



DURSA Overview for Secretarial Committee on Data Sharing

November 8, 2011

Steven D. Gravely, J.D., M.H.A.
(804) 697-1308
steve.gravely@troutmansanders.com



Trust is a Choice

How do we make trust a reasonable choice for health information exchange?



Universal Components of Trust

Developed by TS in collaboration with NeHC, funding provided by ONC

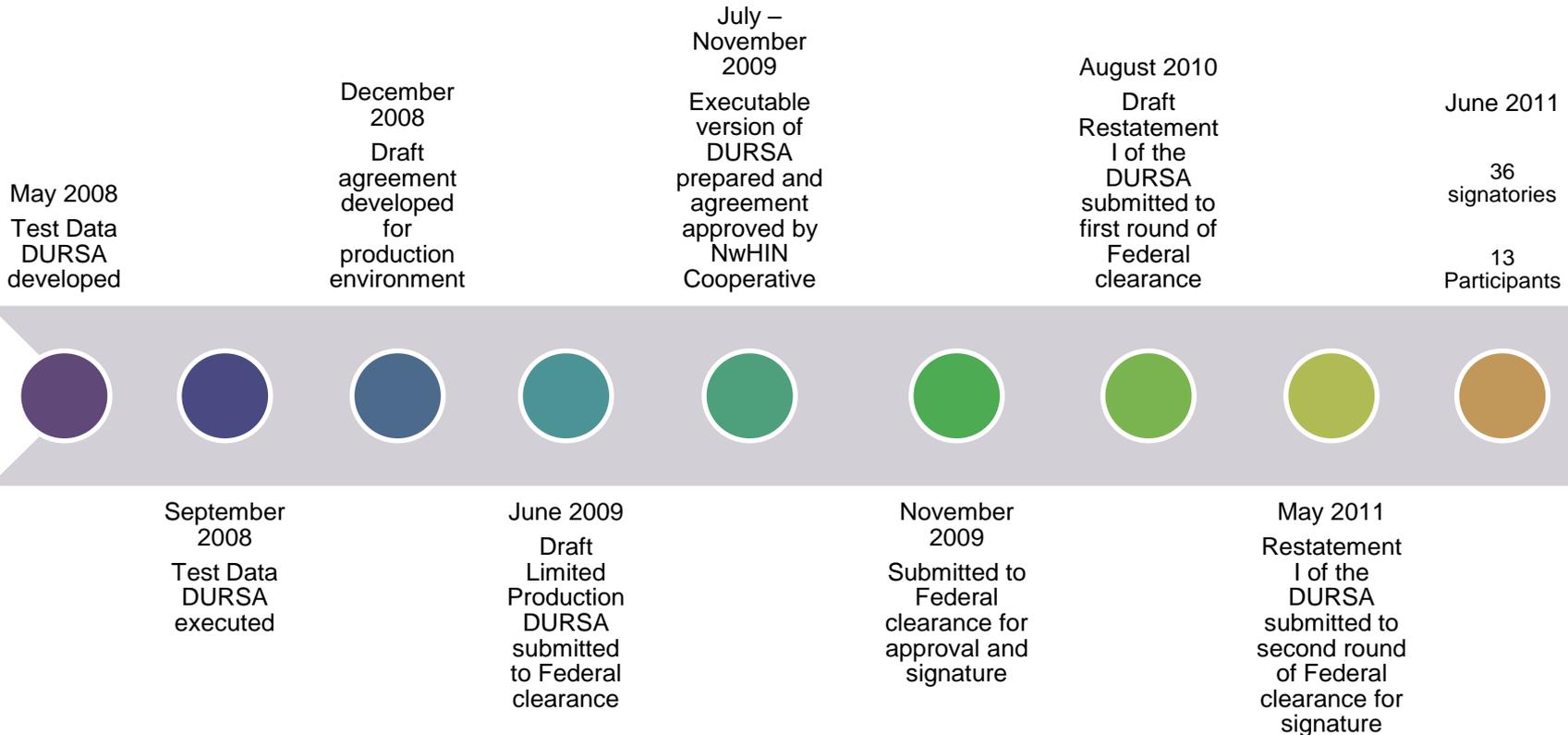
NwHIN Work Group has recommended this framework to the HIT Policy Committee



Data Use and Reciprocal Support Agreement

- A comprehensive, multi-party trust agreement that is signed by all eligible entities who wish to exchange data among Participants
- A scalable alternative to multiple “point-to-point” agreements, which Federal participants have asserted are not sustainable for widespread information exchange
- Requires signatories to abide by common set of terms and conditions that establish Participants’ obligations, responsibilities and expectations
- The obligations, responsibilities and expectations create a framework for safe and secure health information exchange, and are designed to promote trust among Participants and protect the privacy, confidentiality and security of the health data that is shared
- As a living document, the agreement will be modified over time
- The DURSA does NOT preempt ONC’s governance rule-making process in any manner.

DURSA Milestones



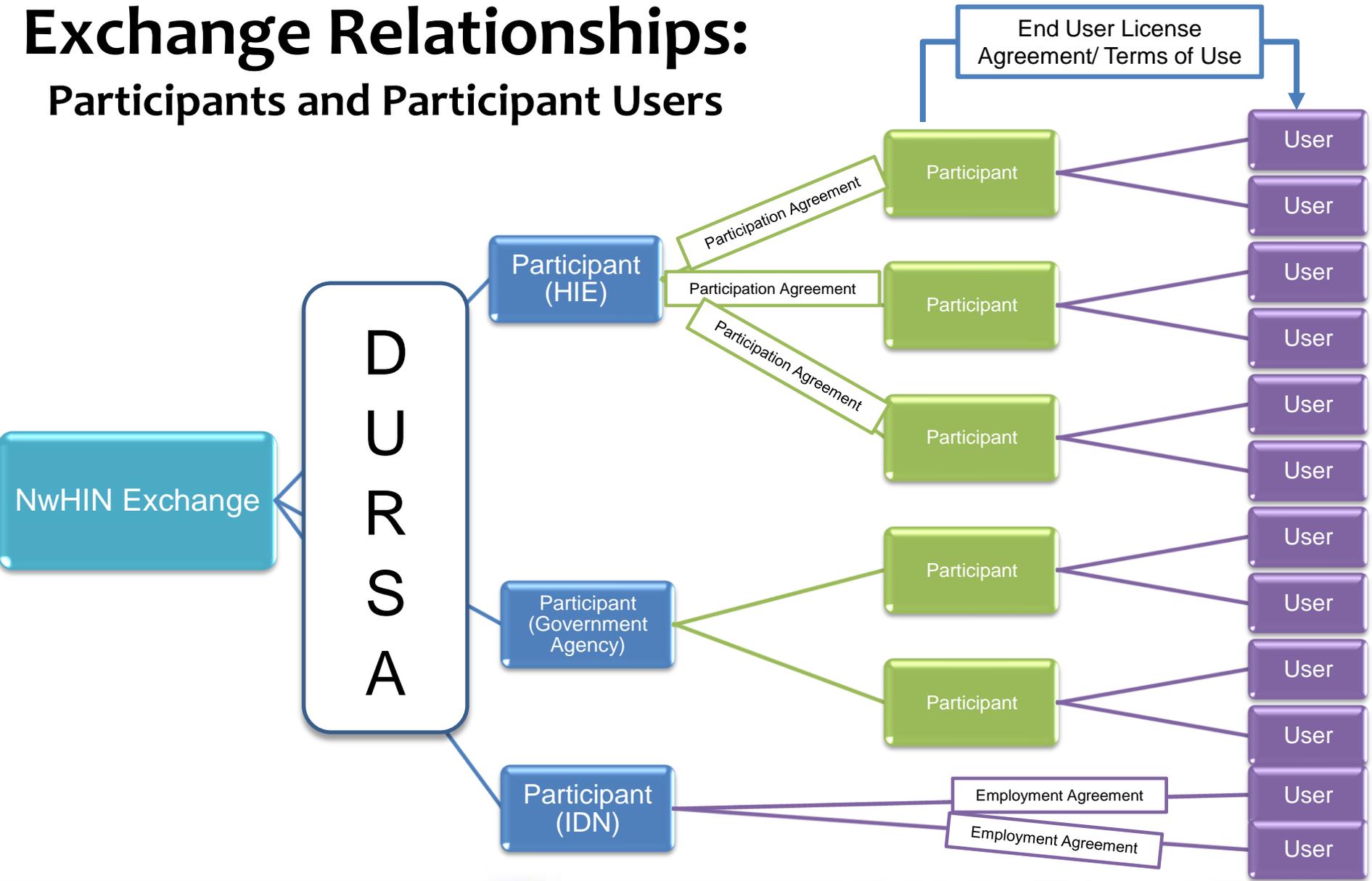
Important Terms

- **Applicable Law:** the law of the jurisdiction in which the Participant operates
 - For non-Federal Participants, this means the law in the state(s) in which the Participant operates and any applicable Federal law.
 - For Federal Participants, this means applicable Federal law.
- **Message:** electronic transmission of Message Content Transacted between Participants using the Specifications
- **Message Content:** information contained within a Message or accompanying a Message
- **Participant:** a signatory to the DURSA
- **Participant Users:** any person who is authorized to Transact Message Content through the respective Participant's system
- **Permitted Purposes:** the reasons for which Participants may legitimately Transact Message Content
- **Specifications:** technical specifications adopted by the Coordinating Committee to prescribe data content, technical and security requirements for the Participants
- **Submitter:** the Participant who submits Message Content through a Message to a Recipient for a Permitted Purpose
- **Transact:** to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content during the Specifications

Basic Premises

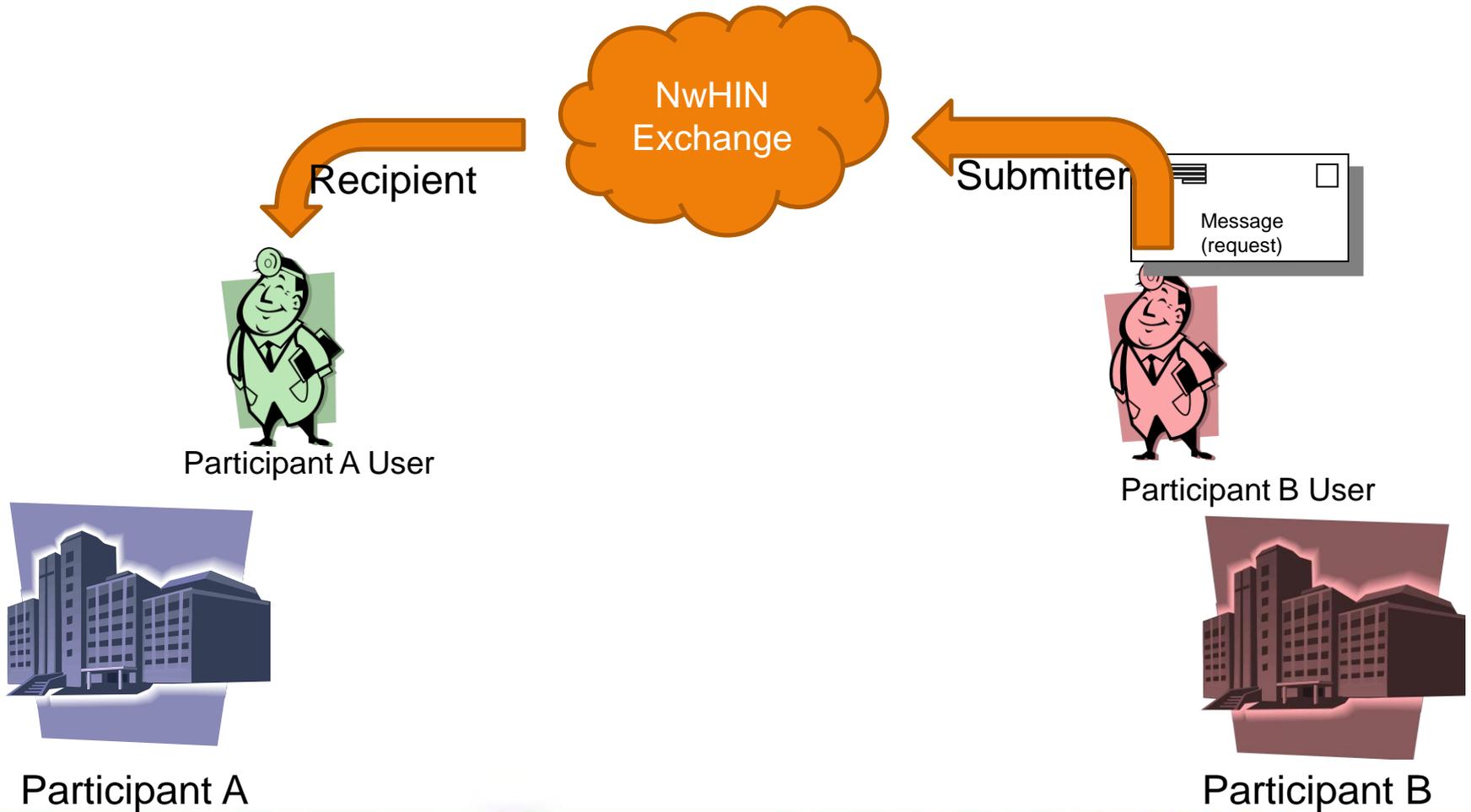
- Assumes that each Participant has trust relationships in place with its agents, employees and data connections (end users, systems, data suppliers, networks, etc.).
- Each Participant must comply with Applicable Law. Nothing in the DURSA is intended to conflict with Applicable Law.
- Each Participant will comply with the HIPAA Privacy and Security rules either because it is a Covered Entity, a Business Associate or because it is required to do so by the DURSA.
- The Coordinating Committee provides oversight and support for the Participants.
- The DURSA is written to apply to all types of transactions, not just query/retrieve.

Exchange Relationships: Participants and Participant Users



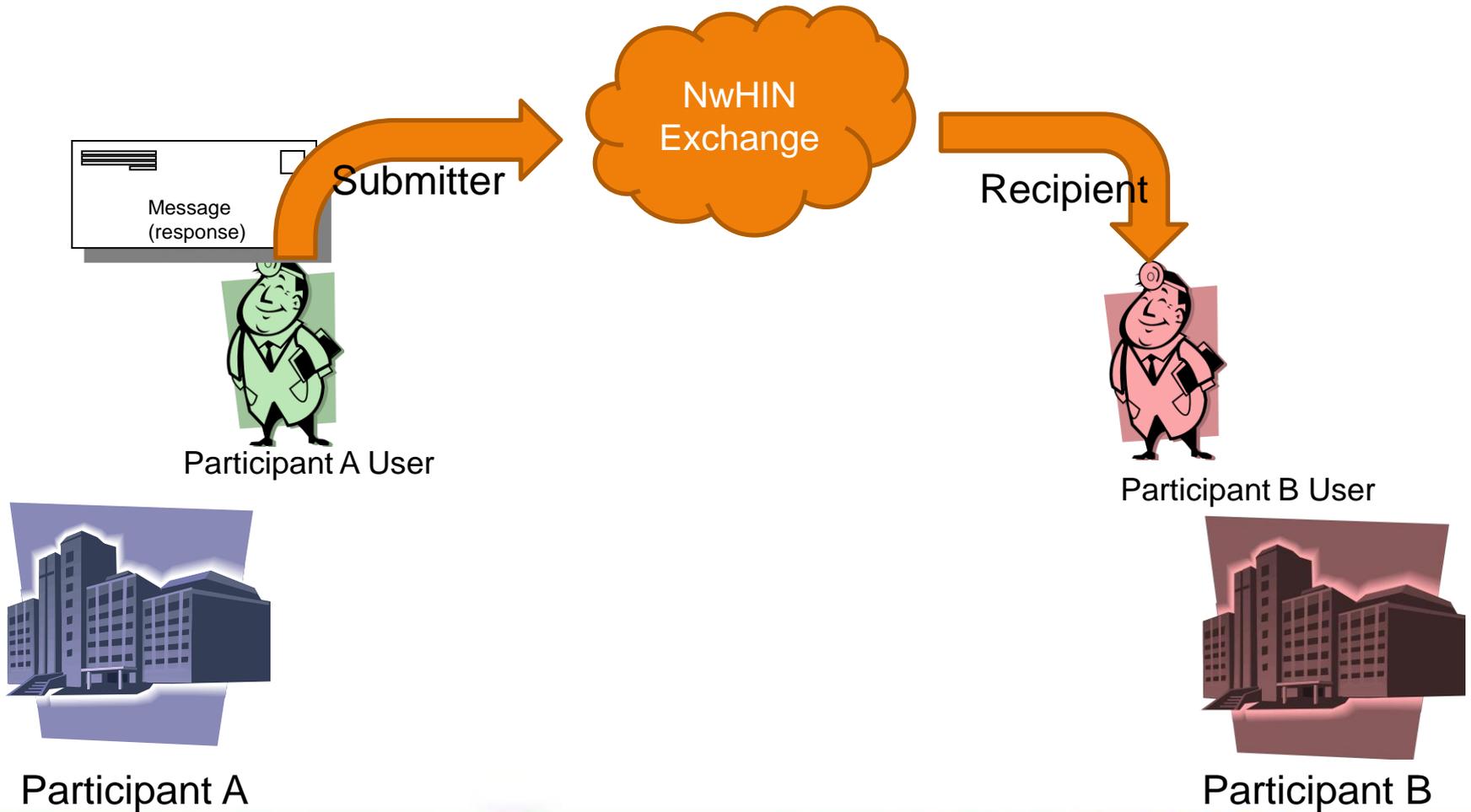
Exchange Relationships:

Submitters and Recipients

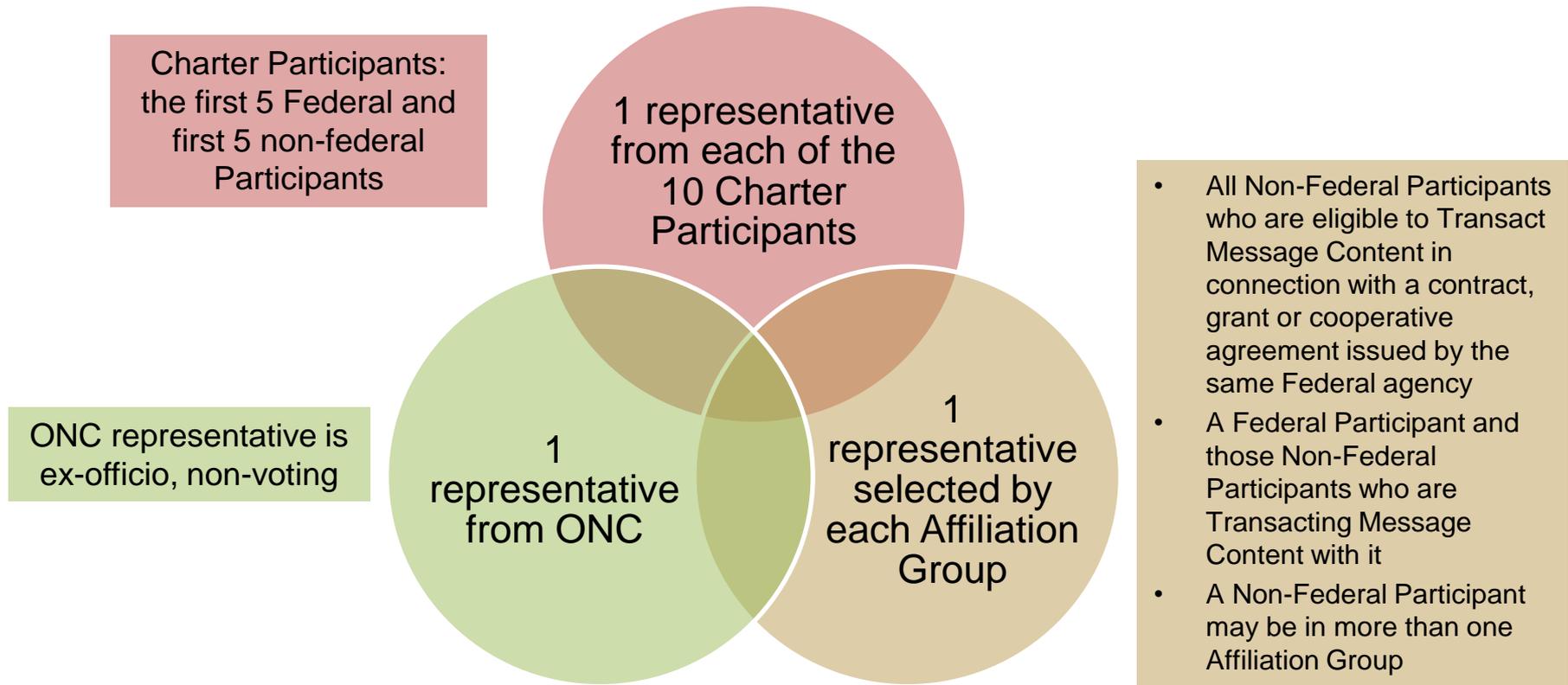


Exchange Relationships:

Submitters and Recipients



Coordinating Committee Composition



No Participant shall have more than one employee or contractor serving concurrently as CC representatives

General Coordinating Committee Responsibilities

General Responsibilities

- Developing and amending Operating Policies and Procedures
- Receiving reports of Breaches and acting upon such reports
- Managing the amendment of the DURSA
- Fulfilling any responsibilities delegated by the Participants to the Coordinating Committee

Participant Oversight Responsibilities

- Determining whether to admit a New Participant
- Maintaining a definitive list of all transaction patterns supported by each of the Participants
- Suspending or terminating Participants in accordance with DURSA
- Resolving disputes between Participants in accordance with DURSA

Technical Responsibilities

- Evaluating, prioritizing and adopting new and revised Performance and Service Specifications and Validation Plans for the Participants
- Maintaining a process for managing versions of the Performance and Service Specifications for the Participants, including migration planning
- Evaluating requests for the introduction of Emergent Specifications into the production environment used by the Participants
- Coordinating with ONC to help ensure the interoperability of the Performance and Service Specification with other health information exchange initiatives

Exchange Only for “Permitted Purposes”



Consent and Authorization

- A Submitter must meet all legal requirements before disclosing the data, including, but not limited to, obtaining any consent or authorization that is required by law applicable to the responding Participant.
- When a request is based on a purpose for which authorization is required under HIPAA (e.g. for SSA benefits determination), the requesting Participant must send a copy of the authorization with the request for data. Requesting Participants are not obligated to send a copy of an authorization or consent when requesting data for treatment purposes.

Future Use of Data

- Once the Participant or Participant's end user receives data from another Participant (i.e. a copy of the other Participant's records), the recipient may incorporate that data into its records and retain that information in accordance with the recipient's record retention policies and procedures.
- The recipient can re-use and re-disclose that data in accordance with all applicable law and the agreements between a Participant and its end users.

Autonomy Principle

- Participants determine their own access policies based on Applicable Law and business practices
- These access policies are used to determine whether and how to Transact Message Content

Duty to Respond for Treatment

- Participants that allow their respective end users to request data for treatment purposes have a duty to respond to requests for data for treatment purposes.
- This duty to respond means that if actual data is not sent in response, the Participant will at a minimum send a standardized response to the requesting Participant.
- Participants are permitted, but not required, to respond to all other (non-treatment) requests.
- The DURSA does not require a Participant to disclose data when such a disclosure would conflict with Applicable Law or its access policies.

Duty to Identity-Proof and Authenticate Users

Identity Proof Users:

Validate information about Users prior to issuing the User credentials

Authenticate Users:

Use the credentials to verify the identity of Users before enabling the User to transact Message Content

Self-Auditing Capability

- Each participant shall have the ability to monitor and audit all access to and use of its System related to the DURSA, for system administration, security, and other legitimate purposes.
- Each Participant shall perform those auditing activities required by the Performance and Service Specifications.

Operating Policies and Procedures

- All Participants must comply with OP&Ps
- OP&Ps address:
 - Qualifications, requirements and activities of Participants when transacting message content with other Participants
 - Support of the Participants who wish to transact message content with other Participants
 - Management, operation and maintenance of the Performance and Service Specifications

Performance and Service Specifications

- Each Participant identifies the Transaction Pattern(s) that it will support.
- For each Transaction Pattern it supports, the Participant will choose whether it will be a Submitter, a Recipient or both.
- Require the Participant to only comply with the Specifications associated with the supported Transaction Pattern(s).
- Require all Participants to comply with the mandatory set of Specifications.

OP&P and Specification Adoption Process

CC solicits
comments from
the Participants

CC approves new
or amended
OP&Ps or
Specifications

30 day objection
period

Did 1/3 of
Participants object?

NO

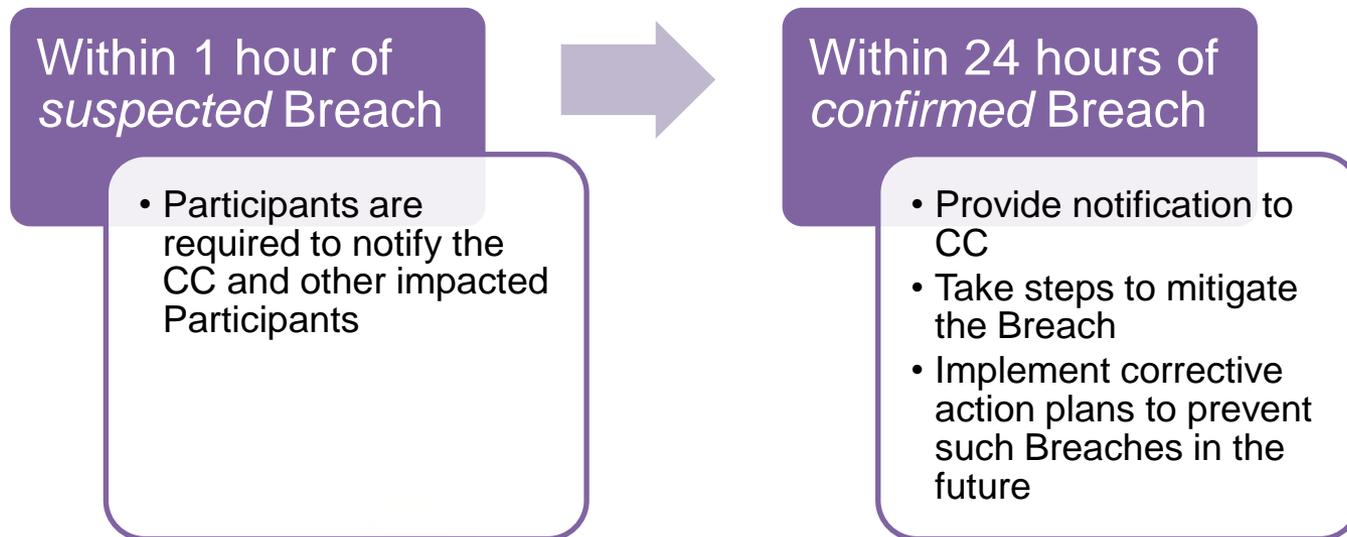
New or amended
OP&Ps or
Specifications go
into effect

YES

Participants Vote
– If 2/3
Governmental
and 2/3 Non-
Governmental
Participants
approve, new or
amended OP&P
or Specification
goes into effect

Breach Reporting

- Breach = “the unauthorized acquisition, access, disclosure, or use of Message Content while Transacting such Message Content pursuant to this Agreement”
- The breach reporting process is **NOT** intended to address any obligations for notifying consumers of breaches, but simply establishes an obligation for Participants to notify each other and the Coordinating Committee when Breaches occur to facilitate an appropriate response.



Dispute Resolution

- Disputes that may arise between Participants will be relatively complex and unique
- Mandatory, non-binding dispute resolution process



Voluntary Suspension by Participant

- Service Level Interruptions – planned or unplanned interruption resulting in Participant having to temporarily cease exchanging Message Content
 - < 8 business hours: Participant may, but is not required to, voluntarily suspend their right to exchange
 - > 8 business hours: Participant must voluntarily suspend their right to exchange
- Participant will send an e-mail notification to CC Secretary informing of their voluntary suspension, including:
 - Reason for suspension
 - Commencement date of suspension
 - Duration of suspension
- Participant will post a message to Secure Site informing of its voluntary suspension
- Approval by CC
 - If the suspension will last <10 days and not cause the Participant to exceed 40 days voluntary suspension in the past 12 months, no CC approval is required.
 - If it will last >10 days or cause the Participant to exceed 40 days in the past 12 months, CC must approve the voluntary suspension.
- At the conclusion of the suspension, the Participant will send an e-mail to the CC Secretary and update the Secure Site that they are ready to begin transacting Message Content again

Suspension with Cause by Coordinating Committee

- Upon receipt of a complaint, report or other information that causes the CC to question whether a Participant is creating an immediate threat or causing irreparable harm to another party, the CC has the authority to launch an investigation
- Upon completion of preliminary investigation and determination of a substantial likelihood that a Participant's acts or omissions created an immediate threat or will cause irreparable harm to another party, CC has the power to summarily suspend a Participant, pending the submission and approval of a corrective action plan
- CC will do following within 12 hours of suspending Participant's right to transact message content
 - Provide notice to all Participants
 - Provide suspended Participant a written summary of reason for suspension
- Participant has 3 business days to provide CC with a detailed plan of correction or an objection to the suspension
- CC will review and either accept or reject the plan of correction within 5 business days
 - If accepted, the Participants right to exchange will be reinstated upon completion of the plan of correction
 - If rejected, the CC and Participant will work together to prepare an acceptable plan of correction
 - If the CC and Participant can not reach agreement on the plan of correction, the CC may terminate the Participant

Termination by Coordinating Committee

- Reasons for termination
 - After suspending a Participant when there is a substantial likelihood that their actions will cause an immediate threat or irreparable harm
 - Participant is in material default of the performance of a duty or obligation imposed by the DURSA and such default has not been cured within 30 days of notice to the Participant
- Participants may appeal their termination through the Dispute Resolution Process
- Once a Participant has been terminated, the CC will provide notice to all other Participants

Allocation of Risk

- The DURSA contains a number of representations, warranties and disclaimers.
- With respect to liability, each Participant is responsible for its own acts or omissions and not for the acts or omissions of any other Participant.
- Each Participant is responsible for any harm caused by its Users, if its Users gained access to the Exchange as a result of the Participant's breach of the Agreement or its negligent conduct.
- There are no hold harmless or indemnification provisions because the Governmental Participants cannot agree to indemnify.

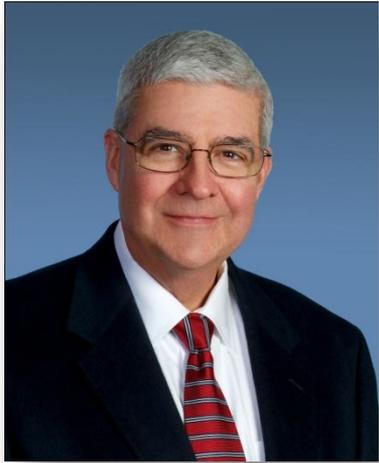
Questions?

Steve Gravely

steve.gravely@troutmansanders.com

(804) 697-1308





Steven D. Gravely, J.D., M.H.A.

Partner, Healthcare Practice Group Leader

Mr. Gravely focuses his practice in the area of health law, health information technology as well as disaster preparedness and response issues for critical infrastructure industries. He has represented hospitals and other healthcare providers for over 25 years in the full spectrum of healthcare legal issues. In the health information technology space, Mr. Gravely was the lead author of the first of its kind Data Use and Reciprocal Support Agreement (DURSA) which is the fundamental legal document which supports interoperable health data exchange using the Nationwide Health Information Network. Mr. Gravely leads and facilitates multiple national workgroups on complex issues related to the legal structure, trust agreements and governance issues of the NHIN. Additionally, Mr. Gravely assists with the development of Health Information Exchanges (HIEs), including advising on: (i) legal structure; (ii) governance; (iii) privacy and security frameworks; (iv) operational policies and procedures; (v) breach notification; and (vi) data exchange agreements. Mr. Gravely provides expert advice to clients on e-health issues including HIPAA Privacy and Security, FISMA, ARRA, and *Health Information Technology for Economic and Clinical Health Act* (HITECH), as well as strategic advice on emerging health information technology issues, privacy and security, and “meaningful use.”