

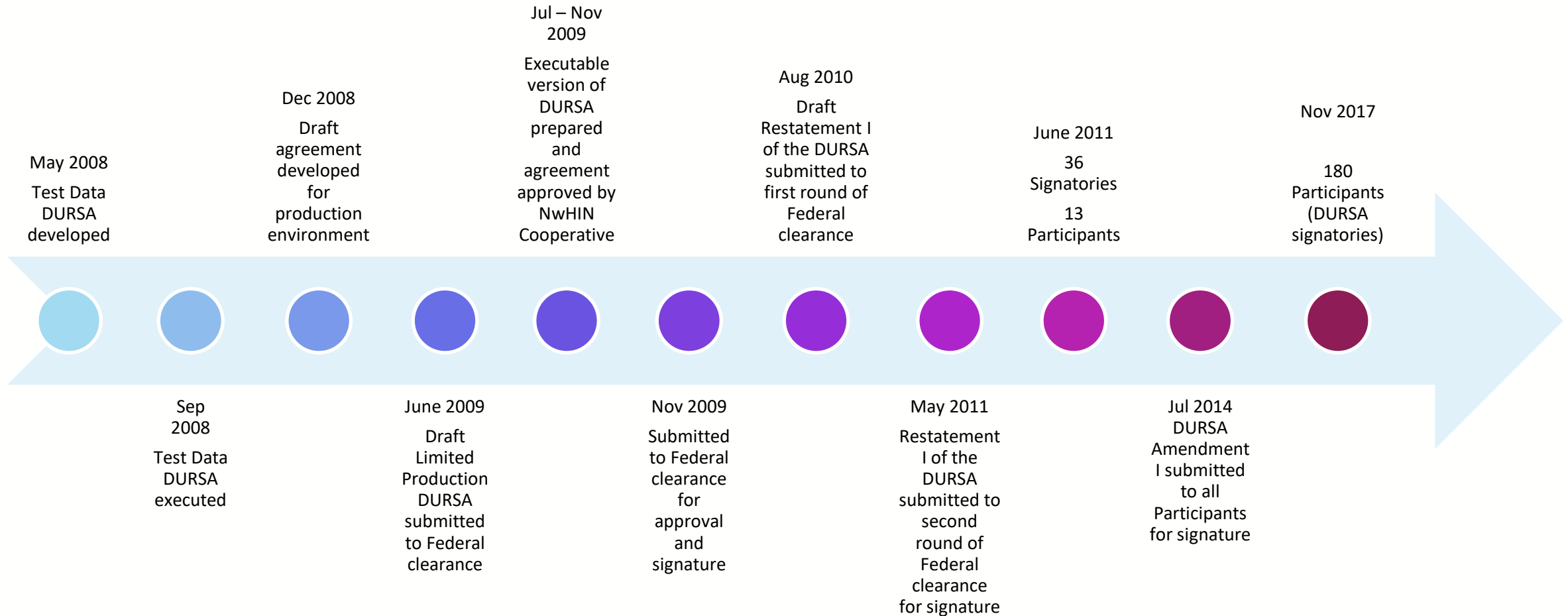


DURSA Amendment Summary

(Updated to reflect Approved Draft DURSA Amendment)

May 15, 2018

DURSA Historical Milestones



Developed by Troutman Sanders

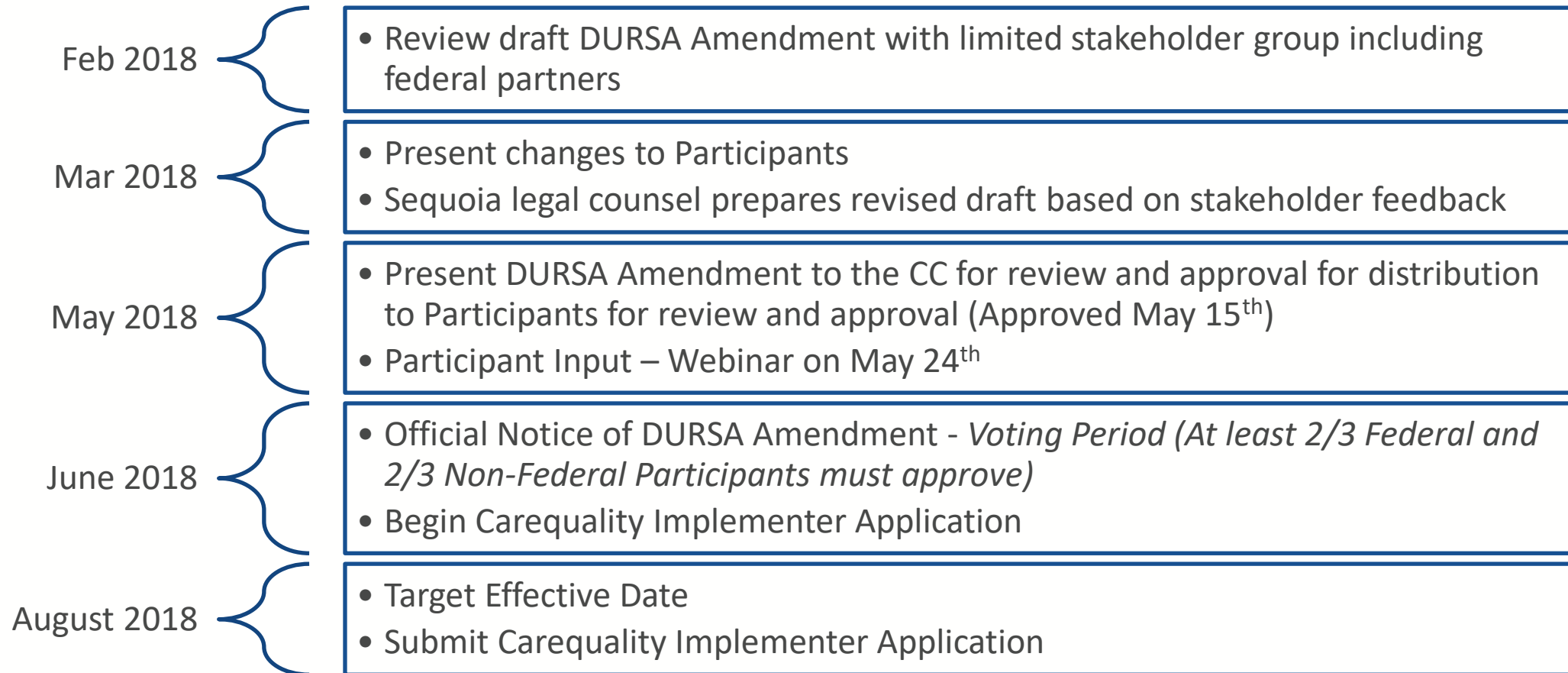
Why are we Amending the DURSA?

- 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

DURSA Amendment Formal Change Control Milestones



PROPOSED DURSA AMENDMENT

Changes since March 2018

- One minor change to Section 1: Definitions since the March 23, 2018 (SLIDES 11 & 12)
 - **Previous definition:**
 - *Treatment was previously defined as Treatment of individual who is the subject of the message*
 - *Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.*
 - **Updated definition:**
 - *Treatment, Payment, Health Care Operations, and Authorization Based Disclosures as defined by HIPAA*

DURSA Amendment Overview

- The following slides will provide a **high level summary** of the proposed DURSA Amendment. This summary is meant to provide a quick review of the major changes. The redline draft DURSA Amendment includes ALL proposed changes and will be distributed to Participants.
- The Draft DURSA Amendment includes changes to the following DURSA sections:
 - Section 1: Definitions
 - Section 4: Coordinating Committee
 - Section 9: Monitoring and Auditing
 - Section 12: Expectations of Participants
 - Section 13: Specific Duties of a Participant When Submitting a Message
 - Section 14: Privacy and Security (Applicability of HIPAA Regulations)
 - Section 14: Privacy and Security (Breach Notification)
 - Section 17: Disclaimers (Third Party Technology)
 - Section 18: Liability (Participant Liability)

Section 1 – New and Deleted Definitions

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>o. Emergent Specifications shall mean the technical specifications that a group of existing and/or potential Participants are prepared to implement to test the feasibility of the specifications, to identify whether the specifications reflect an appropriate capability for the Participants, and assess whether the specifications are sufficiently mature to add as a production capability that is available to the Participants.</p> <p>x. Network shall mean all of the standards, services and policies identified by ONC that enables secure health information exchange over the Internet. As of December 2010, the group of ONC identified standards, services and policies is called the Nationwide Health Information</p> <p>ss. Transaction Pattern shall mean a type of information exchange service(s) enabled by the Specifications. The Operating Policies and Procedures will identify the Transaction Pattern(s) and the Specifications required to implement each Transaction Pattern. As of December 2010, the Transaction Patterns are submission, query and respond, publish and subscribe, and routing. The Transaction Patterns may be amended from time to time through amendment of the Specifications and the Operating Policies and Procedures.</p>	<p>a. Applicant means anyone that submits an application to become an eHealth Exchange Participant.</p> <p>m. eHealth Exchange shall mean the data sharing network which was developed under the auspices of the Office of the National Coordinator for Health Information Technology and consists of governmental and non-governmental exchange partners who share information under a multi-purpose set of standards and services which are designed to support a broad range of information exchange activities using various technical platforms and solutions</p> <p>n. Deleted Emergent Specifications</p> <p>y. Network shall mean the eHealth Exchange.</p> <p>z. Network Utilities shall mean any shared infrastructure used to facilitate the transmission of Message Content for the Network including, but not limited to, gateway services, healthcare directory, master patient indices, record locator services.</p> <p>uu. Transaction Pattern shall mean a type of information exchange service(s) enabled by the Specifications. The Validation Plan will identify the Transaction Pattern(s) and the Specifications required to implement each Transaction Pattern. The Transaction Patterns may be amended from time to time through amendment of the Specifications and the Operating Policies and Procedures.</p> <p>vv. 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.</p>

Section 1 - Expanded Definition of Participant

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>Definition of Participant</p> <p>e. 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.</p>	<p>g. Participant shall mean any (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 that need to exchange health information with others as part of their official function; (iii) organizations that support program activities or initiatives that are involved in healthcare in any capacity and have the technical ability to meet the applicable Performance and Service Specifications to electronically transact health information on their own behalf or on behalf of their Participant Users; have the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require their Participant Users to comply with applicable requirements in this Agreement</p>

Section 1 - Updated Definition of Breach

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>Definition of Breach</p> <p>c. Breach shall mean the unauthorized acquisition, access, disclosure, or use of Message Content while Transacting such Message Content pursuant to this Agreement. The term “Breach” does not include the following:</p> <ul style="list-style-type: none">(i) 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—<ul style="list-style-type: none">(I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and(II) such Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or(ii) any acquisition, access, disclosure or use of information contained in or available through the Participant’s System where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.	<p>Renamed Breach to Adverse Security Event</p> <p>d. Adverse Security Event shall mean the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content in the process of being transacted in a manner permitted by this Agreement by anyone who is not a Participant or Participant User or by a Participant or Participant User in any manner that is not a Permitted Purpose under this Agreement. For the avoidance of doubt, an “Adverse Security Event” under this Agreement does not include the following:</p> <ul style="list-style-type: none">(i) 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—<ul style="list-style-type: none">(I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and(II) such Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or(ii) any acquisition, access, disclosure or use of information contained in or available through the Participant’s System where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.

Section 1 - Expanded Definition of Permitted Purpose

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<ol style="list-style-type: none"> 1. Treatment of individual who is the subject of the message 2. Payment activities of the Health Care Provider for the individual who is the subject of the Message which includes, but is not limited to, Transacting Message Content in response to or to support a claim for reimbursement submitted by a Health Care Provider to a Health Plan. 3. Health Care Operations of either <ol style="list-style-type: none"> .01. the Submitter if the Submitter is a Covered Entity; .02. a Covered Entity if the Submitter is Transacting Message Content on behalf of such Covered Entity; or .03. the Recipient if (i) the Recipient is a Health Care Provider who has an established Treatment relationship with the individual who is the subject of the Message or the Recipient is Transacting Message Content on behalf of such Health Care Provider; and (ii) the purpose of the Transaction is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance of such Health Care Provider; 4. 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); 	<ol style="list-style-type: none"> 1. Treatment, Payment, Health Care Operations, and Authorization Based Disclosures as defined by HIPAA; of individual who is the subject of the message(Note that this was updated since the March 23 DURSA Webinar) 2. Payment as defined by HIPAA 2. 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, participation in Medicare bundled payments, the Medicare Shared Savings Program, other Medicare Alternate Payment programs, Medicaid Managed Care programs or commercial value-based payment programs 3. Health Care Operations as defined by HIPAA; 3. Transaction of Message Content for certain specialized government functions which are necessary to fulfill an agency's statutory obligations for programs the agency administers including, but not limited to : (i) activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission; (ii) 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; (iii) to determine eligibility for or entitlement to or provision of other government benefits; (iv) for activities related to eligibility for or enrollment in a health plan that is a government program; (v) for administering a government program providing public benefits, to coordinate covered functions; or, (vi) to improve administration and management relating to the covered functions of such government programs; 4. 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);

Section 1 - Expanded Definition of Permitted Purpose (2)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-4 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. “Meaningful use of certified electronic health record technology” shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and</p> <p>6. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual’s personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.</p>	<p>5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-46 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA Regulations. “Meaningful use of certified electronic health record technology” shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and</p> <p>6. 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. For the avoidance of doubt, a Participant may be prevented from disclosing information due to Applicable Law even though the individual asserts this Permitted Purpose;</p> <p>7. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual’s personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.</p>

Section 4 - Coordinating Committee

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>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”</p> <p>Section 4.03 lists specific activities the CC is authorized to do</p>	<ul style="list-style-type: none">• Evaluating requests for and approving new Use Cases;• Approving the type, source and use of Network Utilities.• Deleted Evaluating requests for the introduction of Emergent Specifications into the production environment used by the Participants to Transact Message Content;• Entering into agreements to broaden access to data to enhance connectivity across platforms and networks as provided in accordance with Operating Policies and Procedures which shall include an express opt-out right for every Participant;• 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.

Section 9 – Monitoring and Auditing

CURRENT DURSA (9/30/14)

Auditing

- 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.

PROPOSED DURSA AMENDMENT

Renamed to **Monitoring** and Auditing with 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. Unless prohibited by Applicable Law or, in the case of a Governmental Participant that Participant's policies or internal guidelines that it has adopted in the normal course of business, Participant agrees to cooperate with eHealth Exchange in these monitoring and auditing activities 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 Participant possesses such information.** 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.

Section 12 – Expectations of Participants

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>Sec. 12.01 Minimum Requirement for Participants that request Message Content for Treatment.</p> <p>Participants that request, or allow their Participant Users, to request data for Treatment must respond to other Participant’s requests for Treatment.</p> <p>a. 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. All responses to Messages shall comply with Performance and Service Specifications, this Agreement, any agreements between Participants and their Participant Users, and Applicable Law. Participants may, but are not required to, Transact Message Content for a Permitted Purpose other than Treatment. Nothing in this Section 12.01(a) shall require a disclosure that is contrary to a restriction placed on the Message Content by a patient pursuant to Applicable Law.</p> <p>12.02. Participant Users and HSPs</p>	<p>Added additional language.</p> <p>12.01. eHealth Exchange exists to promote the seamless exchange of health information across a variety of technical platforms and Health Information Networks. A core principle of eHealth Exchange is that Participants make commitments to the minimum level of data sharing that they will support so that all other Participants can know, and rely on, each Participant’s commitment. All Participants that choose to participate in a specific Use Case 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.</p> <p>12.01b – Changed Breach to Adverse Security Event</p> <p>12.02 – Changed HSPs to Technology Partners</p> <p>Added new provisions:</p> <p>12.04. Network Utilities. The Coordinating Committee may approve the use of various Network Utilities to support the operation of the Network. If necessary, the Coordinating Committee may develop an Operating Policy and Procedure for implementation and use of the Network Utility by Participants. The Network Performance and Service Specifications may be updated as needed to effectively implement a Network Utility. The procedures outlined in sections 10.03 and 11.03 of this Agreement shall be followed in developing or updating Operating Policies and Procedures or Performance and Service Specifications.</p>

Section 12 – Expectations of Participants

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
<p>Sec. 12.01 Minimum Requirement for Participants that request Message Content for Treatment.</p>	<p>Added additional provisions.</p> <p>12.05. Opt-out for new networks. If the Coordinating Committee exercises its authority, provided to it by section 4.03(m) of this Agreement, to enter into agreements to broaden access to data to enhance connectivity across platforms and networks, the Participant may choose to opt-out of participation in those platforms or networks in the event that the Participant determines that the relevant terms, conditions, policies or procedures of the platform or network include requirements that mean that the Participant would be in violation of Applicable Law or would be required to violate its own duly adopted internal policies or guidance if Participant complies with the platform or network terms, conditions, policies or procedures. Participant shall provide the Coordinating Committee with a written explanation of the basis for its decision to opt-out which sets forth the reasons that compliance would result in Participant violating Applicable Law or its internal policies or procedures. If Participant later determines that participation in a platform or network no longer creates a compliance issue, the Participant shall notify the Coordinating Committee that it no longer is opting-out of participation in the platform or network. At any time, a Participant may reverse its decision to opt-out.</p>

Section 13 - Specific Duties of a Participant When Submitting a Message

CURRENT DURSA (9/30/14)

Section 13 – Specific Duties when Submitting a Message

13.03. Submitting a copy of the Authorization, if the Submitter is requesting Message Content from another Participant or Participant User based on the Permitted Purpose described in Section 1(jj)(6). 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)(6), even though certain other Participants or Participant Users require such Authorization to comply with Applicable Law.

PROPOSED DURSA AMENDMENT

- 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(jkk)(8) or (9). 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(kk)(9), even though certain other Participants or Participant Users require such Authorization to comply with Applicable Law.

Section 14 - Privacy and Security (Applicability of HIPAA Regulations)

CURRENT DURSA (9/30/14)

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

PROPOSED DURSA AMENDMENT

New Section 14.02

- **Business Associate Agreement.** Some Use Cases will involve the Transaction of Message Content among Participants, or their Participant Users, that result in a Participant, or Participant User, being considered a Business Associate under the HIPAA Regulations. While this will not be the general rule, when it does occur, 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 below to address situations in which a business associate agreement is required.

Section 14 – Privacy and Security (Breach Notification)

CURRENT DURSA (9/30/14)

The DURSA defines a Breach very narrowly to only include unauthorized access, use or disclosure of Message Content while it is being transacted.

14.03 a. Each Participant agrees that within one (1) hour of discovering information that leads the Participant to reasonably believe that a Breach may have occurred, it shall alert other Participants whose Message Content may have been Breached and the Coordinating Committee to such information. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach has occurred, the Participant shall provide a Notification to all Participants likely impacted by the Breach and the Coordinating Committee of such Breach.

PROPOSED DURSA AMENDMENT

Changed the term 'Breach' to Adverse Security Event and clarified the definition.

14.04 a. 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.

Section 17 - Disclaimers (Third Party Technology)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT
N/A	<p data-bbox="1302 476 1528 501">New Section 17.05</p> <ul data-bbox="1302 511 2407 819" style="list-style-type: none"><li data-bbox="1302 511 2407 819">• 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.

Section 18 – Liability (Participant Liability)

CURRENT DURSA (9/30/14)

Sec. 18.01 – 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 Transact Message Content or Confidential Participant Information through the Participant or by use of any password, identifier, or log-on received or obtained directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant Users, each Participant shall be responsible for such harm to the extent that the individual's access was caused by the Participant's breach of the Agreement or its negligent conduct for which there is a civil remedy under Applicable Law. Notwithstanding any provision in this Agreement to the contrary, Participant shall not be liable for any act or omission if a cause of action for such act or omission is otherwise prohibited by Applicable Law. This section shall not be construed as a hold harmless or indemnification provision.

PROPOSED DURSA AMENDMENT

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**, each Participant shall be responsible for such harm to the extent that the individual's access was caused by the Participant's breach of the Agreement or its negligent conduct for which there is a civil remedy under Applicable Law. Notwithstanding any provision in this Agreement to the contrary, Participant shall not be liable for any act or omission if a cause of action for such act or omission is otherwise prohibited by Applicable Law. This section shall not be construed as a hold harmless or indemnification provision.

Q & A

For more information:

Website: <http://www.ehealthexchange.com>

E-mail: administrator@ehealthexchange.com