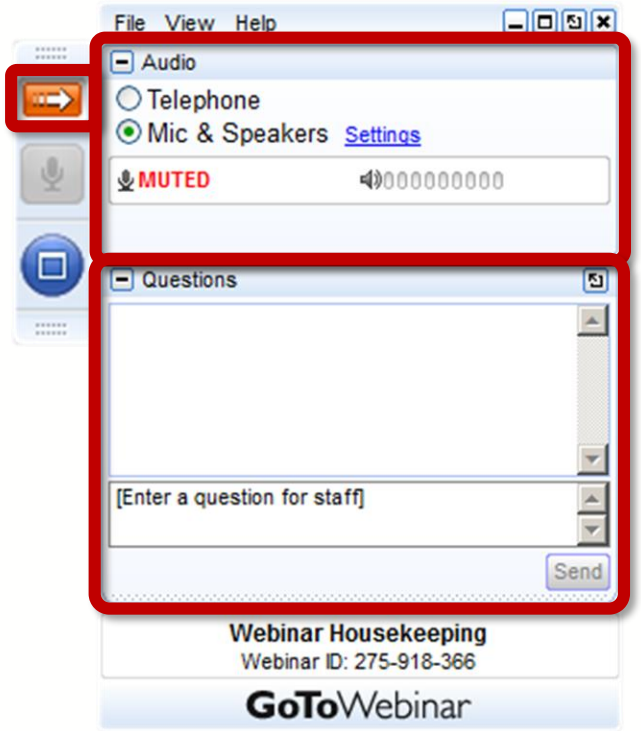
eHealth Exchange™

eHealth Exchange All Participant Call

November 17, 2017

How Do I Participate?



Your Participation

Open and close your control panel

Join audio:

- Choose "Mic & Speakers" to use VoIP
- Choose "Telephone" and dial using the information provided

Submit questions and comments via the Questions panel

Note: Today's presentation is being recorded and will be provided within 48 hrs

Problems or Questions? Contact Dawn Van Dyke

dvandyke@sequoiaproject.org or 703.864.4062

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

Agenda

- Overview of New OPP #12: Vendor Participation
- DURSA Amendment Summary
  - Context and DURSA Historical Milestones
  - DURSA Provisions with Proposed Revisions
- Q & A

NEW OPP #12: VENDOR PARTICIPATION

Background

- The eHealth Exchange is primarily composed of federal agencies, large health systems, and health information exchange organizations (HIOs) along with other organizations such as pharmacies and dialysis providers.
- Vendors which provide cloud-based solutions, or other vendor-intermediated models that have the ability to initiate queries on behalf of their healthcare provider customers have shown interest in joining the eHealth Exchange to share data with federal agencies.
- The CC approved this category of Participant with additional eligibility criteria.
- OPP #12 documents a set of additional criteria for Vendor Applicants that want to join the eHealth Exchange.
- Vendor Applicants will be required to attest to the additional criteria as part of the application process.

Eligibility Requirements for Vendors that will initiate queries on behalf of its Customers (1)

- The Vendor Applicant agrees to facilitate exchange solely as an agent of its covered entity healthcare provider or health plan Customer. This means that the Vendor Applicant may use the interoperability available through the eHealth Exchange only to transmit or receive information on behalf of its Customers and not on its own behalf. The Vendor Applicant does not have rights to, and shall not, for its own benefit, re-use, re-disclose, aggregate, de-identify or sell any information transmitted or received by its Customers through the eHealth Exchange. The Vendor Applicant will not use the data being exchanged through its system for any purpose other than serving its Customers unless its respective Customers have given the Vendor Applicant he explicit written authority to do so.
- The Vendor Applicant shall have entered into a HIPAA compliant Business Associate Agreement with its Customers.
- The Vendor Applicant agrees that it may store data transacted via eHealth Exchange solely for the purpose of serving its Customers. Specific examples of acceptable reasons that a vendor would store data include: saving the data temporarily for the purpose of transforming the data; aggregate the data for the purpose of creating a longitudinal record; or retain data for specified period of time to support the operational service for its Customer (e.g. for auditing purposes, or authorization/consent tracking).

Eligibility Requirements for Vendors that will initiate queries on behalf of its Customers (2)

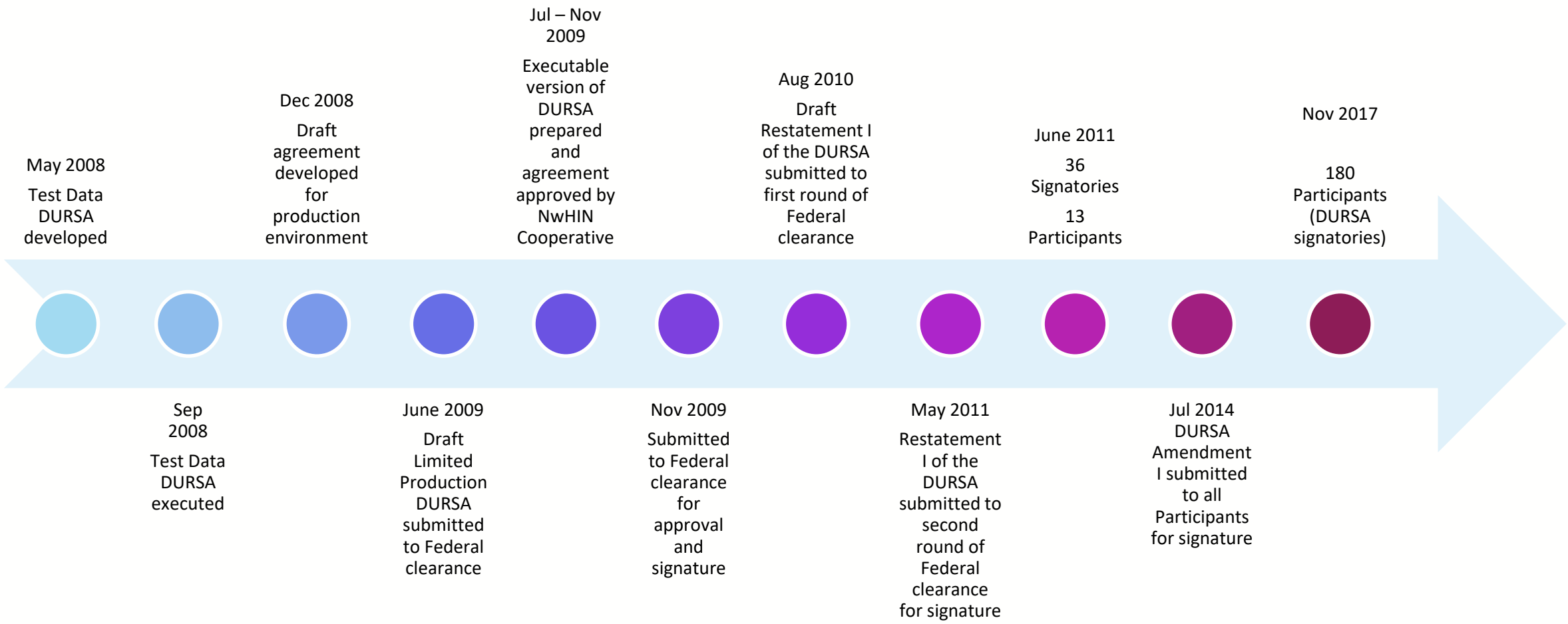
- The Vendor Applicant agrees that it has the ability to terminate its Customers' access to the eHealth Exchange if requested by the CC or if the Customer presents a risk to the privacy or security of information transacted with other eHealth Exchange Applicant s or the security of the eHealth Exchange network.
- The Vendor Applicant agrees that it has formal contractual mechanisms in place with its Customers that authorize the vendor Applicant to initiate and respond to requests on behalf of its healthcare provider or health plan customers through the eHealth Exchange. The Vendor Applicant will provide representative samples of the contractual mechanisms to the CC upon request.
- The Vendor Applicant attests that it has established mechanisms to assure that it can effectively flow down the DURSA requirements to its Customers and that its Customers are aware of and understand the Vendor Applicant's obligations under the DURSA (e.g. how patient / member information may be used and exchanged, the Vendor Participant's accountability to its Customers, etc.)
- The Vendor Applicant shall identify and attest that every Customer exchanging health information via the eHealth Exchange is legally obligated to comply with the DURSA flow-down provisions.
- The Vendor Applicant has the organizational structure, resources, governance mechanisms and resources to govern this activity and to fulfill its responsibilities in the DURSA.

OPP#12 Formal Change Process Milestones

Approval Milestones	Target Dates
Present to CC for Review (Draft):	10/17/17 – Complete
Participant Input (Webinar to review updates):	11/17/17
CC Approval:	11/21/17
Participant Input (Post draft to eHealth Exchange Wiki):	11/21/17
30 day notice to participants:	11/22/17
Objection Period Ends:	12/22/17
Target Effective Date:	12/23/17

DURSA AMENDMENT SUMMARY

DURSA Historical Milestones



Developed by Troutman Sanders

Why are we Amending the DURSA?

- The Coordinating Committee (CC) has been exploring the requirements for the eHealth Exchange to become a Carequality Implementer
- A policy review determined that a DURSA Amendment is necessary to pursue becoming and Carequality Implementer
- In addition, the DURSA has been in effect since 2010 additional updates are necessary to align the network with the current market (i.e. expanded permitted purposes to support new use cases).
- Changes to the DURSA must be done in accordance with the DURSA Amendment Process detailed in OPP #8.

Proposed Changes cover the following DURSA Provisions

- Definition of Participant
- Permitted Purposes
- Coordinating Committee
- Minimum Participation Requirements
- Duties When Submitting a Message
- Auditing and Monitoring
- Privacy and Security
- Data Breach Notification
- Third Party Technology
- Liability

PROPOSED DURSA REVISIONS

Definition of Participant

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Whereas, the Participants are: (i) organizations that oversee and conduct, on their own behalf and/or on behalf of their Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations (ii) federal, state, tribal or local governments, agencies or instrumentalities; (iii) program activities or initiatives that are involved in healthcare in any capacity Definition: Participant shall mean any (i) organization that (a) meets the requirements for participation as contained in the Operating Policies and Procedures; (b) is provided with Digital Credentials; and (c) is a signatory to this Agreement or a Joinder Agreement.	(ii) federal, state, tribal or local governments, agencies or instrumentalities; (iii) program activities or initiatives that are involved in healthcare in any capacity Participant shall mean any (i) organization (ii) federal, state, territorial or local government, agency or instrumentalities or (iii) program activities or initiatives that are involved in healthcare in any capacity that (a) meets the requirements for participation as contained in the Operating Policies and Procedures; (b) is provided with Digital Credentials; and (c) is a signatory to this Agreement or a Joinder Agreement.

Permitted Purposes

DURSA	DURSA Amendment
Section 5 provides that Participants can Transact Message Content for a Permitted Purpose. Permitted Purpose is defined and as of today includes: • Treatment of individual who is the subject of the message • Payment activities of health care provider of individual who is the subject of the message • Health Care Operations of a Submitter of Message Content if the Submitter is a HIPAA Covered Entity • Health Care Operations of a Covered Entity if a Submitter is Transacting Message Content on behalf of the Covered Entity • Health Care Operations of a Recipient if (i) the Recipient is a health care provider and (ii) purpose of transaction is for Health Care Operations listed in 45 CFR 164.501 paragraphs (1) or (2) or (iii) health care fraud and abuse detection or compliance of the health care provider. • Public health activities and reporting as permitted by Applicable Law • Any purpose to demonstrate Meaningful Use of certified EHR technology • Uses and disclosures pursuant to a HIPAA Authorization Future Use – Participant may retain, use and re-disclose Message Content as permitted by Applicable Law and its own policies The CC may request Message Content from a Participant in order to do its job and Participant must provide it. • Participant is not required to disclose PHI • Participant must label all information Confidential	1. Treatment of individual who is the subject of the message 2. Payment as defined by HIPAA 3. Transaction of Message Content related to value based payment models, alternative payment arrangements or financial risk sharing models of any nature whether for Medicare, Medicaid, other federal programs, commercial payers or employer self-insured arrangements. This could include, but is not limited to, Accountable Care Organizations, Medicare Incentive Payments, Clinically Integrated Networks, Managed Care Organizations or Bundled Payments; 4. Health Care Operations as defined by HIPAA; 5. Transaction of Message Content for certain specialized government functions which are necessary to fulfill an agencies statutory obligations for programs the agency administers including, but not limited to: activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission; or, for the purpose of the Department of Veterans Affairs determining the individual's eligibility or entitlement to benefits under the VA upon separation or discharge of the individual from military service; or, to determine eligibility for or entitlement to or provision of other government benefits; or, for activities related to eligibility for or enrollment in a health plan that is a government program; or, for administering a government program providing public benefits, to coordinate covered functions or to improve administration and management relating to the covered functions of such government programs; 6. Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e); 7. Transaction of Message Content in support of an individual's: (i) right to access their health information, or; (ii) right to direct with whom their information can be shared or where their information should be sent. 8. Uses and disclosures pursuant to a HIPAA Authorization

Coordinating Committee

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Section 4.03 is the Grant of Authority to the CC which is to "provide oversight, facilitation and support to Participants Transacting Message Content with other Participants" • Section 4.03 lists specific activities the CC is authorized to do, but this list is not exclusive • Grant of authority to CC by Participants is unconditional unless prohibited by law • CC may delegate authority to CC Chairperson or a subcommittee • Delegation of authority to other than the Chairperson or a subcommittee shall be done via adoption of an Operating Policy and Procedure (OPP)	Additional items: • Evaluating requests for and approving new Use Cases; • Enter into agreements to broaden access to data to enhance connectivity across platforms and networks as provided in accordance with Operating Policies and Procedures; and • Section 4.05 Members of the Coordinating Committee shall carry out their duties in a diligent and responsible manner as more specifically identified in an applicable Operating Policy and Procedure.

Minimum Participation Requirement

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Sec. 12.01 – Participants that request, or allow their Participant Users, to request data for Treatment must respond to other Participant's requests for Treatment.	Added the term Use Case: • Use Case shall mean a particular activity involving Transacting Message Content using the Network in order to support a specific function or facilitate an identified outcome. • All Participants that choose to participate in a specific Use Case must fully participate in that Use Case. This means that a Participant must comply with all of the Performance and Service Specifications for a Use Case and must take measures to require that its Participant Users comply with all of the Performance and Service Specifications for a Use Case. By way of example only and not to limit the applicability of the foregoing, for the Query/Retrieve Use Case, all Participants that request, or allow their respective Participant Users to request, Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that request Message Content for Treatment. A Participant shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or, (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged. • Each Participant that chooses to participate in a Use Case shall Transact Message Content with all other Participants which are participating in that Use Case

Specific Duties of a Participant When Submitting a Message

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Section 13 Submitting a copy of the authorization	• Provide evidence that the Submitter has obtained an Authorization or other evidence of an individual directed transaction if the Submitter is requesting Message Content from another Participant or Participant User based on the Permitted Purpose described in Sections 1(jj)(7) or (8). Nothing in this Section shall be interpreted as requiring a Submitter who is requesting Message Content to obtain or transmit an Authorization for a request based on a Permitted Purpose other than the one described in Section 1(jj)(8), even though certain other Participants or Participant Users require such Authorization to comply with Applicable Law.

Auditing

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Auditing and Monitoring • Each Participant represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to this Agreement, for system administration, security, and other legitimate purposes. Each Participant shall perform those auditing activities required by the Performance and Service Specifications.	Additional language added • eHealth Exchange, acting through its agents and independent contractors, in order to confirm compliance with this Agreement, shall have the right, but not the obligation, to monitor and audit Network exchange activities. Participant agrees to cooperate with eHealth Exchange in these monitoring and auditing activities to the extent that it is permitted to by Applicable Law and to provide, upon the reasonable request of eHealth Exchange, information in the furtherance of eHealth Exchange's monitoring and auditing including, but not limited to, audit logs of exchange transactions and summary reports of exchange activities, to the extent that Applicant possesses such information. Note to reviewers: We have revised this section to make it conform to the language used in the Carequality Connected Agreement which reflects more recent thinking about the need for Networks like eHealth Exchange to be able to audit and monitor its Participants.

Privacy and Security

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Section 14.01 Applicability of HIPAA Regulations. Message Content may contain PHI. Furthermore, some, but not all, Participants are either a Covered Entity or a Business Associate. Because the Participants are limited to Transacting Message Content for only a Permitted Purpose, the Participants do not intend to become each other's Business Associate by virtue of signing this Agreement or Transacting Message Content. As a result, the DURSA is not intended to serve as a Business Associate Agreement among the Participants	New Section 14.02 • Business Associate Agreement. In the event that a particular Use Case involves the Transaction of Message Content among Participants, or their Participant Users, that result in any Participant, or Participant User, being considered a Business Associate under the HIPAA Regulations, then the Participants agree that they will enter into a Business Associate Agreement in substantially the form included in Attachment 8. Compliance with this section's requirements may be satisfied by an existing business associate agreement that includes, at a minimum, the terms listed in Attachment 8, by adopting a Business Associate Addendum, in substantially the form included in Attachment 8, to an existing agreement or by adopting a new Business Associate Agreement in substantially the form included in Attachment 8. *NOTE: Given the expansion of the definition of Permitted Purposes, we expect that for some Use Cases it will be necessary for Participants to have a Business Associate Agreement with each other. Therefore, we have deleted this language which specifically disavows a business associate relationship. We have inserted a new section to address situations in which a business associate agreement is required.*

Data Breach Notification

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
The DURSA defines a Breach very narrowly to only include unauthorized access, use or disclosure of Message Content while it is being transacted. Sec. 14.03 requires a Participant to notify the CC (and any other Participants whose information might have been affected) within one hour of discovering information that causes reasonable belief that a Breach may have occurred. If a Participant determines that a Breach has occurred, it must provide written notice to the CC (and any other Participants likely impacted) not later than 24 hours after making this determination of the Breach. The DURSA specifies the required notice content.	Changed the term 'Breach' to Adverse Security Event and clarified the definition. Adverse Security Event shall mean the attempted or successful acquisition, access, disclosure, or use of unencrypted Message Content while in the process of being transacted in a manner permitted by this Agreement by anyone who is not a Participant User or by a Participant User in any manner that is not a Permitted Purpose under this Agreement. As soon as reasonably practicable, but no later than five (5) business days after determining that an Adverse Security Event (or "Event") has occurred and is likely to have an adverse impact on the Network or another Participant; Participant shall provide a notification to the Coordinating Committee and all Participants that are likely impacted by the Event. Participant shall supplement the information contained in the notification as it becomes available and cooperate with other Participants. Notwithstanding the foregoing, Participant agrees that (a) within one (1) hour of learning that an Adverse Security Event occurred and that such Event may involve a Federal Participant, it shall alert the Federal Participant in accordance with the procedures and contacts provided by such Federal Participant, and (b) that within twenty-four (24) hours after determining that an Adverse Security Event has occurred and is likely to have an adverse impact on a Federal Participant(s), Participant shall provide a notification to all such Participants that are likely impacted by the Event, and the Coordinating Committee, in accordance with the procedures and contacts provided by such Federal Participant *NOTE: We have revised this section to conform it to the approach followed in the Carequality Connected Agreement. Most notably, Participants have a longer amount of time to report incidents if no federal government Participants are involved. We are retaining the 1-hour and 24-hour reporting requirements for incidents involving all federal government Participants.*

Third Party Technology

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
N/A	New Section 17.05 • Third Party Technology. All Participants acknowledge that other Participants use technology solutions, applications, interfaces, software, platforms, clearinghouses and other IT resources that are provided by third parties (Third Party Technology). Each Participant shall have agreements in place that require Third Party Technology vendors to provide reliable, stable and secure services to the Participant. However, all Participants acknowledge that Third Party Technology may be non-functional or not available at times and that this could prevent a Participant from Transacting Message Content. Participants do not make any representations or warranties as to their Third Party Technology.

Liability

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT REVISIONS
Sec. 18.01 - Each Participant is responsible for their own acts or omissions. A Participant is responsible for harm caused to another Participant by an individual who Transacts Message Content through the Participant, if that Participant was negligent or breached the DURSA by providing the individual with access. But this liability is only to the extent that the Participant can be sued under Applicable Law.	Participant Liability. As between Participants to this Agreement: Each Participant shall be responsible for its acts and omissions and not for the acts or omissions of any other Participant. In circumstances involving harm to other Participants caused by the acts or omissions of individuals who: (i) Transact Message Content or Confidential Participant Information through the Participant; (ii) improperly and without permission access a Participant's system whether directly or indirectly, lawfully or unlawfully; or, (iii) use the digital credentials of a Participant or Participant User to access Message Content or Confidential Participant Information

DURSA Amendment Key Milestones – Update (1)

Milestones	Target Date
Identify revisions needed to address known issues and discuss initial draft language	Jun 14 - Completed
Discuss DURSA Amendment process with the CC	Jun 20 - Completed
Review draft DURSA Amendment with limited stakeholder group	Jul-Nov - In Process
Present DURSA Amendment Summary to Participants	Nov
Sequoia legal counsel prepares revised draft based on stakeholder feedback	Nov / Dec
Present DURSA Amendment to the CC for review and approval for distribution to Participants for review and approval	Dec 21

DURSA Change Management Milestones – Update (2)

Milestones	Target Date
Participant Input (Post draft to eHealth Exchange Wiki)	Dec 22
Participant Input (Webinar to review)	Jan 12
Official Notice of DURSA Amendment • Voting Period (At least 2/3 Federal and 2/3 Non-Federal Participants must approve) • Submit Revised DURSA Amendment for Federal and Non-Federal Participant Signature	Jan 17
Target Effective Date • All Participants must execute the Amendment before the Target Effective Date to remain a participant.	Apr 1