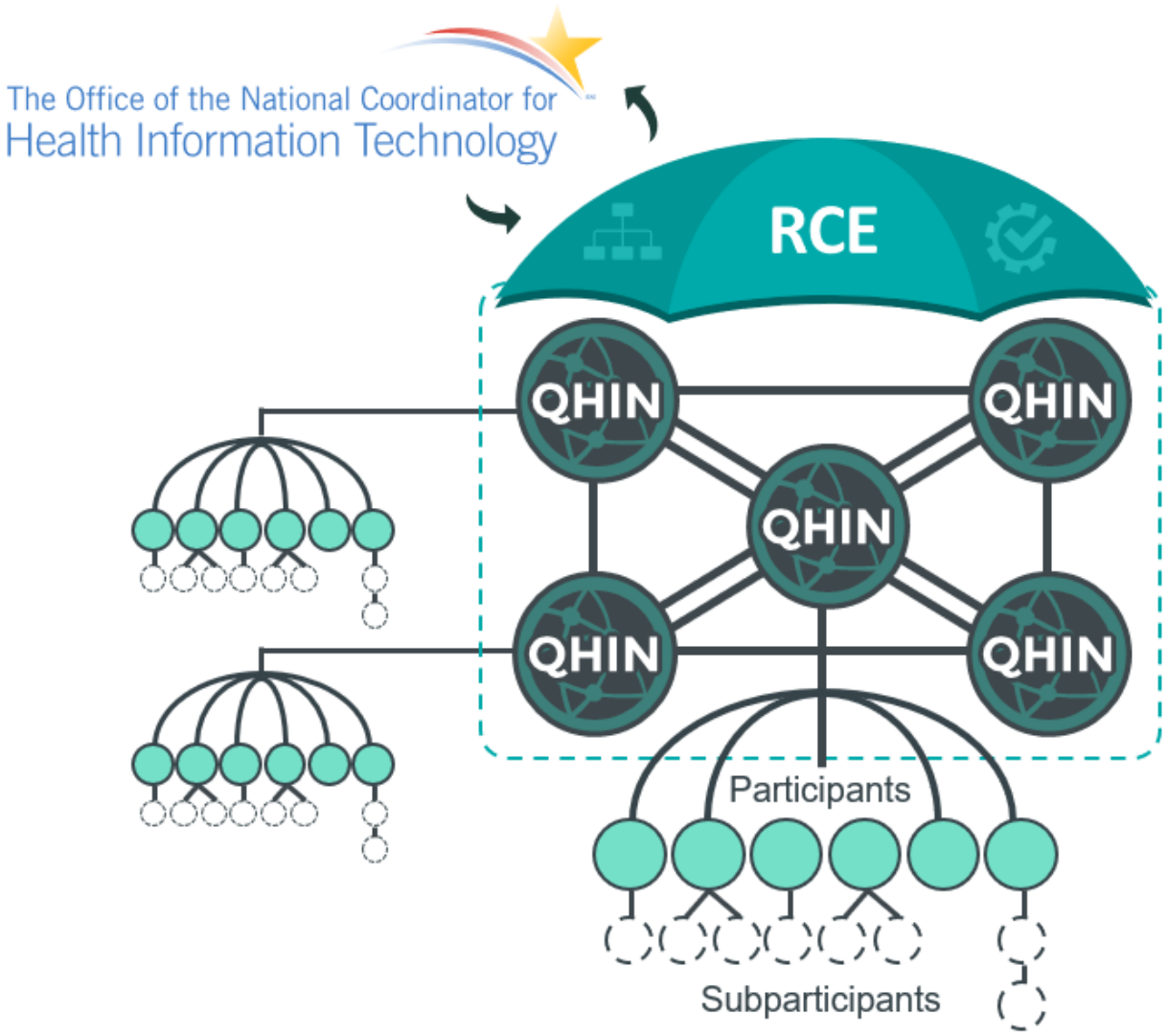
Agenda

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- How will exchange work under TEFCA?
- What are TEFCA components?
- Timeline to Operationalize TEFCA
- SOP Status & Release Schedule
- Recently Released SOPs and Resources
  - *Draft* Types of Entities that can be a Participant/Subparticipant SOP
  - *Draft* QHIN Application
  - *Draft* Onboarding & Designation SOP
  - SOP: QHIN Security Requirements for the Protection of TEFCA Information – Rev 1 (with initial QHIN Cybersecurity Certification List)
- Key Takeaways
- Questions & Answers

How will exchange work under TEFCA?

ONC TEFCA RECOGNIZED COORDINATING ENTITY



ONC defines overall policy and certain governance requirements.

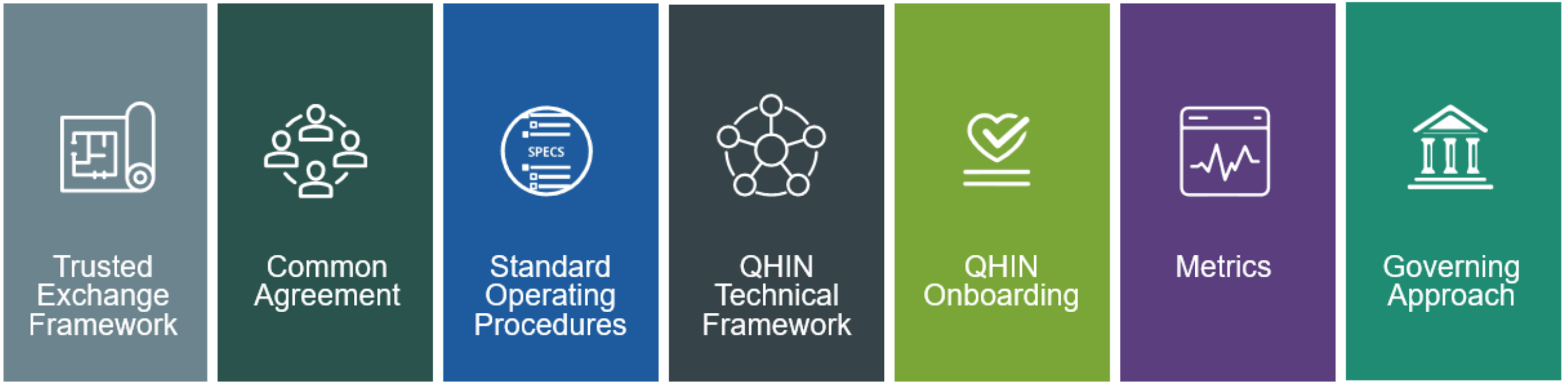
RCE provides oversight and governing approach for QHINs.

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



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

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

SOP Status & Release Schedule

SOP Status

Previously Completed

- Advisory Groups
- Conflicts of Interest
- Cyber Security Insurance
- Dispute Resolution Governing Council
- QHIN Security Requirements for the Protection of TEFCA Information
- Transitional Council

Recently Released

- *Draft* QHIN Onboarding and Designation (feedback requested)
  - *Draft* QHIN Application (feedback requested)
- QHIN Security Requirements for the Protection of TEFCA Information (Rev. 1)
- *Draft* Types of Entities that Can be a Participant or Subparticipant in TEFCA (feedback requested)

TEFCA SOP Release Schedule

ONC TEFCA RECOGNIZED COORDINATING ENTITY

SOP Name	Expected Publication of Version 1 Final
QHIN Security Requirements for the Protection of TI (Update)	Version 1.1 released 5/16
Exchange Purposes	June 2022
RCE Fee Structure for QHINs (Schedule 1)	June 2022
Types of Entities That Can Be a Participant or Subparticipant in TEFCA	July 2022 (Draft released 5/16)
QHIN Onboarding & Designation (and QHIN Application)	August 2022 (Draft released 5/16)
Means to Demonstrate U.S. Ownership and Control of a QHIN	August 2022
Individual Access Service (IAS) Provider Privacy and Security Notice	August 2022
Individual Access Services (IAS) Exchange Purpose Implementation	August 2022
Participant and Subparticipant Security	October 2022
Other Security Incidents and Reportable Events	End of 2022
Payment and Health Care Operations Exchange Purpose Implementation	Early 2023
Public Health Exchange Purpose Implementation	Early 2023
Government Benefits Determination Exchange Purpose Implementation	Mid 2023
Suspensions Process	2023
Successor RCE & Transition	2023

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Draft Types of Entities That Can Be a Participant or Subparticipant In TEFCA SOP

Draft Types of Entities That Can Be a Participant/Subparticipant

ONC TEFCA RECOGNIZED COORDINATING ENTITY

If an entity is not of a type that is entitled to request information under one or more of the Exchange Purposes, it shall not qualify as a Participant or Subparticipant for purposes of any Framework Agreement.

Only an entity that is one or more of the following types shall be permitted to be a Participant or a Subparticipant:

- **Covered Entity (or a Business Associate)**
- **IAS Provider**
- **Government Health Care Entity**
- **Federal, state, local, or tribal agency, instrumentality, or other unit of government that determines whether an Individual qualifies for government benefits for any purpose other than health care**
- **Health Care Provider (not a Covered Entity or a Government Health Care Entity)**
- **Public Health Authority**
- **Any entity that contracts with and enables connectivity for any of the entities listed above**

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Draft QHIN Application

QHIN Application Process

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Pre-application Activities

Prospective QHIN reviews the Common Agreement, QTF, and SOPs.

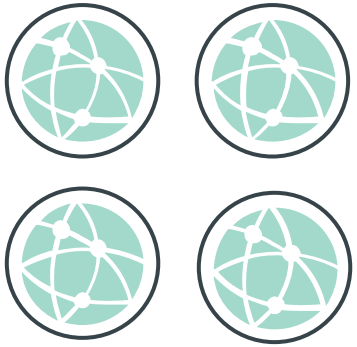
Prospective QHIN participates in educational sessions.

Prospective QHIN signs the Common Agreement and submits QHIN Application package.

The RCE makes an eligibility determination.

QHIN onboarding

If application is accepted, prospective QHIN begins the QHIN onboarding process, including technical testing and production connectivity validation.



If all requirements are met, RCE counter-signs the Common Agreement and designates the applicant as a QHIN.

RCE provides written notice of QHIN Designation to both the applicant and ONC.

All relevant materials and resources will be available at www.RCE.SequoiaProject.org.

Draft QHIN Application

ONC TEFCA RECOGNIZED COORDINATING ENTITY

The application provides the Recognized Coordinating Entity (RCE) with the information needed to determine a prospective Qualified Health Information Network's (QHIN) ability to meet its obligations and responsibilities under the Common Agreement. Exchange activities under the Common Agreement rely heavily on trust among the community of QHINs, and the application will assist an applicant in demonstrating their readiness to join that community of trust.

In order for an organization to be Designated as a QHIN, the following requirements must be met:

- The RCE must notify applicant of its acceptance of this application;
- Applicant must pay any applicable fees to the RCE; and
- Applicant must complete any additional pre-requisites specified in the QHIN Onboarding & Designation SOP.

The information contained in the application shall be treated as Confidential Information and shall only be shared consistent with the governance process.

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Draft Onboarding and Designation SOP

QHIN Eligibility Requirements

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- Applicant must demonstrate that it meets the definition of a U.S. Entity and is not owned or controlled by any non-U.S. person(s) or entity(-ies).
- Applicant must be able to exchange Required Information, as defined in the Common Agreement.
- Applicant must demonstrate that it has the ability to perform all of the required functions of a QHIN in the manner required by the Common Agreement, the SOPs, the QTF, and all other applicable guidance from the RCE.
- Applicant must demonstrate that it has in place, at the time of its application to be Designated, the organizational infrastructure and legal authority to comply with the obligations of the Common Agreement and a functioning system to govern its Health Information Network. Must demonstrate it has the resources and infrastructure to support a reliable and trusted network.

Draft Onboarding and Designation SOP

This draft SOP identifies the process and specific requirements for Onboarding and Designation, including demonstrating satisfaction of the QHIN Eligibility Criteria, the review and disposition of all QHIN applications, and the testing process.

Section I: Eligibility Requirements

Section II: QHIN Application Process

1. Beginning the application process
2. RCE review of applications for completeness
3. RCE review of complete applications
4. Assertion of compliance

Section III: Pre-Production Testing Process

1. QHIN Onboarding
2. QHIN Onboarding Process
3. Testing Overview
4. Pre-Production Testing Timeline
5. Conformance Testing Process
6. Non-Production Partner Testing

Section IV: Designation & Post-Production Testing

1. Production Connectivity Validation

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

SOP: QHIN Security for the Protection of TEFCA Information

Rev. 1 (updated as of May 2022)

SOP: QHIN Security Requirements for the Protection of TEFCA Information

- **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. Independent Review: Certification bodies and third-party assessment organizations must be qualified, independent third parties.
  5. Confidentiality of Security Assessment Reports or Summaries, POA&Ms, and Related Security Documentation
  6. Cybersecurity Council

Third-Party Cybersecurity Certification

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- Every QHIN must be certified under a nationally recognized security framework from a list of pre-approved certifications/certifying bodies developed by the RCE.
- The RCE will maintain and publish a list of certifying bodies which meet the RCE's security certification requirements
  a) Any third-party accreditation or certification body that can demonstrate adherence to the requirements listed in the SOP may be considered for inclusion
  b) Interested parties should refer to the official RCE-published list of currently approved certifications available at https://rce.sequoiaproject.org/qhin-cybersecurity-certification
  c) Certification bodies providing services that meet these requirements, but that have not yet been utilized by a designated QHIN, may also request approval to be included

ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Key Takeaways

Takeaways

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- TEFCA SOP Release Schedule is now available.
  - » SOPs and resources will provide more implementation details and will help potential QHINs, Participants, and Subparticipants make decisions regarding how they will leverage the network of TEFCA-compliant QHINs to meet their organizational goals.
  - » The RCE looks forward to engaging with stakeholders to inform the development of these SOPs, including by receiving feedback on the RCE monthly calls.

- Stay tuned for more information about upcoming plans for FHIR standards pilots, in alignment with the FHIR Roadmap for TEFCA Exchange.

- We are excited about the broad interest and engagement among stakeholders in TEFCA and look forward to continuing to engage through upcoming educational webinars and outreach events.

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/

Draft QHIN SOP and Application Webinar
Wednesday, May 25 | 3:00 – 5:00 p.m. ET

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

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Appendix: Additional Information for SOP: QHIN Security for the Protection of TEFCA Information

Rev. 1 (updated as of May 2022)

Third Party Cybersecurity Certification (Ctd). (summarized)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- As part of a QHIN's third-party cybersecurity certification process, the certification body must:
  a) Ensure assessments are conducted in accordance with the NIST Cybersecurity Framework (CSF), specifically all categories in the CSF and NIST 800-171 are required, with assessments conducted using NIST 800-53 moderate as a reference
  b) Review the QHIN's HIPAA security analysis (consistent with §164.308(a)(1)(ii)(A))
  c) Verify Common Agreement requirements for technical audits and assessments are met

Refer to the draft SOP for all draft requirements and/or details.

Annual Technical Audits (summarized)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

Each QHIN must obtain a third-party technical audit of in-scope systems on no less than an annual basis. A QHIN's annual third-party technical audit must include the following:

(a) Adoption of the NIST CSF: All categories in the CSF and NIST 800-171 are required, with technical audits conducted using NIST 800-53 moderate as a reference

(b) Requirements of the HIPAA Security Rule, including HIPAA security analysis (consistent with §164.308(a)(1)(ii)(A))

(c) Comprehensive internet-facing penetration testing

(d) Internal network vulnerability assessment

(e) A review of security requirements from the Common Agreement, security related SOPs, and other security requirements as may be required by the RCE at time of assessment

(f) Utilize methodologies and security controls consistent with Recognized Security Practices, as defined by Public Law No: 116-321

Refer to the draft SOP for all draft requirements and/or details.

Reports or Summaries of Certification Assessments & Annual Technical Audits (summarized)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- The QHIN shall provide a report or summary of the results of its certification renewal assessments and annual technical audits within thirty (30) days of the QHIN's receipt of the report.
- If the assessment identifies any unaddressed deficiencies that meet the definition of moderate impact or high impact, the QHIN must take appropriate action(s) to mitigate the risk(s) of any such deficiencies.
- The SOP contains further requirements for the development, implementation, and routine reporting of an appropriate plan of action and milestones (POA&M) to identify the necessary activities, resources needed, responsible party/parties, reasonable mitigation efforts and/or compensating controls, and the timetable to full remediation.

Refer to the draft SOP for all draft requirements and/or details.

Independent Review (summarized)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- Certification bodies and third-party assessment organizations utilized by Certification bodies or QHINs must be qualified, independent third parties.
  - (a) Organizations conducting assessments must attest (in the assessment report) to having no organizational conflicts of interest with the certification body or the organization being assessed
  - (b) Assessors must be security professionals with active or current security certifications requiring ongoing credential maintenance
  - (c) Third party assessments and certification activities are subject to quality review or sampling by the certification body to ensure consistency and quality

Refer to the draft SOP for all draft requirements and/or details.

Confidentiality of Documentation (summarized)

ONC TEFCA RECOGNIZED COORDINATING ENTITY

- The RCE shall treat reports or summaries of the security assessment, POA&Ms, and any related documentation, such as milestone updates requested by the RCE or Cybersecurity Council, as Confidential Information and will not disclose them to anyone except:
  - (a) To the Cybersecurity Council, at the RCE's discretion
  - (b) To the Governing Council, upon recommendation of the Cybersecurity Council
  - (c) As required by law; or
  - (d) As requested by ONC in furtherance of the RCE's obligations under the Cooperative Agreement

Refer to the draft SOP for all draft requirements and/or details.