eHealth Exchange

Data Use and Reciprocal Support Agreement (DURSA)

Policy Assumptions

May 3, 2011

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.

The following outlines the key policy assumptions which underscore the agreement:

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

- **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.
- **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.
- **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.
- **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.
- **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).
- **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.
- **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.
- **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.
- **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.

- 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.
- 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.