eHealth Exchange™

Please e-mail questions or concerns to
administrator@ehealthexchange.org

DURSA Policy Assumptions

July 9, 2020

DURSA Policy Assumptions

The Data Use and Reciprocal Support Agreement (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 wish to query and retrieve data or exchange data that is pushed to others in the network or with those in other data sharing networks approved by the Coordinating Committee.

https://ehealthexchange.org/onboarding/dursa

DURSA Policy Assumptions

1. Shared Rules of the Road and Shared Governance. The DURSA codifies a 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 these requirements. The DURSA is the same for EVERY Participant. We do not negotiate one-off changes to the DURSA. The eHealth Exchange may negotiate a few terms in the Participation Agreement and the BAA, but not the DURSA. This assures that the rules are the same for everyone, which is a fundamental component of trust.

As a multi-party agreement, changes cannot be negotiated

DURSA Policy Assumptions

2. **Representative Governance.** Participants are governed by a representative group of Participants, who share data in production, called the Coordinating Committee. The Coordinating Committee has only the authority given to it in the DURSA.

   The 2019 DURSA Restatement expanded the authority of the Coordinating Committee to adopt Network Utilities to make the exchange of Message Content more effective and allowing the Coordinating Committee to join other data sharing networks.

DURSA Policy Assumptions

3. Stakeholder input. Effective governance requires an ability to obtain input from a broad range of organizations that are invested in the success of the eHealth Exchange. The Coordinating Committee is a representative body, but it cannot reasonably be expected to include every stakeholder because there are simply too many of these stakeholders. Therefore, 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.

DURSA Policy Assumptions

4. **Participants in Production**. The DURSA assumes that Participants are in production and leverages a Participant's existing end user agreements, policies, and vendor agreements.

5. **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.

6. **New Networks.** If the Coordinating Committee exercises its authority to enter into agreements to broaden access to data to enhance connectivity across platforms and networks, Participants may choose to opt-out of participation in those platforms or networks for any reason by providing the Coordinating Committee written notification of its decision to opt-out. At any time, a Participant may reverse its decision to opt-out.

DURSA Policy Assumptions

7. Privacy and Security Obligations. Many Participants are HIPAA covered entities or business associates of the Participant's covered entity customers. Other Participants are governmental agencies that are subject to their own legal requirements to protect the privacy and security of health information. For any Participants that are not already subject to HIPAA, or government agencies, the DURSA requires them to comply with HIPAA as a matter of contract. Participants are also subject to other state or federal laws, referred to as Applicable Law. The DURSA does include specific requirements that address areas of high risk to the network related to: system access policies, identification, authentication, enterprise security, malicious software, and auditing and monitoring access.

DURSA Policy Assumptions

8. eHealth Exchange HUB and data privacy and security. The eHealth Exchange HUB enables more efficient exchange of Message Content by eliminating the need for Participants to develop a multiplicity of data connections with other Participants. eHealth Exchange has limited access to Participants' PHI so that it can operate the HUB. This means that the eHealth Exchange is a business associate of each Participant and has entered into a Business Associate Agreement with each Participant.

9. 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.

The eHealth Exchange is a business associate of each Participant

DURSA Policy Assumptions

10. **Permitted Purposes.** Permits the exchange of information among eHealth Exchange Participants for the following purposes:
    - Treatment, Payment and Healthcare Operations as defined by HIPAA;
    - Transaction of Message Content related to innovative payment models, including value-based payment, alternative payment and financial risk-sharing models;
    - Public Health as permitted by Applicable Law including HIPAA;
    - Any purpose to demonstrate the meaningful use of certified EHR technology;
    - Individual right to access their own health information.

11. **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

12. 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 between 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.

13. 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 uniformly-applied standardized response that data are not available. Participants may respond to requests for other purposes.

DURSA Policy Assumptions

14. 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.

15. 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

16. Data Breach Notification. The unauthorized access, use, or disclosure of PHI may be a reportable data breach under the HIPAA Breach Notification Rule. A Breach occurs when there is a likelihood that the PHI can be read because it is unencrypted or because of other circumstances. The DURSA deals with this by talking about Adverse Security Events instead of "breaches," since a reportable breach is really a legal conclusion based on the finding after an investigation. Participants are required to promptly notify the eHealth Exchange Coordinating Committee and other impacted Participants of Adverse Security Events related to the eHealth Exchange (i.e., unauthorized acquisition, access, disclosure, or use of the data transmitted among participants, which occurs while transmitting the data). Federal agencies require a one-hour notification; for non-federal Participants, an Adverse Security Event must be reported within 5 days.

Adverse Security Events are limited to events that occur while Message Content is being transacted (in transit) via eHealth Exchange. Adverse Security Events do not apply to unauthorized acquisition, access, disclosure, or use of Message Content within a Participant's data center

DURSA Policy Assumptions

17. 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.

18. Mandatory, Non-Binding Dispute Resolution. Participants will agree to take part 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.

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.

DURSA Policy Assumptions

19. Allocation of Liability Risk. Each Participant is responsible for its 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.

20. 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 are an accurate representation of the data in their system at the time the data are transmitted.

DURSA Policy Assumptions

20. Representations and Warranties (continued):

- 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 that 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 healthcare 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

20. **Representations and Warranties** (continued):
    - Participants are not accountable for failure of carrier lines (e.g., third party carriers for communications, Internet backbone, etc.) that are beyond the Participant's control. Data are provided "as is" and "as available," without a warranty of their "fitness for a particular purpose."
    - Participants are not liable for erroneous transmissions or loss of service resulting from communication failures by telecommunication service providers or other third parties.

DURSA Policy Assumptions

21. Business Associate Agreement (BAA):

- The BAA template provided in section 14.02 is intended for use in the uncommon event that one Participant becomes the Business Associate of another Participant due to one Participant providing a service to another Participant who provides access to PHI.
- The BAA template reduces the chance Participants get locked into a disagreement regarding use of respective business associate agreements.
- Participants can propose the other Participant agree to change terms, but may not insist upon adding components not required by HIPAA.

The DURSA's BAA template might be used with another, specific Participant, but not with the eHealth Exchange.