

# Overview: Data Use and Reciprocal Support (DURSA)

## Provisions Overview

November 20, 2009

As part of ongoing work on the Nationwide Health Information Network (“NHIN”) Trial Implementations – Option Year 1, a large, multi-stakeholder team was assembled to develop a comprehensive agreement that would govern the exchange of health data across a diverse set of public and private entities. This agreement – the Data Use and Reciprocal Support Agreement (“DURSA”) – is a comprehensive, multi-party trust agreement that will be signed by all entities who wish to exchange data on a nationwide basis (“Participants”). The DURSA provides the legal framework governing participation in nationwide information exchange by requiring the signatories to abide by a common set of terms and conditions that establish the Participants’ obligations and the trust fabric to support the privacy, confidentiality and security of the health data that is exchanged.

Key terms and conditions of the DURSA are summarized below. This summary is not all inclusive nor does it attempt to address all of the intricacies in the DURSA that have been memorialized in carefully crafted contract language. Instead, it is offered as a basic overview of the DURSA to help facilitate review of the agreement.

- **Multi-Party Agreement.** The DURSA must accommodate and account for a variety of Participants so that it can successfully serve as a multi-party agreement among all Participants. This multi-party agreement is critical to avoid the need for each Participant to enter into “point-to-point” agreements with each other Participant, which becomes exceedingly difficult, costly and inefficient as the number of Participants increases.
- **Participants in Production.** The DURSA expressly assumes that each Participant is in “production” and, as a result, already has in place trust agreements with or written policies applicable to its end users. These end user trust agreements and policies support the trust framework memorialized in the DURSA.
- **Privacy and Security Obligations.** To the extent that each Participant has existing privacy and security obligations under applicable law (e.g. HIPAA or other state or federal privacy and security statutes and regulations), the Participant is required to continue complying with these obligations. Participants, which are neither HIPAA covered entities, HIPAA business associates nor governmental agencies, are obligated to comply with specified HIPAA Privacy and Security Rules as a contractual standard of performance.
- **Requests for Data Based on Permitted Purposes.** Participant’s end users may only request information through the NHIN for “Permitted Purposes,” which include treatment, limited purposes related to payment, limited health care operations with respect to the patient that is the subject of the request, specific public health activities, quality reporting for “meaningful use” and disclosures based on an authorization from the individual.
- **Duty to Respond.** Participants that allow their respective end users to seek data through the NHIN for treatment purposes have a duty to respond to requests for data for treatment purposes. This duty to respond means that the Participant will send a standardized response to the requesting Participant, which may or may not include the actual data requested. Participants are permitted, but not required, to respond to all other (non-treatment) requests. The DURSA does not require a Participant to disclose data when such a disclosure would violate applicable law or conflict with any restrictions an individual may have placed on the data in accordance with the HIPAA Privacy Rule.
- **Future Use of Data Received Through the NHIN.** Once the Participant or Participant’s end user receives data from a responding Participant (i.e. a copy of the responding Participant’s records), the recipient may incorporate that data into its records and retain that information in accordance with the recipient’s record retention policies and procedures. The recipient can re-use and

re-disclose that data in accordance with all applicable law and the agreements between a Participant and its end users.

- **Duties of Requesting and Responding Participants.** Each Participant has certain duties when acting as a requesting or responding Participant.
  - When responding to a request for data, Participants will apply their local policies to determine whether and how to respond to the request. This concept is called the “autonomy principle” because each Participant can apply its own local policies before requesting data from other Participants or releasing data to other Participants.
  - It is the responsibility of the responding Participant – the one disclosing the data – to make sure that it has met all legal requirements before disclosing the data, including, but not limited to, obtaining any consent or authorization that is required by law applicable to the responding Participant. This policy is essential for nationwide health information exchange given the number of different state laws, Federal statutes and local policies related to consent or authorization to exchange data for treatment purposes. To effectively enable the exchange of health information in a manner that protects the privacy, confidentiality and security of the data, the DURSA adopts the HIPAA Privacy and Security Rules as minimum requirements.
  - Under HIPAA, data can be exchanged for treatment purposes without obtaining a separate consent or authorization. Under some state laws and other Federal laws, however, patient consent or authorization is required to exchange data for treatment. Responding Participants who are subject to these more restrictive laws will be required to obtain those consents or authorizations that they deem necessary under their applicable laws before sending data through the NHIN. As the DURSA is written, the responsibility for obtaining this consent or authorization will not fall to the requesting Participant, usually a healthcare provider, because there is simply no way for the requesting healthcare provider to keep track of the rapidly changing laws and regulations in every state. It is unlikely that even patients will know what specific consent forms may be required for data exchange by their local Health Information Exchange (HIE). Requiring the requesting Participant to obtain a consent or authorization that complies with the responding Participant’s applicable law would create an undue burden on requesting Participants. Essentially, this would require the requesting Participant to track the laws of all 50 states and federal laws beyond HIPAA and have consent or authorization forms that meet each individual state’s requirements. Instead, it is more reasonable to expect each responding Participant to remain current on the legal requirements to which it is subject and take steps to comply with those laws.
  - When a request is based on a purpose for which authorization is required under HIPAA (e.g. for SSA benefits determination), the requesting Participant must send a copy of the authorization with the request for data. As described in the bullet above, requesting Participants are *not* obligated to send a copy of an authorization or consent when requesting data for treatment purposes.
- **NHIN Coordinating Committee.** The NHIN Coordinating Committee will be responsible for accomplishing the necessary planning, consensus building, and consistent approaches to developing, implementing and operating the NHIN, including playing a key role in NHIN breach notification; dispute resolution; Participant membership, suspension and termination; NHIN operating policies and procedures; and, will inform the Technical Committee when proposed changes for interface specifications have a material impact on Participants.
- **NHIN Technical Committee.** The NHIN Technical Committee will be responsible for determining priorities for the NHIN and creating and adopting specifications and test approaches. The NHIN Technical Committee will work closely with the NHIN Coordinating Committee to assess the impact that changes to the specifications and test approaches may have on Participants.
- **Breach Notification.** Participants are required to promptly notify the NHIN Coordinating Committee and other impacted Participants of breaches which involve the unauthorized disclosure of data through the NHIN, take steps to mitigate the breach and implement corrective action plans

to prevent such breaches from occurring in the future. Suspected breaches must be reported within one (1) hour of discovering information that leads the Participant to believe that a breach may have occurred. As soon as reasonably practicable, but no later than twenty-four (24) hours, Participants must notify affected Participants and the NHIN Coordinating Committee. This process is not intended to address any obligations for notifying consumers of breaches, but simply establishes an obligation for Participants to notify each other when breaches occur to facilitate an appropriate response.

- **Mandatory Non-Binding Dispute Resolution.** Because the disputes that may arise between Participants will be relatively complex and unique, the Participants will agree to participate in a mandatory, non-binding dispute resolution process.
- **Allocation of Liability Risk.** With respect to liability, the DURSA memorializes the Participant's understanding that each Participant is responsible for its own acts or omissions.
- **Applicable Law.** The DURSA reaffirms each Participant's obligation to comply with "Applicable Law." As defined in the DURSA, "Applicable Law" is the law of the jurisdiction in which the Participant operates. For non-Federal Participants, this means the law in the state(s) in which the Participant operates and any applicable Federal law. For Federal Participants, this means applicable Federal law.