eHealth Exchange™

DURSA Reference Packet

September 4, 2019

Relevant background information

- We have been working on a comprehensive amendment to the DURSA since 2017 to keep up with changes in how health information is exchanged and used.

- In May 2018, the Coordinating Committee approved a revised DURSA but we could not move forward with eHealth Exchange Participant approval because of issues surrounding Controlled Unclassified Information (CUI).

- Since then, we have worked diligently with the federal partners and the Coordinating Committee to work through the complex issues related to CUI.

Coordinating Committee Recommendation

- We worked out a suitable approach for CUI that is acceptable to our federal Participants which are reflected in the currently revised DURSA and a new Operating Policy and Procedure

- On August 13, 2019, the Coordinating Committee **recommended** Participants **approve** the August 2019 draft amended DURSA.

- The Coordinating Committee believes amending the DURSA now will position the eHealth Exchange as a stronger network.

Copies of the Proposed Amended DURSA

The current version of the DURSA, the proposed amended DURSA (redlined), and the proposed amended DURSA (clean, executable version) are all available at https://ehealthexchange.org/onboarding/dursa

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. The amended DURSA authorizes the Coordinating Committee to enter into new network sharing agreements with organization such as Carequality when appropriate.
- Adjustments are necessary to align our network with the current market (i.e. expanded Permitted Purposes to support new use cases) given that the DURSA hasn't been changed in 8+ years.
- Changes to the DURSA must be accomplished 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

Foreseeable Impacts

- Once the DURSA is amended, the Coordinating Committee may move forward with signing the Carequality data sharing agreement providing Participants the option, if they do not already have the ability, to connect with Carequality enabled networks.

- Amending the DURSA may also result in more organizations, like “value-based care” organizations becoming eHealth Exchange Participants.

Timeline

- **August 13, 2019**: Coordinating Committee approval

- **Late August 2019**: Coordinating Committee will distribute official notice

  Participants have fifteen (15) calendar days to request 2/1/2020 effective date be postponed based on unforeseen complications or other good cause.

- **September 2019**: Recorded web meetings and other materials provided to educate Participants regarding DURSA changes

- **October 1, 2019 through November 30, 2019**: Participants vote to amend the DURSA

- **December 1, 2019 through January 31, 2020**: All Participants must sign the amendment to the DURSA prior to the effective date of the amendment or terminate their participation (required by the DURSA and Operating Policy and Procedure 3).

- **February 1, 2020**: Target effective date

eHealth Exchange™

DURSA Policy Assumptions

September 4, 2019

DURSA Policy Assumptions

The DURSA is a comprehensive legal agreement used to establish trust for information exchanged among Participants in the eHealth Exchange. This agreement is based upon a set of policy assumptions that bridge varying state and federal laws and regulations, as well as differing local policies. The agreement, while articulated as a contract, underscores a framework for broad-based information exchange among a set of trusted entities who either wish to query and retrieve data or push data to others in the network.

DURSA Policy Assumptions

1. **Shared Rules of the Road and Shared Governance**. Common framework that binds all Participants to a set of technical requirements, testing requirements, policies, governance structure and accountability measures, including a process for adding or changing requirements.

2. **Representative Governance**: Participants are governed by a representative group of Participants who share data in production. Additional methods for obtaining broad community input and engagement (e.g. task groups, outreach, industry collaboration, etc.) shall be supported to assure support and alignment with national policy.

3. **Participants in Production**. Assumes that participants are in production and leverages a participant's existing end user trust agreements, policies and vendor agreements.

DURSA Policy Assumptions

4. **Multiple Exchange Methods and Profiles**. Enables Participants to declare which profiles or use cases they wish to support in production. Supports multiple exchange methods, or "Transaction Patterns", such as: push, query / retrieve and publish/subscribe.

5. **Privacy and Security Obligations.** Defers to Applicable Law and establishes HIPAA as contractual standard of performance for those who are not governmental agencies and not otherwise subject to HIPAA. Highlights specific requirements which represent the most likely risk to the network, related to: system access policies, identification, authentication, enterprise security, malicious software, auditing and monitoring access.

6. **Identification and Authentication.** Each user who shares data as part of the eHealth Exchange shall be uniquely identified and their identity verified prior to granting access to a Participant's system.

DURSA Policy Assumptions

7. **Permitted Purposes.** Permits exchange of information among eHealth Exchange Participants for certain purposes, including: treatment, limited payment and health care operations, public health activities and reporting, any purpose to demonstrate meaningful use, and disclosures based upon an individual's authorization. These purposes may be revisited over time as additional use cases are brought forward.

8. **Future Use of Data Received Through the eHealth Exchange**. Data are received and integrated into end-user's system and may be reused or disclosed as any other information in its records, in accordance with Applicable Law and local record retention policies.

DURSA Policy Assumptions

9. **Local autonomy** - Each Participant shall have Participant Access Policies that establish a Participant's Users are permitted to exchange data using the Participant's system. Each Participant acknowledges that these access policies will differ among them as a result of varying Applicable Law and business practices. A Participant may not discriminate and refuse to share data with another Participant solely on the basis of differing system access privileges. A Participant is not required or permitted to release information in conflict with Applicable Law.

10. **Reciprocal Duty to Respond.** Participants who query data for treatment purposes also have a duty to respond to requests for data for treatment purposes, either with a copy of the data or with a standardized response that data are not available. Participants may respond to requests for other purposes.

DURSA Policy Assumptions

11. **Responsibilities of Party Submitting Data**. Participants who submit data are responsible for submitting the information in compliance with applicable law and representing 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.
12. **Authorizations.** When a request is based on an authorization (e.g. for SSA benefits determination), the requesting Participant must send a copy of the authorization with the request for data.

DURSA Policy Assumptions

13. **Participant Breach Notification**. Participants are required to promptly notify the eHealth Exchange Coordinating Committee and other impacted Participants of breaches related to the eHealth Exchange (i.e. unauthorized acquisition, access, disclosure or use of the data transmitted among participants, which occur while transmitting the data).

14. **Chain of Trust.** A participant's obligations to comply with the DURSA must "flow down" to users or other participating organizations that connect through a Participant's system, as well as the technology partner.

15. **Mandatory Non-Binding Dispute Resolution**. Participants will agree to participate in a mandatory, non-binding dispute resolution process that preserves the Participants' rights to seek redress in the courts if not resolved through the dispute resolution process.

DURSA Policy Assumptions

16. **Allocation of Liability Risk**. Each participant is responsible for their own acts and omissions, but not the acts and omissions of other participants. Participants are responsible for harm caused if they breach the DURSA or if, due to their negligence, there is a breach of data being transmitted.
17. **Representations and Warranties**:
    - Protected Health Information (PHI) may not be used in test data sets used for testing purposes. PHI may not be sent to the Coordinating Committee.
    - Participants represent that the data they transmit is an accurate representation of the data in their system at the time the data are transmitted.

DURSA Policy Assumptions

- Participants warrant that they have the authority to transmit information.
- Participants assert that they are not subject to a final order issued by a court, regulatory or law enforcement organization which materially impacts their ability to fulfill their obligations under the DURSA. In addition, 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. Data transmitted do not include a full and complete medical record or history. In addition, data transmitted are not a substitute for health care providers to obtain whatever information they deem necessary to properly treat patients. Healthcare providers are accountable for treating patients. Participants, by virtue of signing the DURSA, do not assume any role in the care of an individual.

DURSA Policy Assumptions

- Participants are not accountable for failure of carrier lines (e.g. third party carriers for communications, Internet backbone, etc.) 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.

eHealth Exchange™

Proposed DURSA Amendment

September 4, 2019

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	Why Changing
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. 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 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.	a. Applicant means anyone that submits an application to become an eHealth Exchange Participant. 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 n. Deleted Emergent Specifications y. Network shall mean the eHealth Exchange. 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 locater services. 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. 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.	Updated some definitions to reflect how the eHealth Exchange is operating and changes to the external environment.

Section 1 - Expanded Definition of Participant

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
Definition of Participant 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.	g. Participant shall mean any (i) organization that oversees and conducts, on its own behalf and/or on behalf of its 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) organization that supports 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 its own behalf or on behalf of its Participant Users; has the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require its Participant Users to comply with applicable requirements in this Agreement	Expand the types of organizations that are able to join the eHealth Exchange as Participants.

Section 1 - Updated Definition of Breach

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
Definition of Breach 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: (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— (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.	Renamed Breach to Adverse Security Event 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: (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— (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.	The term "breach" is actually a legal conclusion that a HIPAA covered entity, or its business associates make after they investigate the unauthorized access, use or disclosure of PHI. We want to make it clear that not every event is a breach. Hence, the change in terms.

Section 1 - Expanded Definition of Permitted Purpose

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	
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 .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);	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, 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 4. Health Care Operations as defined by HIPAA; 5. 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; 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);	We are expanding the definition of Permitted Purposes to include new exchange opportunities such as value-based care.

Section 1 - Expanded Definition of Permitted Purpose (2)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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	7. 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	
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.	8. 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; 9. 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.	

Section 4 - Coordinating Committee

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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	• 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.	We are giving the CC the authority to approve new Use Cases for the eHealth Exchange to expand the scope of what the Exchange can be used for. We are also allowing the CC to approve new Network Utilities, such as potentially future iterations of the Hub for use in the eHealth Exchange. We are also giving the CC the authority to sign data sharing agreements with other networks.

Section 7 – Enterprise Security

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
Section 7.01 states that Participants are required to comply with Performance and Service Specifications and/or Operating Policies and Procedures related to enterprise security	• Clarified that Performance and Service Specifications and OPPs don't simply define expectations, but also identify requirements.	We wanted the DURSA language to conform to how the CC has always interpreted this issue.

Section 9 – Monitoring and Auditing

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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.	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.	The ability to monitor the new HUB is necessary for cyber-security and system performance.

Section 12 – Expectations of Participants

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	
Sec. 12.01 Minimum Requirement for Participants that request Message Content for Treatment. Participants that request, or allow their Participant Users, to request data for Treatment must respond to other Participant's requests for Treatment. 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. 12.02. Participant Users and HSPs	Added additional language. 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. 12.01b – Changed Breach to Adverse Security Event 12.02 – Changed HSPs to Technology Partners Added new provisions: 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.	These amendments reflect the expanded scope of exchange activity using eHealth Exchange.

Section 12 – Expectations of Participants

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
Sec. 12.01 Minimum Requirement for Participants that request Message Content for Treatment.	Added additional provisions. 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 for any reason. Participant shall provide the Coordinating Committee written notification of its decision to opt-out. At any time, a Participant may reverse its decision to opt-out.	This new section allows an eHealth Exchange Participant to opt-out of new networks that the CC joins .

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

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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.	• 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.	This is mainly a clean-up change.

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

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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. 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 same 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 same form included in Attachment 8, to an existing agreement or by adopting a new Business Associate Agreement in substantially the same 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.*	In some situations, Participants might want to exchange PHI in a way that results in the recipient of PHI be considered a business associate of the sending Participant. For example, a Participant may provide PHI to another Participant so that the recipient Participant can evaluate what community services a patient might qualify for. Available services would be shared with the Participant that provided the PHI to help it properly disposition the patient. This might result in the recipient participant being considered a business associate of the sending Participant. We do not anticipate this being a regular occurrence, but it may happen. We wanted the DURSA to recognize this situation and provide a neutral template BAA for the Participants to use .

Section 14 – Privacy and Security (Breach Notification)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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.	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.*	The short timeframe for reporting a data breach is the number one objection that we hear from new Participants. We are revising this to only require the 1-hour reporting for federal data and allowing a more generous timeline for everyone else.

Section 14 – BAA

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
Section 14.02	• **New section** to support use cases in which one Participant is providing a service to another Participant and has access to PHI. This makes the Participant receiving the PHI a business associate under HIPAA. The DURSA recognizes this situation and provides a template business associate agreement for the Participants to use so that they do not get locked into a disagreement over their respective business associate agreements.	

Section 17 – Disclaimers (Patient Care)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
Section 17.03 states that Message Content is not a substitute for any Participant or Participant User, if that person/entity is a Health Care Provider, obtaining whatever information he/she/it deems necessary, in his/her professional judgment, for the proper treatment of a patient.	• Corrected typo by replacing “through” with “through”	

Section 17 - Disclaimers (Third Party Technology)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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.	We want to be certain that all Participants require their third-party technology vendors to provide reliable, stable and secure services. We think that all Participants already have these in place.

Section 18 – Liability (Participant Liability)

CURRENT DURSA (9/30/14)	PROPOSED DURSA AMENDMENT	Why Changing
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.	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.	Clarify when a Participant is liable to other Participants.

Q & A

For more information:

Website: http://www.ehealthexchange.com

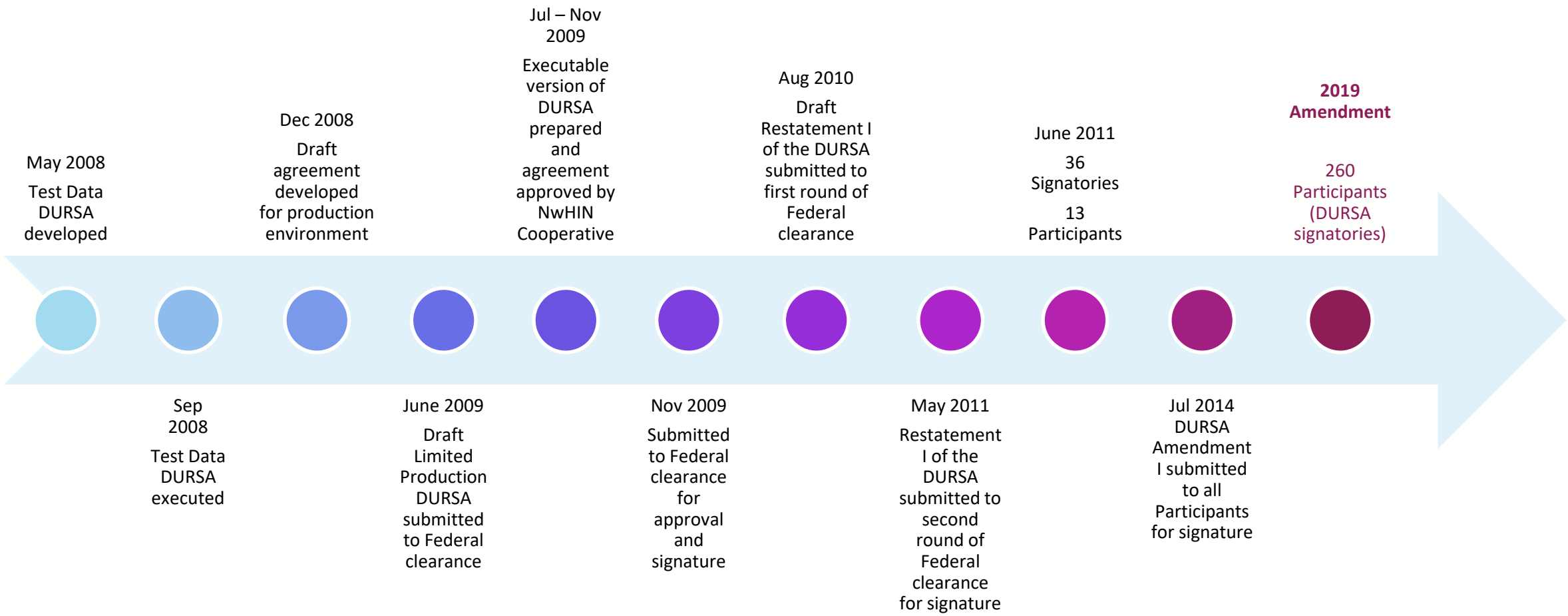
E-mail: administrator@ehealthexchange.com

eHealth Exchange™

Background

September 4, 2019

DURSA Historical Milestones



Developed by Troutman Sanders

Major Amendment Steps (when terms not required by law)

1. Coordinating Committee provides initial amendment review

2. [Optional] Coordinating Committee-appointed Task Group recommends amendment or not

3. Coordinating Committee:
   a. Approves recommending the amendment & seeking approval from Participants to amend DURSA
   b. Specifies timeframe for Participants' vote to approve
   c. Specifies timeframe for subsequent Participant signatures (effective date)

See DURSA section 23.02 & OP&P 8 for additional details and context

4. Coordinating Committee provides Participants:
   a. Recommendation to approve amendment
   b. Copy of proposed amendment
   c. Reasons for the proposed amendment
   d. Foreseeable impacts of the change
   e. Statement regarding whether the proposed amendment is necessary to comply with Law
   f. Projected effective date
   g. Time period for Participants to approve or reject

5. 2/3 of non-governmental Participants plus 2/3 of governmental Participants must vote to approve

6. Coordinating Committee provides Participants notice of approval 30+ days prior to the amendment effective date

7. Coordinating Committee distributes amendment to Participants to execute before the effective date or terminate participation