



# Establishing Trust in Health Information Exchange: The eHealth Exchange Model

August 21, 2014

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



TROUTMAN  
SANDERS

# 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

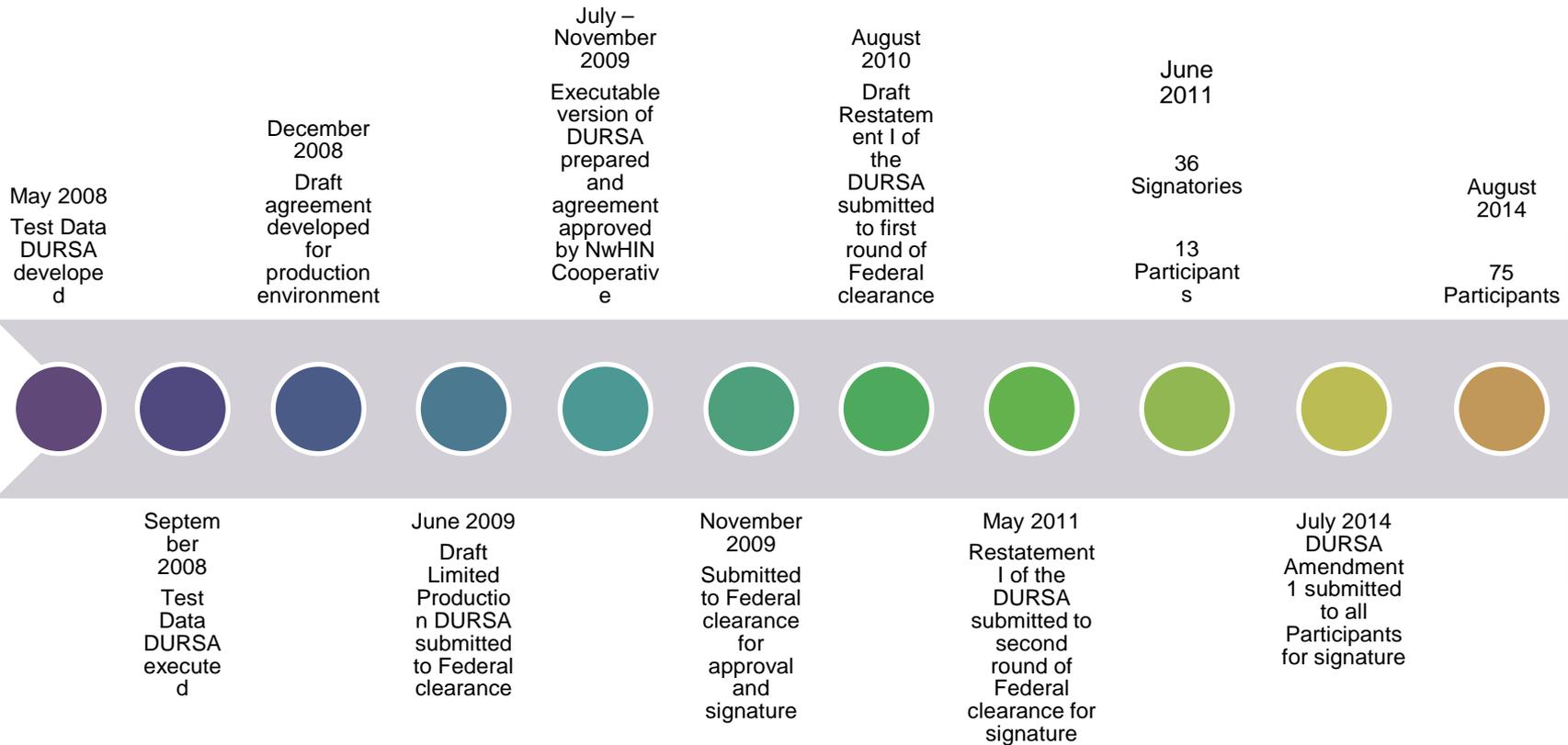
Endorsed by the  
federal HIT Policy  
Committee



# 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-it has already been revised twice since first adopted

# DURSA Milestones



# 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.

# Coordinating Committee Composition

5 representatives  
selected by the  
Federal  
Participants

9 representatives  
selected by the  
Non-Federal  
Participants

1 representative  
from ONC

1 representative  
selected by the  
HealtheWay  
Board of Directors

**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

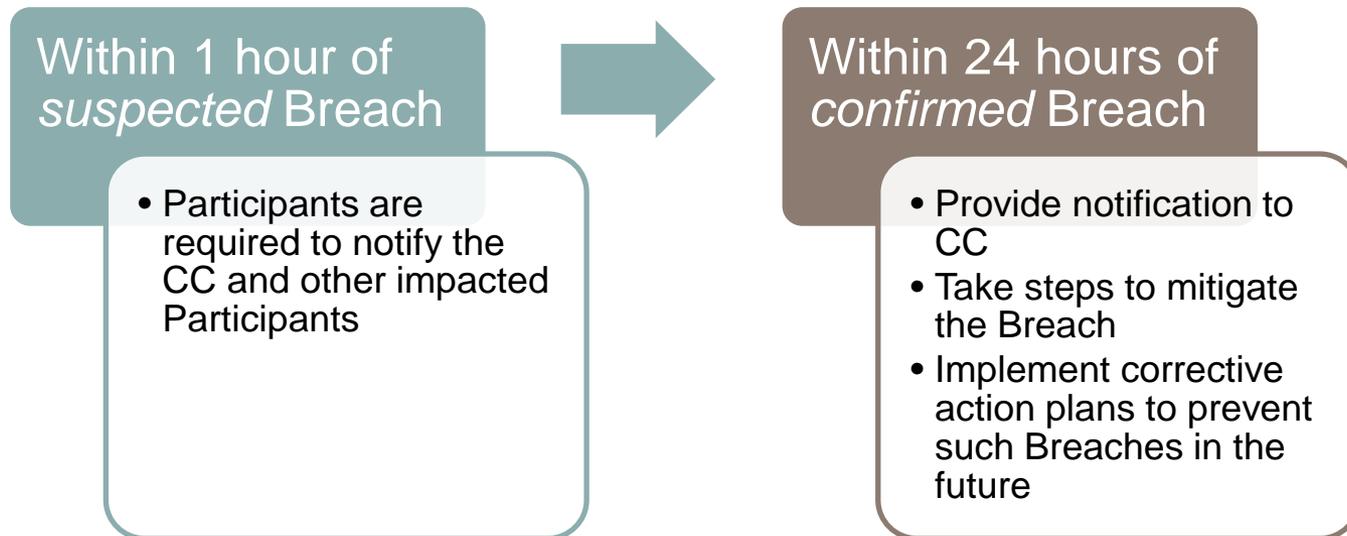
- All Participants must comply with OP&Ps
- OP&Ps address:
  - Governance of the network
  - Qualifications, requirements and activities of Participants when transacting message content with other Participants
  - Support of the Participants who wish to transact message content with other Participants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

# 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.

# 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.



# 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.

# Enforcement

- Participants are expected to monitor their use of eHealth Exchange and take all necessary actions to protect the network
- Coordinating Committee has the authority to suspend a Participant's use of eHealth Exchange
  - Immediate threat to the Network
  - Irreparable harm to another party
- Coordinating Committee has the authority to terminate a Participant's use of the Network
  - Failure to correct after suspension
  - Material breach of DURSA that is not cured within 30 days

# Dispute Resolution

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



Informal  
Conference  
between the  
Participants  
involved in  
the dispute

If not resolved  
through the Informal  
Conference, the  
Dispute Resolution  
Subcommittee hears  
the dispute and is  
encouraged to  
develop an  
appropriate and  
equitable resolution

Coordinating  
Committee can  
review the  
Subcommittee's  
recommendation, if  
requested by any  
Participant involved  
in the dispute, and  
issue its own  
resolution

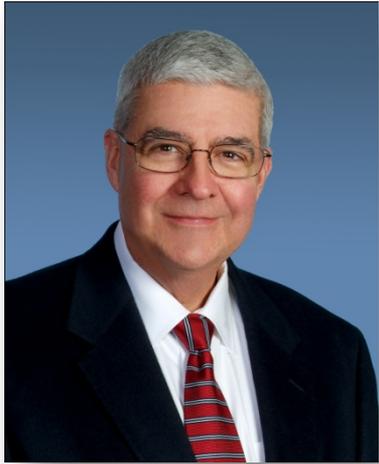
# Questions?

**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.”