eHealth Exchange™

Data Use and Reciprocal Support Agreement (DURSA) Overview

Steve Gravely, Troutman Sanders LLP
Jennifer Rosas, eHealth Exchange Director

January 12, 2017

Introduction

Steve Gravely

- Partner and Healthcare Practice Group Leader, Troutman Sanders LLP
- Nearly 40 years experience in the healthcare industry including hospital operations and hospital management and law
- Led the national workgroup that developed the DURSA
- Serves as General Counsel for The Sequoia Project and other digital health companies

DURSA Topics

- Context and Drill-Down
- DURSA Flow-Down Provisions
- DURSA Breach and Breach Notification Requirements
- Q & A

DURSA Webinar

CONTEXT AND DRILL-DOWN

The eHealth Exchange is the Network

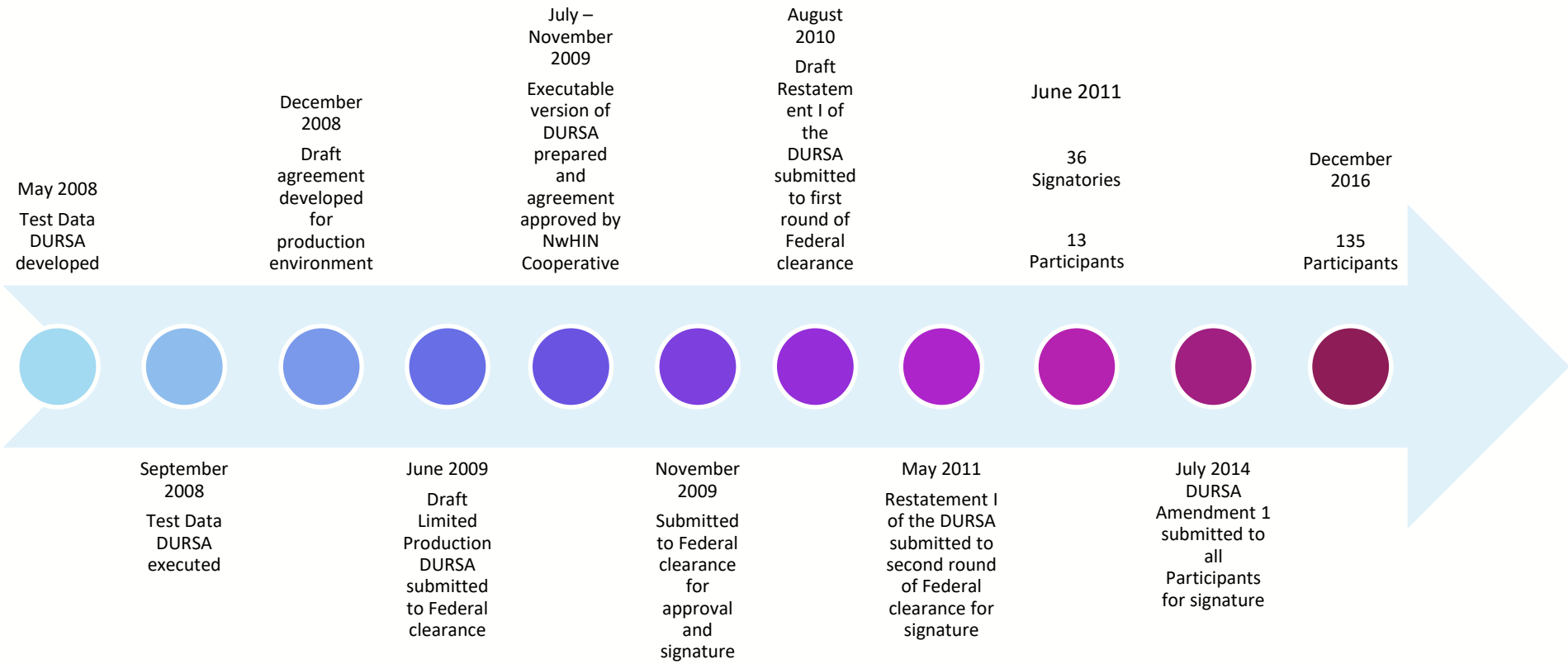
- The eHealth Exchange network started as an ONC program initiative related to the nationwide health information network (e.g. NHIN, NwHIN Exchange)
- The network discontinued operating under the NHIN moniker and changed its name to eHealth Exchange when it moved to a private sector initiative, supported by The Sequoia Project
- The eHealth Exchange network exists independently of Sequoia, the company
- eHealth Exchange support staff provide support to the eHealth Exchange network, the Coordinating Committee and Participants – *under the direction of the Coordinating Committee*
- The Coordinating Committee has authority over the eHealth Exchange network, not Sequoia and Sequoia is not a party to the DURSA,

What is the DURSA?

- 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 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
- The DURSA was developed through an intensive effort facilitated by ONC, with consensus among a diverse group of private and state entities and federal agencies. As a living document, the agreement will be modified over time under the direction of the Coordinating Committee.

Developed by Troutman Sanders

DURSA Historical Milestones



Developed by Troutman Sanders

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
- **Performance & Service Specifications**: technical specifications and testing requirements adopted by the Coordinating Committee to prescribe data content, technical and security requirements, and test plans 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

Developed by Troutman Sanders

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 of eHealth Exchange and support for the Participants.
- Participants choose which use cases they wish to support in production, which includes a variety of exchange methods, such as: push, query / retrieve and publish/subscribe. The DURSA is written to apply to all types of transactions, not just query/retrieve.

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.
- Participants must comply with a core set of mandatory specifications.
- In addition, Participants must comply with the additional Specifications associated with the supported Transaction Pattern(s).
- The current Specifications are available on the eHealth Exchange website.

Operating Policies and Procedures (OPPs)

- All Participants must comply with OPPs.
- OPPs 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.
- The OPPs are available on the eHealth Exchange website.

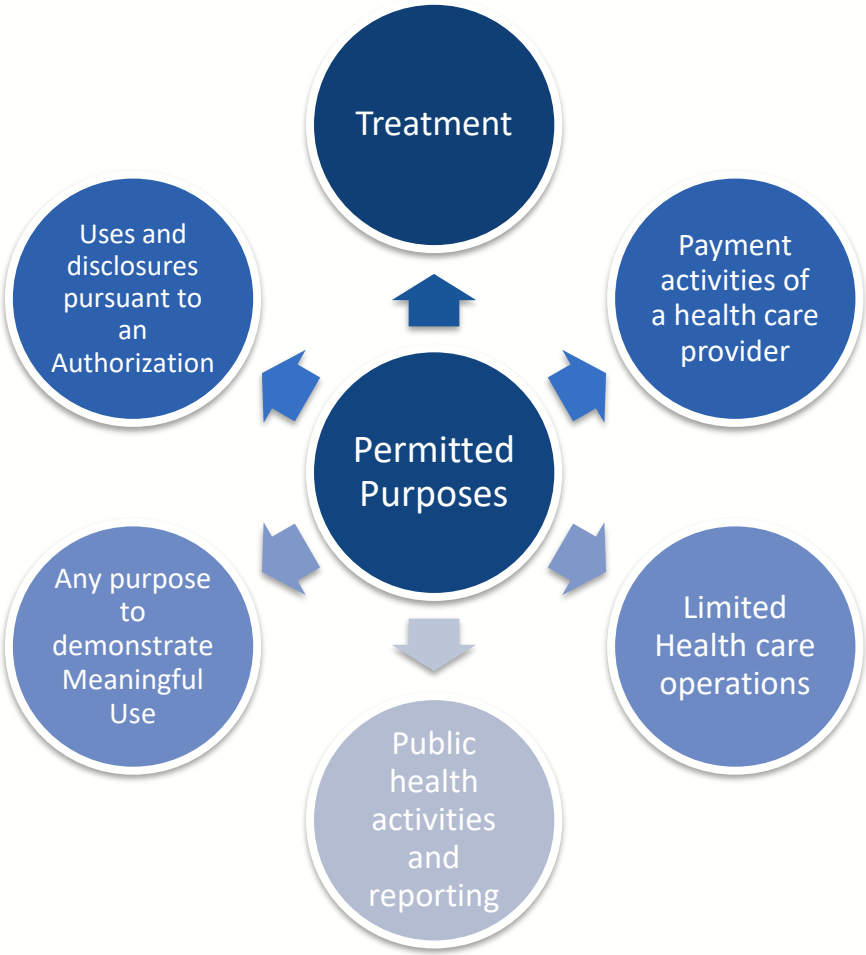
Developed by Troutman Sanders

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.

Developed by Troutman Sanders

Exchange Only for "Permitted Purposes"



The DURSA limits treatment, payment and operations beyond what HIPAA permits.

Developed by Troutman Sanders

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.

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.

Developed by Troutman Sanders

DURSA Webinar

DURSA FLOW-DOWN PROVISIONS

DURSA Flow-Down Provisions (Sections 15.04 & 15.05)

Each Participant has the duty to make sure their users, participating organizations and/or technology partners comply with certain DURSA provisions.

Section 15.04: Enforceable Agreements or user policies with participating organizations or users that:

- Comply with Applicable Law
- Reasonably cooperate with issues related to the DURSA
- Permitted Purpose
- Use of data in accordance w/DURSA
- 1hr/24hr breach notification
- Protect passwords and security measures

Section 15.05: Enforceable agreements with technology partners that:

- Comply with Applicable Law
- Protect privacy and security of Message Content
- Breach notification as soon as reasonably practicable
- Reasonably cooperate on issues related to the DURSA

Developed by Troutman Sanders

DURSA Webinar

DURSA BREACH AND BREACH NOTIFICATION REQUIREMENTS

DURSA Breach: Definition

- **Breach:** "the unauthorized acquisition, access, disclosure, or use of Message Content **while Transacting such Message Content**"
- A breach does not include either of the following:
  1. **any unintentional acquisition, access, disclosure**, or use of Message Content by an employee or individual acting under the authority of a Participant or Participant User **if** —
     - Made in good faith and within the course / scope of that individual's employment / engagement; and
     - The information is not further acquired, accessed, disclosed or used by the individual;
  2. any acquisition, access, disclosure or use of information contained in or available through the Participant's System that was not ***directly related to Transacting Message Content***.
- ***A DURSA Breach IS NOT the same as a HIPAA breach. The definition is more narrow than HIPAA.***
- 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 a DURSA Breach occurs, to facilitate an appropriate response.

Developed by Troutman Sanders

Examples of a DURSA Breach

- The server where the eHealth Exchange certificates are installed is compromised.
- Man in the middle attack where data is intercepted
- In most cases, the IT personnel managing the server (not the end user) would become aware of a DURSA breach since it is specific to the connection

Breach Reporting

- Participants are required to notify the eHealth Exchange Coordinating Committee and other impacted Participants of Breaches within specific timeframes.

Within 1 hour of *suspected* Breach

- Participants are required to notify the CC and other impacted Participants.
- It may take time to confirm a 'suspected' breach and the notification is expected within one hour AFTER that.

Within 24 hours of *confirmed* Breach

- Provide notification to CC
- Take steps to mitigate the Breach
- Implement corrective action plans to prevent such Breaches in the future
- It may take time to complete the investigation to confirm that a Breach occurred. Notification is expected within 24 hours AFTER that process as additional information is required per OPP #7 – Breach Notification.

Ways to Implement the DURSA Flow-Down Provisions

- The eHealth Exchange Application asks for a statement which explains whether / how applicant's policies and procedures and /or agreements obligate users with eHealth Exchange connectivity to comply with the flow-down provisions.
- Take steps to explain how you will modify / create policies and procedures to comply with the provisions.
  - **Involve your legal department and review eHealth Exchange OPP #7: Breach Notification**
  - Develop an addendum to existing agreements with other organizations and technology partners to ensure that each of the provisions are covered contractually.
  - Establish a training program to train employees and other organizations and technology partners .
  - Provide education regarding the responsibilities to the DURSA
  - Update internal policies, procedures, and forms to include all of the provisions.
  - Provide evidence that the plan has been implemented prior to Go-Live.

Developed by Troutman Sanders

Modification to Policies (Sample Guidance)

- **Include the DURSA Definition of Breach**
  - *Data Use and Reciprocal Support Agreement (DURSA) – the legal, multi-party trust agreement that is entered into voluntarily by eHealth Exchange Participants in order to engage in electronic health information exchange activity (Exchange) using an agreed upon set of national standards, services and policies. For the purposes of meeting the DURSA requirements, a "Breach" shall mean the following:*
    - The unauthorized acquisition, access, disclosure, or use of message content while transacting such message content pursuant to the DURSA.
    - The term "Breach" does not include the following:
      - Any unintentional acquisition, access, disclosure or use of Message Content by an employee or individual acting under the authority of ABC Organization if such acquisition, access, disclosure or use was made in good faith and within the scope of the employee's duties and such message content is not further acquired, accessed, disclosed or use by the employee.
      - Any acquisition, access, disclosure or use of information contained in or available through an ABC Organization system where such acquisition, access, disclosure or use was not directly related to transacting message content.
  - The DURSA designates a Coordinating Committee to govern the operations of the Exchange and the DURSA which sets out the responsibilities and composition of the Coordinating Committee.

Sample Guidance

- **Review OPP #7 and Include Notification Procedures**
  - Upon discovering a potential Breach, immediately notify _____.
  - ABC Organization shall, within one (1) hour of discovering information that leads it to reasonably believe that a Breach may have occurred, alert other Exchange participants whose information may have been Breached and the Coordinating Committee. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach has occurred, ABC Organization shall provide a notification to all Exchange participants likely impacted by the Breach and the Coordinating Committee of such Breach.
  - The notification should include sufficient information for the Coordinating Committee to understand the nature of the Breach.
  - _____will be responsible for ensuring that such notification is consistent with the requirements set forth in the DURSA.

Q & A

For more information:

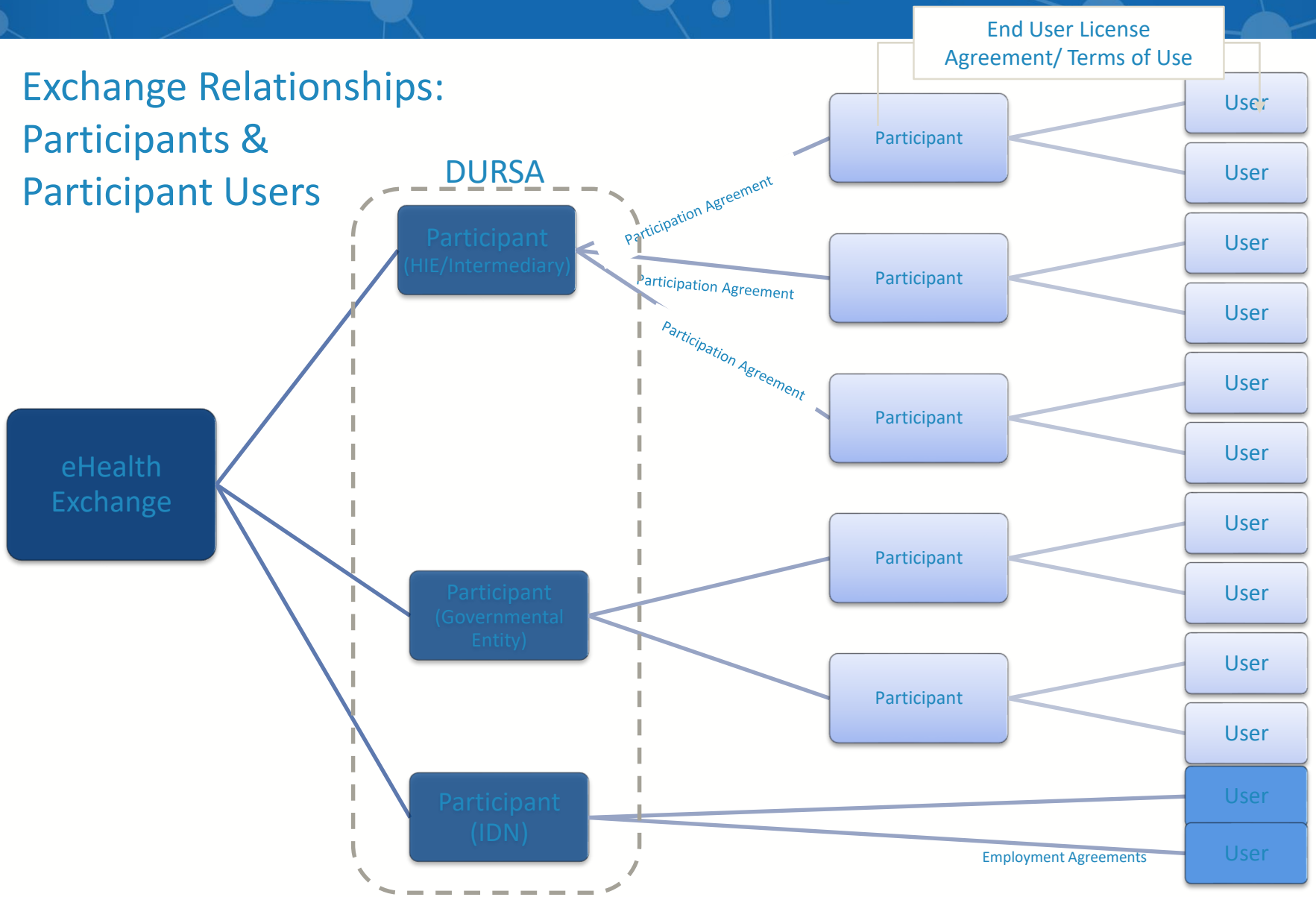
Website: http://www.ehealthexchange.com

E-mail: administrator@ehealthexchange.com

DURSA Webinar

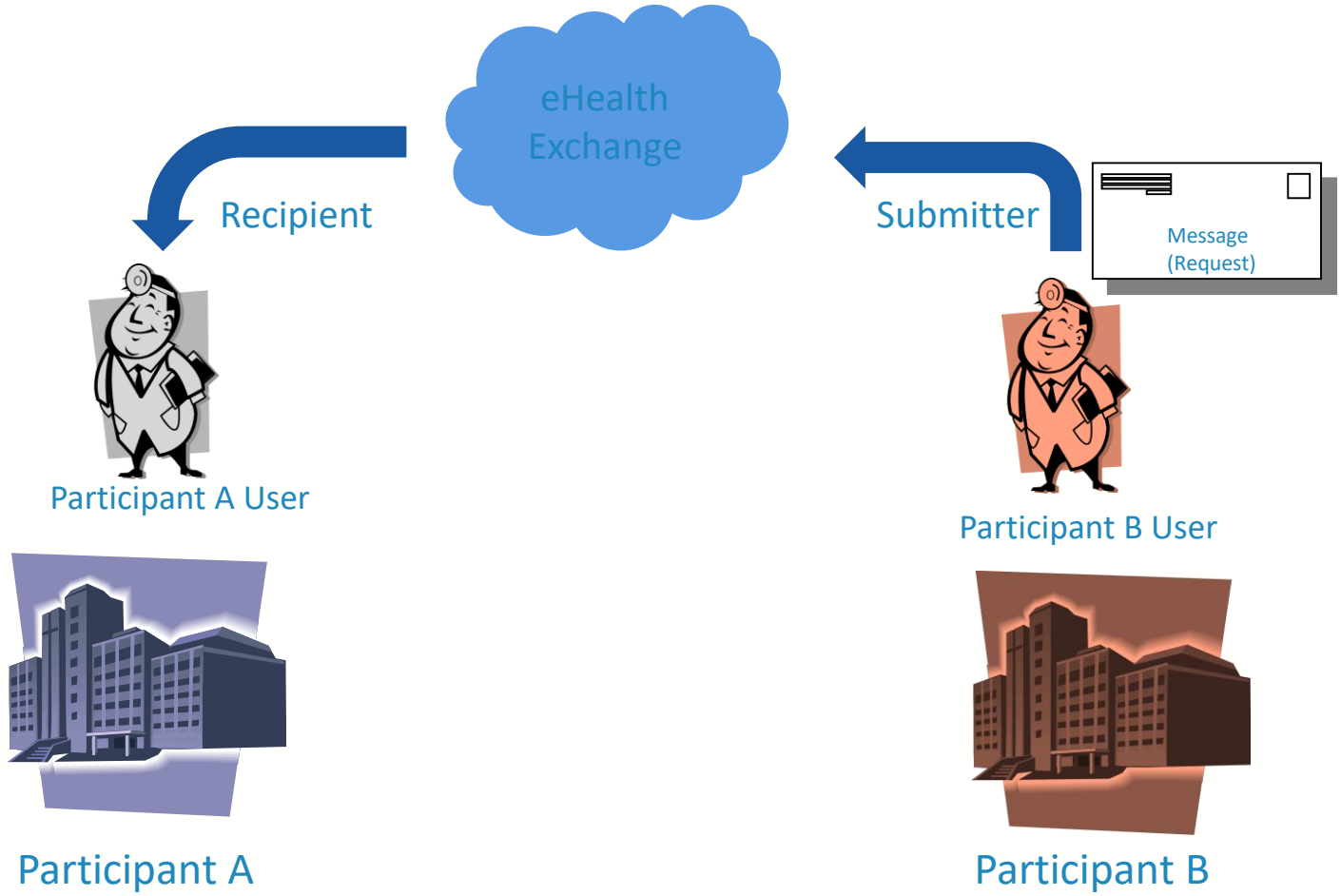
SUPPLEMENTAL SLIDES

Exchange Relationships: Participants & Participant Users



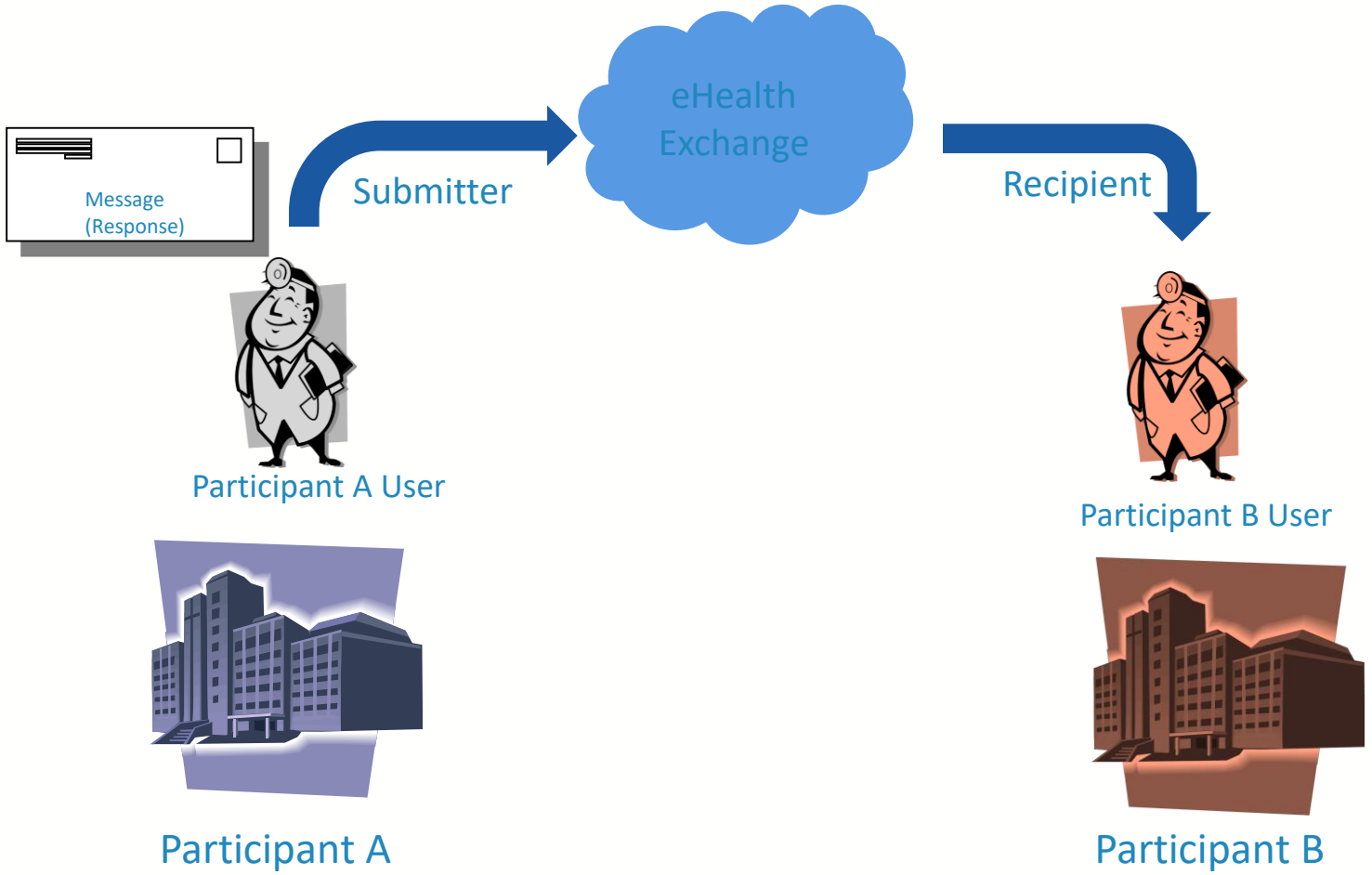
Developed by Troutman Sanders

Exchange Relationships: Submitters and Recipients Query Use Case - Request for Documents



Developed by Troutman Sanders

Exchange Relationships: Submitters and Recipients
Query Use Case - Respond to Request for Documents



Developed by Troutman Sanders

Identification and Authentication

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

Developed by Troutman Sanders

Developed by Troutman Sanders

Submitter Responsibilities

- Must submit the information in compliance with applicable law and represent that the message is:
  - for a Permitted Purpose;
  - sent by the Participant who has requisite authority to do so;
  - supported by appropriate legal authority, such as consent or authorization, if required by Applicable Law; and
  - sent to the intended recipient.
- Represent that assertions or statements related to the submitted Message, if required by the Performance and Service Specification or Operating Policies and Procedures, are true and accurate

Developed by Troutman Sanders

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.

Developed by Troutman Sanders

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.

Allocation of Risk

- 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.

Developed by Troutman Sanders

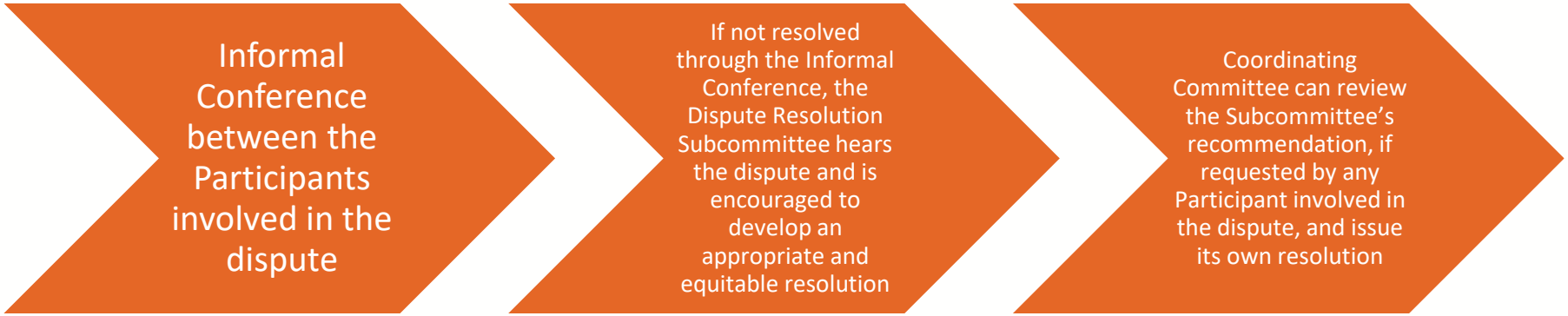
Representations & Warranties

- Protected Health Information (PHI) may not be used for eHealth Exchange testing and may not be sent to the Coordinating Committee.
- Participants represent data transmitted are an accurate representation of the data in their system at the time of transmission.
- Participants warrant that they have the authority to transmit information.
- Participants assert that they are not subject to a final order related to its obligations in the DURSA
- Participants represent that they are not excluded, debarred or ineligible for participating in federal contracts, or grants.
- Participants do not guarantee clinical accuracy, content or completeness of the messages transmitted.
- Participants, by virtue of signing the DURSA, do not assume any role in the care of an individual.
- Participants are not accountable for failure of carrier lines which are beyond the Participant's control.
- Data are provided "as is" and "as available", without a warranty of its "fitness for a particular purpose".
- Participants are not liable for erroneous transmissions, and loss of service resulting from communication failures by telecommunication service providers or other third parties.

Developed by Troutman Sanders

Dispute Resolution

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



Developed by Troutman Sanders