eHealth Exchange™

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

# DURSA Highlights

*February 23, 2022*

# DURSA Highlights

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 are 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 Highlights

**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 Highlights

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 Highlights

**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.) are employed to assure support and alignment with national policy.

# DURSA Highlights

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 Highlights

**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 Highlights

**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 is 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 Highlights

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;
    - An Individual's right to access his/her own health information.

11. **Future Use of Data Received Through the eHealth Exchange**. Data are received and integrated into the 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 Highlights

**12. Local autonomy.** Each Participant shall have Participant Access Policies that establish how 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 Highlights

**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 Highlights

**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 Highlights

**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 Highlights

**19. Allocation of Liability Risk**. Each Participant is responsible for its own acts and omissions but not the acts and omissions of other Participants.

**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 Highlights

**20. Representations and Warranties** (continued):

- Participants warrant that they have the authority to transmit the 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 Highlights

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 Highlights

**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.

eHealth Exchange™

# Frequently Asked Questions (FAQ)

# May I ask other participants to demonstrate that they follow DURSA requirements and/or Applicable Law?

A Participant may **NOT** require other Participants to provide proof of their adherence to DURSA or Applicable Law. By signing the DURSA, each Participant already represents that each of its Transactions complies with the requirements of the DURSA and with Applicable Law. Section 13 of the DURSA details these representations and embodies these core principles of trusted exchange.

If a Participant has concerns that another Participant may not be complying with the DURSA and/or Applicable Law, the Participant should raise those concerns with the other Participant. If informal communications with the other Participant do not alleviate the Participant's concerns, the concern may be brought to the attention of eHealth Exchange management to facilitate further informal discussion and/or the Participant may initiate the Dispute Resolution Process. However, the appropriate recourse is NOT for one Participant to require proof of DURSA and/or Applicable Law compliance from another Participant.

# May I require other participants follow my organization's internal policies? What about my state's laws?

A Participant may **NOT** impose its laws or policies upon other Participants. The DURSA requires that all Participants comply with the terms of the DURSA, as well as the eHealth Exchange Operating Policies and Procedures ("OPPs"). Provided a Participant's internal policies are not in conflict with the DURSA and/or OPPs, a Participant is free to maintain such policies on its own behalf but may not impose such policies upon other Participants.

The DURSA requires each Participant to comply with Applicable Law, but **what is Applicable Law for one Participant may not be Applicable Law for another Participant**. Because many states have their own medical record privacy laws, the full scope of Applicable Law across all Participants will be different. Part of the beauty of the DURSA is that it requires and permits each Participant to fully comply with its Applicable Law without requiring all Participants to comply with the laws of all 50 states, D.C., and U.S. territories.

Here is an example of how this situation could unfold:

An individual has recently relocated from Virginia to Alaska. The individual is HIV+ and was actively under the care of a physician for this condition while residing in Virginia. The individual establishes a treatment relationship with a physician in Alaska to, among other things, manage the individual's HIV. Both the Virginia and Alaska physicians are part of networks that exchange electronic health information with Virginia and Alaska eHealth Exchange Participants. The individual's Alaska physician wants information from the individual's former physician in Virginia about how the individual responded to a specific antiretroviral medication as part of the Alaska physician's treatment of the individual. The Alaska physician initiates a query through the Alaska network and, since it is an eHealth Exchange Participant, the query is routed to the Virginia physician via the Virginia network in which the Virginia physician participates.

The Alaska eHealth Exchange Participant and the Virginia eHealth Exchange Participant are either Covered Entities themselves or Business Associates of the physician Covered Entities under HIPAA. Therefore, HIPAA is Applicable Law for both the Alaska and Virginia eHealth Exchange Participants. However, let's assume that Virginia state law requires that an individual provide written authorization to the Virginia physician before the physician can disclose any HIV-related information, even if the reason for the disclosure is to help another physician provide treatment to the individual. The Virginia law is not preempted by HIPAA because it is not in conflict with HIPAA by being more protective of the individual's privacy. Let's assume that Alaska law simply tracks HIPAA and does not impose any additional protections for medical records that reveal an individual's HIV status and related information.

It is important to be clear that the Virginia requirement is state law that applies to the Virginia physician and is mandatory. This is very different from a policy that an eHealth Exchange Participant might adopt to limit disclosure of electronic health information outside the Participant's network. It is appropriate for the Alaska physician to request the individual's HIV information for treatment purposes, and this request can be sent via the eHealth Exchange to the Virginia physician. However, Virginia law requires the Virginia physician to obtain the individual's written authorization before the physician may disclose those records to the Alaska physician. In other words, the query is valid since it is for a Permitted Purpose—Treatment—and the Alaska physician and the Alaska eHealth Exchange Participant have complied with HIPAA and Alaska law. However, the Virginia physician is not permitted by law to disclose the HIV information unless the individual provides written authorization to the Virginia physician.

The Virginia eHealth Exchange Participant may refuse to respond to the request from the Alaska eHealth Exchange Participant if the Virginia Participant does not have the patient's written authorization for the disclosure because Virginia law prohibits disclosure of HIV-related information without such a written authorization.

Contrast that with a situation in which there is no state law that imposes requirements more stringent than HIPAA for the disclosure of HIV information, and the state HIE that serves as an eHealth Exchange Participant adopts a policy that imposes additional consent/authorization requirements on the disclosure of HIV-related information. There may be many reasons that a Participant would adopt such a policy, but the key point is that it is not required by law. Therefore, the Participant is not permitted to use the policy as a reason to refuse to provide HIV-related information that is requested by another eHealth Exchange Participant for a Permitted Purpose.

# Recognizing that I request data for Treatment purposes from at least 1 other Participant, may I respond to Participant A but not Participant B?

**No**, Participants may **NOT** choose to whom they respond for purposes of Treatment. If a Participant requests data for Treatment purposes from any Participant, it must respond to requests for Treatment purposes **from all Participants**. This is referred to as the DURSA's "Duty to Respond" (see Section 12.01), and it is a foundational principle of the eHealth Exchange.

The Duty to Respond also includes a "null-response" obligation. This means that the Participant must respond to all Treatment-based requests with either: (i) the information requested; or (ii) a standardized response that the information is not available (i.e., the Participant does not have and/or cannot locate the information requested) or that it cannot be exchanged (e.g., the information is subject to an individual's restriction in accordance with 45 C.F.R. § 164.522).

**Participants cannot discriminate against other Participants when responding to Treatment requests**. The Duty to Respond means that an eHealth Exchange Participant must respond in the same manner to all other Participants that request information for Treatment. Any Participant requesting information for Treatment must still have appropriate legal authority to make the request, including valid consent or authorization if required by Applicable Law. However, if a Participant that requests information for Treatment receives a Treatment-based request from another Participant, the Participant must respond under the Duty to Respond. **A Participant cannot "pick and choose" the other Participants to which it will respond**.

# After receiving data requested for Treatment purposes, are participants permitted to subsequently disclose that data to others for non-Treatment purposes?

**Yes**, DURSA section 5.02 (Permitted Future Uses) generally permits Recipients retain, use and re-disclose Message Content in accordance with Applicable Law and the Recipient's record retention policies and procedures.

If the Recipient is a Participant that is a Business Associate of its Participant Users, such Participant may retain, use and re-disclose Message Content in accordance with Applicable Law and the agreements between the Participant and its Participant Users.

eHealth Exchange™

# How to Flow Down DURSA Terms

# Which provisions of the DURSA must Participants flow down within their organization to their users?

**Participant Users:** The 7 DURSA obligations listed below must be flowed down within a Participant's organization to each of its Participant Users in one or more legally enforceable written documents. These documents may take different forms depending on your organization and may include contracts, addenda, or company policies and procedures.

1. Comply with all Applicable Law (DURSA Section 15.04 (i))
2. Reasonably cooperate with your organization regarding any issues related to the DURSA (DURSA Section 15.04 (ii))
3. Only request, retrieve, and send data for a Permitted Purpose, as defined in the DURSA (DURSA Section 15.04 (iii))
4. Only use data received via eHealth Exchange in accordance with Applicable Law, consistent with your data retention policies, and subject to any other applicable terms and conditions set forth in the DURSA dealing with the use of Message Content (DURSA Section 15.04 (iv))

# Which provisions of the DURSA must Participants flow down within their organization to their users? Cont'

5. Report suspected and confirmed Adverse Security Events to your organization in a manner and timeframe that will allow you to fulfill your obligations for Adverse Security Event notification (DURSA Section 14.04 and 15.04 (v))
6. Refrain from disclosing any passwords, digital security certificates issued for use on the eHealth Exchange, or any other security measures issued by you or by the eHealth Exchange (DURSA Section 15.04 (vi))
7. Comply with any applicable Performance Specification(s) (DURSA Section 15.06)

# Which provisions of the DURSA must Participants flow down to their technology partners?

**Technology Partners:** To the extent a Participant uses technology partners in connection with the Transaction of Message Content, the 5 DURSA obligations listed below must be flowed-down to those technology partners in one or more legally enforceable written agreements.

1. Comply with all Applicable Law (DURSA Section 15.05 (i))
2. Protect the privacy and security of any Message Content to which the technology partner(s) have access (DURSA Section 15.05 (ii))
3. Report suspected and confirmed Adverse Security Events to your organization in a manner and timeframe that will allow you to fulfill your obligations for Adverse Security Event notification (DURSA Section 14.04 and 15.05 (iii))
4. Reasonably cooperate with other Participants, at your organization's direction, regarding any issues related to the DURSA (DURSA Section 15.05 (iv))
5. Comply with any applicable Performance Specification(s) (DURSA Section 15.06)

# Which provisions of the DURSA must Participants flow down to their participating organizations?

**Participating Organizations:** To the extent a Participant allows other organizations to connect to the eHealth Exchange through the Participant, the 7 DURSA obligations listed below must be flowed down to those participating organizations in one or more legally enforceable written agreements.

1. Comply with all Applicable Law (DURSA Section 15.04 (i))
2. Reasonably cooperate with your organization regarding any issues related to the DURSA (DURSA Section 15.04 (ii))
3. Only request, retrieve, and send data for a Permitted Purpose, as defined in the DURSA (DURSA Section 15.04 (iii))
4. Only use data received via eHealth Exchange in accordance with Applicable Law, consistent with your data retention policies, and subject to any other applicable terms and conditions set forth in the DURSA dealing with the use of Message Content (DURSA Section 15.04 (iv))

# Which provisions of the DURSA must Participants flow down to their participating organizations? Cont'

5. Report suspected and confirmed Adverse Security Events to your organization in a manner and timeframe that will allow you to fulfill your obligations for Adverse Security Event notification (DURSA Section 14.04 and 15.04 (v))
6. Refrain from disclosing any passwords, digital security certificates issued for use on the eHealth Exchange, or any other security measures issued by you or by the eHealth Exchange (DURSA Section 15.04 (vi))
7. Comply with any applicable Performance Specification(s) (DURSA Section 15.06)

# DURSA Flow-Down Best Practices and Additional Considerations

Best Practices:

- No best practices for *how* to flow these DURSA provisions down can be referenced.
  - The DURSA is clear on the specific provisions that Participants are required to flow down, but the DURSA allows each Participant to decide how to meet this requirement.
- *However*, the Participant may **not** simply require its customers to sign the DURSA as a way to flow down the required provisions.
  - The DURSA is a multi-party agreement between and among the eHealth Exchange Participants only.

Additional Considerations:

- eHealth Exchange Participants must carry through DURSA obligations to participating organizations or users who will use the Participant's eHealth Exchange connection.
- Any organization or individual who is able to access and either initiate or receive messages through **your** eHealth Exchange connection is held to the same standards in the DURSA, in order to maintain a chain of trust in the exchange.