

Recommendations For Texas Health Information Exchange Trust Agreements

Cynthia Marietta, J.D., LL.M.

UNIVERSITY of **HOUSTON** | LAW CENTER
Health Law & Policy Institute

Prepared for the Texas Health and Human Services Commission and the
Texas Health Services Authority with support from the State Health
Information Exchange Cooperative Agreement Program

August 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
I. OVERVIEW ON THE DEVELOPMENT AND PURPOSE OF HEALTH INFORMATION EXCHANGES	3
A. A Brief History of Health Information Technology.....	3
B. Electronic Health Record (EHR)	5
C. Health Information Exchange (HIE).....	6
D. Ongoing Federal HIE Initiatives.....	7
II. TRUST AGREEMENTS PROVIDE THE TRUST FRAMEWORK FOR HEALTH INFORMATION EXCHANGES	9
A. What is a Trust Agreement?	10
B. Essential Elements of Trust Agreements Necessary for Supporting Health Information Exchanges	11
III. THE FEDERAL TRUST AGREEMENT FOR HIE: THE DATA USE AND RECIPROCAL SUPPORT AGREEMENT (DURSA)	13
A. What is the Data Use and Reciprocal Support Agreement (DURSA)?	13
B. Key Provisions of the DURSA	14
C. DURSA is a Living Agreement	18
IV. RECOMMENDATIONS FOR TRUST AGREEMENT FOR TEXAS HEALTH INFORMATION EXCHANGES	19
A. Issues Concerning Data Segmentation:	19
B. Participant Indemnification Provision:	26
C. Monetary Penalties Imposed Against Violators	28
D. HIPAA Compliance Requirements and Business Associates Provisions.....	28
E. Designation of Management and Operational Committees	27
Key Policy Questions	28
V. CONCLUSION	28

EXECUTIVE SUMMARY

There is statistical evidence to suggest that the systematic use of health information technology (health IT) will improve the quality and efficiency of health care. For more than a decade, the federal government has played an active role in promoting use of health IT. In 1994, the Office of the National Coordinator for Health Information Technology (ONC) was created to further nationwide implementation of an interoperable health IT infrastructure with the goal of providing most Americans with access to secure electronic health records by 2014. In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH), an integral part of the American Recovery and Reinvestment Act of 2009, to promote the use of health IT to improve health care quality, safety, and efficiency in the United States. The ONC continues to be the principal federal entity responsible for coordinating nationwide efforts to implement advanced use of health IT and the electronic exchange of health information.

Electronic health records (EHRs) are computerized versions of patients' records. EHRs may be accessed from off-site locations when linked into a health information exchange (HIE), which is defined as the electronic movement of health information among organizations using nationally recognized standards. Experts believe that nationwide HIE will benefit the U.S. health care system by improving health care quality, safety, and efficiency. However, the full benefits of nationwide HIE can be realized only if patients and health care providers have confidence that electronic health information will be kept private and secure.

A trust agreement provides the means for supporting exchange of health information and ensuring privacy, security, and trust among participants within an HIE. It is a contract that outlines the rights, responsibilities, and obligations of all HIE participants. To be effective, an HIE trust agreement must be a multi-party agreement to accommodate multiple participants. It must define the legal framework within which participants may exchange health data in compliance with federal and state privacy laws. Further, it must require participants to have trust agreements with their end-users and allow additional participants to join in the future.

The current federal trust agreement for nationwide HIE is called The Data Use Reciprocal Agreement (DURSA), which provides the legal framework for participants engaged in nationwide exchange of health data. DURSA requires participants to abide by specific terms and conditions that establish participants' obligations and responsibilities.

DURSA could serve as the model basis for an effective Texas HIE trust agreement, but would require some modifications and may require additional provisions. Consideration of modifications for a Texas HIE specific trust agreement may include issues concerning data segmentation, participant indemnification requirements, imposition of monetary penalties for violators of the trust agreement, HIPAA compliance expectations for business associates, Texas medical records privacy laws, and designation and duties of management and/or technical oversight committees. Drafters of the trust agreement for a Texas HIE should take into account any policy considerations and implications and effectively address such policy issues.

I. OVERVIEW ON THE DEVELOPMENT AND PURPOSE OF HEALTH INFORMATION EXCHANGES

Key Points

- The HITECH Act of 2009 promotes the electronic use and exchange of health information as a means to improve the quality and efficiency of health care in the U.S.
- Electronic health records (EHRs) are computerized versions of patients' records.
- EHRs may be accessed from off-site locations when linked into a health information exchange (HIE).
- An HIE is defined as the electronic movement of health information among organizations using nationally recognized standards.
- Experts believe a nationwide HIE will benefit the U.S. health care system by improving health care quality, safety, and efficiency.
- The full benefits of a nationwide HIE can be realized only if patients and health care providers are confident that electronic health information will be kept private and secure.

A. A Brief History of Health Information Technology

Statistical evidence suggests the systematic use of health information technology (health IT) may offer improvements in quality and efficiency of health care.¹ In the past decade, the federal government has played an active role in the evolution and use of health IT, including the adoption and ongoing support for standards needed to achieve nationwide interoperability.² In April 2004, through Executive Order 13335, former President George W. Bush created the position of Office of the National Coordinator for Health Information Technology (ONC) and called for nationwide implementation of interoperable health IT infrastructure, with the goal of providing most Americans with access to secure electronic health records by 2014.³ ONC, which is organizationally located within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS), is the principal federal entity responsible for coordinating nationwide

¹ Chaudhry, et al., *Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care*, ANNALS OF INTERNAL MEDICINE, Vol. 144, No. 10: 742-752 (2006).

² U.S. Department of Health and Human Services (HHS), *Executive Summary: The Office of the National Coordinator for Health Information Technology (ONC)*, Nov. 9, 2004, <http://www.himss.org/handouts/executiveSummary.pdf>.

³*Id.*; see Executive Order 13335 of April 27, 2004, available at http://edocket.access.gpo.gov/cfr_2005/janqtr/pdf/3CFR13335.pdf; see also HHS, *The Office of the National Coordinator for Health Information Technology (ONC)*, Dec. 8, 2010, available at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_onc/; HHS/ONC, *American Health Information Community (AHIC)*, Oct. 30, 2009, available through <http://www.healthit.hhs.gov/>.

efforts to implement advanced use of health IT and the electronic exchange of health information.⁴

In 2005, to advance former President Bush's vision, then-Secretary of HHS Michael O. Leavitt chartered the American Health Information Community (AHIC) to serve as a federal advisory body to make recommendations on how to accelerate the development and adoption of health IT.⁵ From 2005 to 2008, the AHIC issued more than 200 recommendations, addressing a wide variety of catalysts and barriers, including a long list of complex inter-related privacy and security issues.⁶ The AHIC recommendations addressed both consumer or patient needs and the technology necessary to advance interoperability of health IT.⁷

Also in 2005, ONC awarded multiple contracts to numerous entities to create processes and protocols to harmonize standards, certify EHR applications, develop health information network prototypes and recommend changes to security and privacy policies.⁸ These contracts led to the creation of the Healthcare Information Technology Standards Panel (HITSP), a cooperative partnership between the public and private sectors.⁹ Between 2005 and 2010, HITSP focused its efforts on developing, through harmonization and integration, a useful set of standards to support widespread interoperability of health care applications and the interchange of health care data.¹⁰

In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH), an integral part of the American Recovery and Reinvestment Act of 2009,¹¹ to invest in and promote the use of health IT in order to improve health care quality, safety, and efficiency in the United States.¹² HITECH expressly charges ONC with the responsibility of developing a nationwide health IT infrastructure that would allow for the electronic use and exchange of information to improve health care quality, reduce medical errors, reduce health care costs due to inefficiency, and advance the delivery of patient-centered medical care, among other things.¹³ As outlined in HITECH,

⁴ See *ONC*, *supra* note 3.

⁵ See *AHIC*, *supra* note 3.

⁶ *Id.*

⁷ *Id.*

⁸ Healthcare Information and Management Systems (HIMSS), *What is the Health Information Technology Standards Panel?*, 2011, available at http://www.himss.org.asp/topics_hitsp.asp.

⁹ *Id.*

¹⁰ *Id.*; *The HITSP contract with HHS concluded on April 30, 2010.* See <http://www.himss.org>.

¹¹ American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, H.R. 1 (2009) (*enacted as the Health Information Technology for Economic and Clinical Health Act (HITECH) in Title XIII and Title IV, Div. B*), 123 Stat. at 230 (codified at 42 U.S.C.A. 300jj-11 (West 2009)).

¹² HITECH, *supra* note 11, at Title XIII, §§13101-13424; see also HHS/ONC, *HITECH Programs*, Jan. 27, 2011, available through <http://www.healthit.hhs.gov>.

¹³ HITECH, *supra* note 11, at Title XIII, §13101; U.S. Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC), *The Nationwide*

ONC's duties include coordinating efforts to facilitate, implement and use health IT, promote meaningful use of electronic health records (EHR), and design the infrastructure for ensuring secure exchange of electronic health information.¹⁴

B. Electronic Health Record (EHR)

An EHR is an electronic record containing an individual's health-related information that conforms to nationally recognized interoperability standards and that can be created, managed, and reviewed by authorized health care providers spanning more than one health care organization.¹⁵ EHRs are computerized versions of patients' clinical, demographic and administrative data and may include treatment histories, medical test reports, and images stored in an electronic format.¹⁶ All medical information stored on paper may be stored in an EHR, but the EHR offers more flexibility and storage capability than paper records.¹⁷ For instance, a patient's electronic record may include a comprehensive list of all diagnostic tests and drugs prescribed to that patient. The physician could access the list and view it in chronological order, or re-arrange it in any other manner using charts or graphs to allow the physician to see trends and changes that could affect the patient's treatment.¹⁸ Moreover, EHRs allow quick retrieval of complete patient information by physicians and other providers.¹⁹ EHRs enable easier access in times of emergency and may be backed up to avoid loss during disasters, especially when the records are linked into a health information network, or health information exchange (HIE).²⁰

An EHR may also include computerized provider order entry (CPOE) and clinical decision support (CDS) systems. CPOE is an application that enables physicians to enter medical orders into a computer system.²¹ CPOE replaces the more traditional methods of placing medication orders, such as by written/paper prescriptions, verbal prescriptions, or by facsimile transmission.²² Most CPOE systems allow providers to electronically

Health Information Network, Direct Project, and CONNECT Software, March 8, 2011, available through <http://www.hhs.gov>; see also HHS/ONC, *Electronic Health Records and Meaningful Use*, Feb. 9, 2011, available through <http://www.healthit.hhs.gov>.

¹⁴ See ONC, *supra* note 3.

¹⁵ The National Alliance for Health Information Technology created this definition. See HHS/ONC, *Frequently Asked Questions About Electronic Health Records and Health Information Networks*, Oct. 7, 2010, available through <http://www.healthit.hhs.gov>. Although EHRs are sometimes referred to as electronic medical records (EMR), EHR is now the preferred term because its definition includes the ability to exchange information interoperability while EMRs do not necessarily have that ability. *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ See *Frequently Asked Questions*, *supra* note 15.

¹⁹ *Id.*

²⁰ *Id.*

²¹ HHS, Agency for Research and Healthcare Quality (ARHQ), *Inpatient Computerized Provider Order Entry (CPOE)*, available at http://www.ahrq.gov/images/jano9cpoereport/cpoe_issue_paper.htm.

²² *Id.*

specify medication orders, as well as laboratory, admission, radiology, referral, and procedure orders.²³ While CPOEs may improve patient safety by ensuring orders are legible, the functional value of CPOEs is increased by adding clinical decision support (CDS) systems, a technology that provides clinicians with real-time feedback about a wide-range of diagnostic and treatment-related information as they enter electronic orders.²⁴ CDS support can check for a variety of potential errors, such as drug interactions, patient allergies to prescribed medications, medication contraindications, and renal and weight-based dosing.²⁵ When implemented together, CPOE and CDS systems can improve medication safety, quality of care, compliance with provider guidelines, and reduce costs of care.²⁶

C. Health Information Exchange (HIE)

Although nearly 80 percent of health care providers still use paper-based medical record systems,²⁷ there are new government programs and incentives to help health care providers make the transition from paper to EHRs.²⁸ The goal is to link EHRs to an HIE, which is defined as the electronic movement of health information among organizations according to nationally recognized standards.²⁹ Industry experts believe that a nationwide health information exchange would benefit patients and the U.S. health care system by improving health care quality, reducing medical errors, reducing health care disparities, and advancing the delivery of patient-centered medical care.³⁰

Achieving these benefits, however, requires the implementation of a sound HIE infrastructure carries with it the challenge of how to effectively protect confidential health information. Health care providers must possess accurate and complete information about their patients in order to deliver quality, coordinated care. Yet, if patients and health care providers lack trust in the electronic exchange of health information due to concerns about the accuracy and completeness of such information or

²³ *Id.*

²⁴ *Id.*; G.J. Kuperman and R.F. Gibson, *Computer Physician Order Entry: Benefits, Costs, and Issues*, ANN. INTERN MED 2003, 139(1):31-9; D.F. Sittig and W.W. Steed, *Computer Based Physician Order Entry: The State of the Art*, J. AM MED INFORM ASSOC 1994, 1(2):108-23.

²⁵ *Inpatient Computerized Provider Order Entry (CPOE)*, *supra* note 24.

²⁶ *Id.*

²⁷ Executive Office of the President, President's Council of Advisors on Science and Technology, *Report To The President Realizing The Full Potential Of Health Information Technology To Improve Healthcare For Americans: The Path Forward*, at 1, Dec. 2010, available through <http://www.whitehouse.gov/ostp/pcast>.

²⁸ *Id.*; *Frequently Asked Questions*, *supra* note 15; Centers for Medicare and Medicaid Services (CMS), *EHR Incentive Programs: Overview*, May 17, 2011, available at <https://www.cms.gov/ehrincentiveprograms/>.

²⁹ *Frequently Asked Questions*, *supra* note 15.

³⁰ HHS/ ONC, *Privacy and Security: Advancing Privacy and Security in Health Information Exchange*, Jan. 19, 2011, <http://www.healthit.hhs.gov>.

the risks of breach of confidential health information, they may be unwilling to disclose necessary health information.³¹ Several recent studies confirm the positive impact that health IT, including the use of EHRs and telehealth, have on improving access to health care and effective management of chronic diseases in rural and inner-city medically underserved areas, and reducing health disparities in minority populations.³² In light of these studies, any withholding of pertinent health information due to the lack of trust would only frustrate the purpose of having health IT and HIE in the first place--to improve health care quality, reduce medical errors, reduce health care costs due to inefficiency, and advance the delivery of patient-centered medical care,³³

The full benefits of health IT can be realized only if patients and health care providers have confidence and trust that electronic health information will be kept private and secure.³⁴ To that end, ONC looks to the federal Health Information Technology Policy Committee (HITPC) and HIT Standards Committee (HITSC) to explore policy and technical methods for allowing patient choice in the exchange of health information.³⁵ The Office of the Chief Privacy Officer³⁶ works with ONC divisions to assure the integration of privacy considerations into all facets of ONC activities and projects.³⁷

D. Ongoing Federal HIE Initiatives

In addition, ONC oversees the technical and policy foundations of one of its initiatives, the Nationwide Health Information Network (NHIN), to ensure that methods for achieving trust among entities exchanging information are utilized while integrating best

³¹*Id.*

³² Ernest I. Carter, et al, *A Patient-Centric, Provider-Assisted Diabetes Telehealth Self-Management Intervention for Urban Minorities*, Perspectives in Health Information Management (Winter 2011): 1-9, available through <http://perspectives.ahima.org/>; Michael C. Gibbons, *Use of Health Information Technology among Racial and Ethnic Underserved Communities*, Perspectives in Health Information Management (Winter 2011): 1-13, available through <http://perspectives.ahima.org/>; Rena Brewer, et. al, *A Peach of a Telehealth Program: Georgia Connects Rural Communities to Better Healthcare*, Perspectives in Health Information Management (Winter 2011): 1-9, available through <http://perspectives.ahima.org/>; Mark Carroll, et. al, *Innovation in Indian Healthcare: Using Health Information Technology to Achieve Health Equity for American Indian and Alaska Native Populations*, Perspectives in Health Information Management (Winter 2011): 1-9, available through <http://perspectives.ahima.org/>.

³³ See, e.g. *supra* notes 12 and 13 and accompanying text.

³⁴ *Id.*; see also David Blumenthal, M.D. and Georgina Verdugo, *Building Trust in Health Information Exchange*, July 8, 2010, available through <http://www.healthit.hhs.gov>.

³⁵ *The Nationwide Health Information Network, Direct Project, and CONNECT Software*, *supra* note 13.

³⁶ *Id.*; HHS, *Office of National Coordinator for Health IT*, Aug. 13, 2010, available through <http://www.healthit.hhs.gov/>.

³⁷ *The Nationwide Health Information Network, Direct Project, and CONNECT Software*, *supra* note 13; HHS/ONC, *ONC Programs*, Mar. 20, 2009, available through <http://www.healthit.hhs.gov>.

practices for privacy and security.³⁸ The NHIN is not a physical network that stores patient records or runs on servers at HHS,³⁹ rather, it is a collection of exchange standards, protocols, legal agreements, specifications, and services designed to provide a secure, nationwide, interoperable health information infrastructure that will connect health care providers, patients or consumers, and supporting third parties involved in health care.⁴⁰ It is designed to move health care from the existing paper-based system to a process where health care information is electronically stored and shared in a secure manner.⁴¹

Using NHIN standards, ONC launched three initiatives to help expand efforts for secure health information exchange.⁴² These initiatives include the: (1) Nationwide Health Information Network Exchange, (2) Direct Project, and (3) CONNECT software solution.⁴³ The Nationwide Health Information Network Exchange (NHIN Exchange) is a group of federal agencies and private organizations that engage in secure exchange of electronic health information. These organizations are in the continuous process of developing NHIN standards, services, and policies and are currently engaged in live health information exchange.⁴⁴ These entities send and retrieve electronic health information to support direct patient care, streamline benefit claims, and improve public health tracking.⁴⁵

The Direct Project, launched in March 2010, is developing standards and services required to enable secure, directed health information exchange at a more local and less complex level among trusted providers in support of the stage 1 “Meaningful Use” incentive requirements.⁴⁶ This project will expand the existing Nationwide Health Information Network standards and services, within a policy framework, to enable the simple, direct, and secure transport of health information, between health care providers at the local level and their patients.⁴⁷ The Direct Project is complementary to the work of the Nationwide Health Information Network Exchange.⁴⁸ According to the ONC, both models may be needed to support nationwide health information exchange.⁴⁹

³⁸ *Id.*

³⁹ *Nationwide Health Information Network, Direct Project, and CONNECT Software, supra* note 13.

⁴⁰ ONC, *ONC Programs, supra* note 35.

⁴¹ *Id.*

⁴² *Id.*

⁴³ ONC, *ONC Programs, supra* note 35.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Nationwide Health Information Network, Direct Project, and CONNECT Software, supra* [note](#) 13.

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *Id.* Some individuals, however, may not agree that the Direct Project is necessary. They believe the Direct Project conflicts with the state-wide HIE initiatives by allowing an “end-run” around the HIE initiatives.

CONNECT is a free, open source software solution that supports health information exchange at both local and national levels.⁵⁰ This software solution was initially developed by federal agencies to support their health-related missions. CONNECT uses NHIN standards, services, and policies to make sure that health information exchanges are compatible with other exchanges being set up throughout the country.⁵¹

ONC refers to the NHIN as a “network of networks,” that is formed when HIEs use NHIN standards and agreements to exchange health information among one another.⁵² NHIN utilizes various technologies and approaches, and is built upon a core set of capabilities to enable nationwide information exchange among a diverse set of organizations. One significant core capability includes the support of a common “trust agreement” that establishes the obligations and assurances to which all NHIN exchange participants must agree and abide.

II. TRUST AGREEMENTS PROVIDE THE TRUST FRAMEWORK FOR HEALTH INFORMATION EXCHANGES

Key Points

- A trust agreement is an essential tool for supporting exchange of health information and for establishing and ensuring privacy, security, and trust within an HIE.
- A trust agreement is a contractual agreement that outlines the rights, responsibilities, and obligations of all HIE participants and imposes accountability requirements on participants
- An effective HIE trust agreement contains four (4) essential elements:
 - 1) It must be multi-party agreement to accommodate multiple participants,
 - 2) It must define the legal framework within which participants may exchange health data in compliance with federal and state privacy laws,
 - 3) It must require participants to have trust agreements with their end-users and
 - 4) It must make provisions to allow additional participants to join in the future.

Trust is the cornerstone for effective HIE. As Protected Health Information (PHI) is exchanged among HIE participating organizations, each participant organization in the data stream has its own legal and business interests to protect.⁵³ Likewise, patients should be able to trust the entire chain of health care providers and business processes that handle their PHI.⁵⁴ They should be able to trust that their health care providers will keep their PHI confidential and will not use or disclose it unless authorized by law or as

⁵⁰ *ONC Programs, supra* note 35.

⁵¹ *Id.*

⁵² *Id.*

⁵³ The Markle Foundation, *Chain-of-Trust Agreements*, 2011, <http://www.markle.org/health/markle-common-framework/connecting-consumers/cp4>.

⁵⁴ *Id.*

consistent with their written consent. Health care providers should be able to trust that the participants in an HIE network will comply with privacy and security laws and honor the scope of their patients' authorization or consent.

Privacy and security protections are essential to establishing the public trust necessary for an effective HIE.⁵⁵ The ONC and the HHS Office of Civil Rights (OCR) are working jointly on a number of projects to ensure that the electronic exchange of health information is built on a foundation of privacy and security.⁵⁶ In July 2010, ONC and OCR issued a joint statement acknowledging the use of health IT technology to improve health care and the significance of building consumer trust in HIE.⁵⁷ The joint statement espouses in pertinent part:

Our Nation is poised to harness the power of information technology to improve health care. . . . As we enter into a new age of electronic health information exchange, it is more important than ever to ensure consumer trust in the privacy and security of their health information and in the industry's use of new technology.⁵⁸

To that end, public and private stakeholders in the health IT field have determined that a "trust agreement" is an essential tool for supporting exchange of health information and for establishing and ensuring trust within an HIE.⁵⁹

A. What is a Trust Agreement?

In the context of HIEs, a trust agreement is a contract that memorializes a common set of trust expectations into a legally enforceable framework. A trust agreement serves as the mechanism to encourage "good network citizenship" among HIE participants and to bind HIE participants to the core set of "network rules" and specified privacy and security policies concerning the confidential information they exchange or share.⁶⁰

⁵⁵ HHS/ONC, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*, Dec. 15, 2008, at 6.

⁵⁶ David Blumenthal, M.D. and Georgina Verdugo, *Building Trust in Health Information Exchange*, July 8, 2010, available through <http://www.healthit.hhs.gov>.

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ NHIN Forum, *Developing Trust Agreements to Support Exchange of Health Information*, available through <http://www.healthit.hhs.gov>.

⁶⁰ *Chain-of-Trust Agreements*, *supra* note 51. A HIPAA required Business Associate Agreement is but one example of a trust agreement between a covered entity and its business associate. *Id.*

B. Essential Elements of Trust Agreements Necessary for Supporting Health Information Exchanges

The trust agreement provides the trust framework for supporting the confidentiality and security of health data to be exchanged among multiple health care provider participants within an HIE. It should clearly outline the rights, responsibilities, and obligations of all HIE participants and impose accountability requirements to maintain the trust of the patients and participants organizations involved in the exchange. Moreover, to be effective, an HIE trust agreement should encompass certain essential elements, to include the following:

1. Multi-Party Agreement vs. Point-to-Point Trust Agreement to Accommodate Multiple Participants:

A multi-party trust agreement is necessary to accommodate and account for all participating entities that want to exchange data within the HIE. Currently, most electronic exchange of health data is “point-to-point,” meaning there is a data originator and a data recipient.⁶¹ A point-to-point trust framework for an HIE, however, is not sustainable with multiple participants on a large-scale basis.⁶²

A multi-party trust agreement, on the other hand, is infinitely scalable and can accommodate an infinite number of participating parties.⁶³ A multi-party agreement precludes the need for each participant to enter into “point-to-point” agreements with each other participant, which would become increasingly difficult, costly and inefficient as the number of participants in an HIE increases.⁶⁴ All participants in an HIE must sign its multi-party trust agreement, indicating their agreement and publicly committing to uphold the core set of “network rules.”⁶⁵ A multi-party agreement is not as customizable as a point-to-point agreement; however, if there is consensus among all participants to the multi-party trust agreement, a fully tailored, customizable agreement may not be necessary.⁶⁶

⁶¹ *Id.*

⁶² *Id.*

⁶³ *Webinar: DURSA is Too Complex to Work, and Other Myths*, June 22, 2010, available at http://www.cmio.net/index.php?option=com_articles&article=22861.

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

2. *Defines the Legal Framework for Participant Exchange in Compliance with Federal and State Laws*

The multi-party trust agreement defines how the participants in the HIE relate to each other and creates the legal framework within which the participants can exchange data electronically within the HIE. It should identify a common set of terms and conditions that establish participants' rights, responsibilities, and obligations to support the privacy, confidentiality, and security of health data that is exchanged.⁶⁷ It should comply with all applicable federal laws, including HIPAA, HITECH, the Privacy Act, the Freedom of Open Information Act, and the Federal Torts Claims Act. Moreover, it should comply with and/or reconcile various state laws, including health records privacy laws and basic contract law.

3. *Assumes Participants Have Trust Relationships In Place with Their End Users*

The multi-party trust agreement expressly assumes that each participant has in place trust agreements with or necessary written policies applicable to its end users, including its agents, employees, data suppliers and connections, networks, etc...).⁶⁸ These end-user trust agreements and policies should support the trust framework memorialized in the multi-party trust agreement.⁶⁹

4. *Viewed as a "Living Document" with Additional Participants Joining the Agreement Over Time*

The initial multi-party trust agreement is executed by the initial set of signatory participants to establish the legal framework to support an operational HIE. However, over time, additional participating entities would be expected to execute the agreement as they join the HIE.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ NHIN, *Overview: Data Use and Reciprocal Support (DURSA) Provisions Overview*, Nov. 20, 2009, available through <http://www.hhs.gov/healthit/nhin>.

III. THE FEDERAL TRUST AGREEMENT FOR HIE: THE DATA USE AND RECIPROCAL SUPPORT AGREEMENT (DURSA)

Key Points

- DURSA is the federal trust agreement for nationwide HIE.
- DURSA provides the legal framework for participants engaged in nationwide exchange of health data and the trust fabric to support privacy and security of health data.
- DURSA requires participants to abide by terms and conditions that establish their obligations.

As part of its on-going work, the NHIN formed the NHIN Cooperative Team, which is a large, diverse, multi-stakeholder team, consisting of private, public and federal entities.⁷⁰ The NHIN Cooperative team collectively developed a comprehensive trust agreement to govern the exchange of health data across the diverse set of public and private entities within the NHIN “network of networks.”⁷¹ This trust agreement--the Data Use and Reciprocal Support Agreement (DURSA)⁷²--provides the legal framework governing participation in nationwide information exchange and the trust fabric to support the privacy, confidentiality and security of the health data that is exchanged. It requires the participating entities that wish to exchange data on a nationwide basis (participants) to abide by a common set of terms and conditions that establish the participants’ obligations.⁷³

A. What is the Data Use and Reciprocal Support Agreement (DURSA)?

The DURSA is a comprehensive agreement designed specifically for multiple parties that establishes the rules of engagement and obligations to which all NHIN participants must agree and sign as a condition of joining⁷⁴ and exchanging health information with each other via the NHIN.⁷⁵ DURSA is based upon an existing body of law (federal, state, and local) and the current NHIN policy for exchange of PHI.

⁷⁰ *Id.* at 1.

⁷¹ National Health Information Network Cooperative DURSA Team, *Data Use and Reciprocal Support Agreement (DURSA)*, at 1, Nov. 18, 2009, available at <http://www.tricare.mil/tma/privacy/downloads/DURSA.pdf>.

⁷² *Id.*

⁷³ *Overview*, *supra* note 67, at 1.

⁷⁴ *DURSA*, *supra* note 69, at 2.

⁷⁵ *Id.* at 2.

B. Key Provisions of the DURSA

The DURSA contains several terms and conditions that form the basis for an effective trust agreement for HIEs. The key provisions in DURSA are outlined and discussed below:

1. ***Multi-Party Agreement:*** The DURSA is a multi-party trust agreement, capable of accommodating and serving a variety of participants. As consistent with what was previously identified as an essential element of an effective trust agreement,⁷⁶ the NHIN Cooperative determined that a multi-party agreement is crucial to avoid the need for “point-to-point” agreements between participants. “Point-to-point” agreements would be exceedingly difficult, costly and inefficient as the number of participants in the NHIN network of networks increases.⁷⁷
2. ***Participants in “Production”:*** The DURSA expressly assumes that each participant is in “production” -- meaning that the participant is operational -- and already has in place trust agreements with or written policies applicable to its end users. These end-user trust agreements and policies should support the trust framework memorialized in the DURSA.⁷⁸
3. ***Privacy and Security Obligations:*** To the extent each participant has existing privacy and security obligations under applicable federal and state laws and regulations, the participant is required to continue complying with these obligations. Participants that are neither HIPAA covered entities, business associates nor governmental agencies are obligated to comply with specified HIPAA Privacy and Security Rules as a contractual standard of performance.⁷⁹
4. ***Requests for Information Based on Permitted Purposes:*** Participants’ end users may only request information through the NHIN for “permitted purposes.” Permitted purposes include treatment, limited purposes related to payment, limited health care operations with respect to the patient who is the subject of the request, specific public health

⁷⁶ See *infra* notes 60 – 64 and accompanying text.

⁷⁷ *Overview, supra* note 67, at 1.

⁷⁸ *Id.*

⁷⁹ *Id.*

activities, quality reporting for “meaningful use,” and disclosures based on an authorization from the individual.⁸⁰

5. ***Duty to Respond:*** Participants who 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.⁸¹

6. ***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.⁸²

7. ***Duties of Requesting and Responding Participants:*** Each participant has certain duties when acting as a requesting or a responding participant. Under the “autonomy principle” each participant must apply its own local policies before requesting data from other participants or releasing data to other participants.⁸³

(a) When responding to a request for data, participants must apply their local policies to determine whether and how to respond to the request.⁸⁴

(b) The responding participant--the entity disclosing the data--has the responsibility to ensure 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

⁸⁰ *Id.*

⁸¹ *Overview, supra* note 67, at 1.

⁸² *Id.* at 1-2.

⁸³ *Id.* at 2.

⁸⁴ *Id.*

applicable to the responding participant.⁸⁵ This policy is essential for nationwide HIE given the number of different state laws, federal statutes and local policies governing consent or authorization to exchange data for treatment purposes. The DURSA adopts the HIPAA Privacy and Security Rules as the minimum standards for exchange of health information in a manner that protects the privacy, confidentiality and security of the data.⁸⁶

(c) 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 purposes.⁸⁷ Responding participants are expected to remain current on the legal requirements to which they are subject and take steps to comply with those laws.⁸⁸ Responding participants, who are subject to more restrictive laws, must obtain consent or authorization necessary under their applicable laws before sending data through the NHIN. Requesting participants, usually healthcare providers, will not have the responsibility for obtaining consent or authorization because it is not feasible for the requesting healthcare provider to keep track of the rapidly changing laws and regulations in every state.⁸⁹ Further, it is unlikely that patients would know what specific consent forms may be required for data exchange by their local HIE.⁹⁰ It is not reasonable to require requesting participants to obtain a consent or authorization that complies with the responding participant's applicable law.⁹¹ To do so would create an undue burden on requesting participants and require them 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.⁹²

(d) As explained in Paragraph III.B.7(c) above, generally, requesting participants are *not* obligated to send a copy of an

⁸⁵ *Overview, supra* note 67, at 2.

⁸⁶ *Id.* at 2.

⁸⁷ *Overview, supra* note 67, at 2.

⁸⁸ *Id.* at 2.

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ *Overview, supra* note 67, at 2.

⁹² *Id.*

authorization or consent when requesting data for treatment purposes. There is an exception, however. When a request is based on a purpose for which authorization is required under HIPAA, such as for psychotherapy notes, the requesting participant must send a copy of the authorization along with the request for data.⁹³

8. Participant Breach Notification: When a participant has reason to believe that a breach involving the unauthorized disclosure of data through the NHIN has occurred, the participant must report such suspected breach to the NHIN Coordinating Committee⁹⁴ and all other affected participants within one (1) hour of discovering the suspected breach.⁹⁵ After determining that a breach has occurred, a participant must notify the NHIN Coordinating Committee and other affected participants as soon as reasonably practicable, or within twenty-four (24) hours of determination that the breach occurred.⁹⁶ The notification should include sufficient information for the NHIN Coordinating Committee to understand the nature of the breach. Participants must take steps to mitigate the breach and implement corrective action plans to prevent such breaches from occurring in the future.⁹⁷ This process is not intended to address any obligations for notifying consumers of breaches; it simply establishes the participants' obligation to notify each other when breaches occur to facilitate an appropriate response.⁹⁸

9. Mandatory Non-Binding Dispute Resolution: Because disputes that arise between participants may be relatively complex and unique, participants must agree to participate in a mandatory, non-binding dispute resolution process.⁹⁹

10. Allocation of Liability Risk: With respect to liability, each participant acknowledges that it is responsible for its own acts or omissions and not for the acts of other participants.¹⁰⁰ Each participant is responsible for harm caused to other participants through acts or omissions

⁹³ *Id.* at 2.

⁹⁴ The NHIN Coordinating Committee is responsible for planning, building consensus, and pursuing consistent approaches to developing, implementing and operating the NHIN. It plays a key role in the NHIN breach notification process; dispute resolution; participant membership, suspension and termination; and NHIN operating policies and procedures. It is also it is responsible for informing the NHIN Technical Committee when proposed changes to interface specifications have a material impact on participants. *Id.* at 2.

⁹⁵ *DURSA*, *supra* note 69, at 18.

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ *Overview*, *supra* note 67, at 2-3.

⁹⁹ *Id.* at 3.

¹⁰⁰ *DURSA*, *supra* note 69, at 23.

of individuals who access the NHIN, either 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, to the extent that the individual's access was caused by the participant's breach of the Trust Agreement or its negligent conduct for which there is a civil remedy under the participant's applicable state law.¹⁰¹ This provision, however, is not to be construed as a hold harmless or indemnification provision.¹⁰²

11. *Applicable Law:* DURSA reaffirms each participant's obligation to comply with "Applicable Law."¹⁰³ As defined in the DURSA, "Applicable Law" for non-federal participants shall mean all applicable statutes and regulations of the state(s) in which the participant operates and any applicable federal statutes, regulations, standards and policy requirements.¹⁰⁴ For federal participants, it means all applicable federal statutes, regulations, standards and policy requirements.¹⁰⁵

12. *NHIN Coordinating Committee Has Oversight Authority:* DURSA confirms that the participants agree that the NHIN Coordinating Committee (NHIN CC) will provide oversight and facilitate continued development, implementation, and operation of the NHIN by conducting certain itemized activities, including playing a key role in NHIN breach notification, dispute resolution, participant membership, suspension and termination, and development of NHIN operating policies and procedures.¹⁰⁶

C. DURSA is a Living Agreement

An executable DURSA was developed and executed by an initial set of five (5) signatories in December 2009 for the purpose of establishing the legal framework to support an operational NHIN.¹⁰⁷ Interested potential participants who want to be signatories to the DURSA and exchange PHI with other DURSA participants must

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.* at 4.

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 2.

¹⁰⁷ *DURSA*, *supra* note 69, at 29 and Attachment 4.

submit an application to the NHIN Coordinating Committee.¹⁰⁸ New participants must execute the DURSA Joinder Agreement as they join the NHIN.¹⁰⁹

IV. RECOMMENDATIONS FOR TRUST AGREEMENT FOR TEXAS HEALTH INFORMATION EXCHANGES

Key Points

- DURSA may serve as the model basis for effective Texas HIEs, but would require some modifications and potentially some additional provisions.
- The modifications and additional provisions could address:
 - Issues concerning data segmentation and its implications in an HIE, if applicable;
 - Participant indemnification requirements;
 - Imposition of monetary penalties for violators of the trust agreement;
 - HIPAA compliance expectations for business associates;
 - Texas medical records privacy laws; and
 - Designation and duties of managing/technical oversight committees.

Although the DURSA was developed for a specific purpose--to establish the legal framework and support the trust framework for a nationwide NHIN network of networks --the ONC, nevertheless, placed it in the public domain for others to review, modify and use in other types of exchange models.¹¹⁰

With some modifications, the key DURSA provisions, as outlined above in Section III, could effectively serve as a model basis for an HIE trust agreement in Texas. Additional provisions, however, may be necessary to effectively address certain challenging issues that may arise in any HIE, such as the issues of (1) data segmentation and the implications it would create in an HIE, (2) whether to include an indemnification provision, and (3) whether and to what extent penalties should be imposed on the violators of the trust agreement who misuse or inappropriately disclose protected health information (PHI). Moreover, additional provisions may be necessary to outline HIPAA-related compliance expectations and requirements and to clarify operational management and technical administrative matters.

A. Issues Concerning Data Segmentation:

Some consideration should be given to the issue of data segmentation and how it will be addressed in a trust agreement for a Texas HIE. The current strategies for protecting PHI must keep pace with the increased use of EHRs and the various electronic exchange

¹⁰⁸ ONC, Health IT Home, DURSA, *Coordinating Committee Operating Policy & Procedure, Policy # CCOP&P: 1, Version 2*, at 1, Feb. 25, 2011, available through [http:// www.healthit.hhs.gov](http://www.healthit.hhs.gov).

¹⁰⁹ *Id.* at 3.

¹¹⁰ *Id.*

vehicles used to facilitate the free flow of PHI.¹¹¹ Data segmentation in a HIE may serve as a promising approach to resolve concerns about privacy of health information and to foster greater patient involvement in their health care.¹¹² However, despite the benefits and the policy rationale for segmenting data, there are many complex issues and challenges that must be overcome before segmentation can be used as a tool to empower patients with the technical means to protect specific data elements within their health record.¹¹³

1. What is Data Segmentation in the Context of Health Care?

Data segmentation within the context of an HIE, is basically defined as the process of withholding from capture, access or view certain data elements that are perceived by an individual, organization, institution, or legal entity as being undesirable to share.¹¹⁴

2. Why Segment Health Care Data?

The impetus behind protecting PHI through the use of data segmentation arises in part from the long-standing concept of patient autonomy and the need to encourage patient trust and confidence in the health care system.¹¹⁵ Another justification for protecting PHI stems from federal and state privacy laws that define and protect certain types of sensitive health information as a means to address the stigma and social hostility associated with specific health issues.¹¹⁶ The HIPAA Privacy Rule,¹¹⁷ as amended by HITECH,¹¹⁸ provides the baseline standard for privacy protection of health information. Other federal and Texas laws offer more stringent privacy protections, such as protecting health information regarding HIV status, mental health conditions, substance abuse, genetic information, minors, and incidents of intimate partner violence and sexual violence.¹¹⁹

¹¹¹ Melissa A. Goldstein and Alison Rein, *Data Segmentation in Electronic Health Information Exchange: Policy Consideration and Analysis*, at 63, Sept. 29, 2010, available through <http://www.healthit.hhs.gov>.

¹¹² *Id.* at 63-64.

¹¹³ *Id.*

¹¹⁴ *Id.*

¹¹⁵ *Id.*; see generally N.P. Terry and L.P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 UNIV. ILL. L.R. 681, 681-736 (2007).; Melissa.M. Goldstein, *Health Information Technology and the Idea of Informed Consent*, 38 J.L.M.E., 27, 27-35 (2010).

¹¹⁶ Goldstein, *supra* note 110, at 2-3.

¹¹⁷ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (1996) (HIPAA”), codified in 45 C.F.R. Parts 160 and 164.

¹¹⁸ HITECH, *supra* note 11.

¹¹⁹ Goldstein, *supra* note 110, at ES-1, ES-2.

3. ***Data Segmentation is Also Beneficial by Providing Means to Protect and Capture Certain Health Information:***

Data segmentation also provides the potential means to protect specific health data within an EHR and in the broader HIE environment. It can facilitate provider compliance with legal privacy requirements and honor patient choice.¹²⁰ Moreover, data segmentation provides the potential means for electronically capturing data in structured fields to facilitate re-use of health data for operations, quality improvement, public health and research purposes.¹²¹

4. ***Data Segmentation Poses Various Challenges in the Context of Electronic Exchange:***

Experts have identified the following four (4) key challenge areas for effectively accommodating the segmentation of health data in the context of electronic exchange:¹²²

(a) *Technical Considerations:* Segmentation policies should take into consideration technical issues. The ability to segment data within an EHR and in the context of electronic exchange depends on a number of technical factors, including the the age of the data systems, the ability to capture information in structured data fields, the application of common data definitions and terminologies for interpretation purposes, and the use of common standards for sharing information.¹²³

Data segmentation relies on documentation of information in a structured and codified manner. Older EHR data systems were designed to bring large amounts of data into the system to translate information recorded on paper into electronic format. These older systems were not designed with a focus on allowing data out of the system. Newer EHR systems on the market, however, have the capacity to capture data in a structured fashion so that it resides in a fixed, computable field

¹²⁰ *Id.*

¹²¹ *Id.*

¹²² *Id.* at 19-38.

¹²³ *Goldstein, supra* note 110, at 20-24.

and corresponds to a coding mechanism that identifies data elements, characteristics and location within a system.¹²⁴

Segmentation complications can arise when providers rely on free-text field, as opposed to structured field, documentation practices that can result in the recording of unstructured data.¹²⁵ Structured data content is capable of being categorized and organized, a crucial cornerstone that leads to consistent and standardized interpretation of data. Systems receiving data must be able to interpret it accurately to identify what has been designated as “sensitive or requiring segmentation.”¹²⁶

(b) Defining “Sensitive Information”: Many policy discussions regarding data segmentation have focused on the issue of whether and how to define the types of data should be afforded special “sensitive” treatment.¹²⁷ Should there be a strict application of the definitions for “sensitive information” or should greater subjectivity and individual autonomy be considered?¹²⁸

Patients have expressed their preference for the subjective approach with the opportunity to define, in their own terms, what information they consider to be too sensitive to expose,¹²⁹ but institutions tend to rely primarily on the federal and state privacy laws,¹³⁰ such as HIPAA, HITECH, and the other laws, referenced above in Section IV.A.2, that address the privacy of medical records and, more specifically, the privacy of certain records that have been regarded by some entities as “sensitive health information” (SHI).¹³¹

¹²⁴ *Id.* at 20.

¹²⁵ *Id.* at 21.

¹²⁶ *Id.* at 22.

¹²⁷ *Goldstein, supra* note 110, at 24.

¹²⁸ *Id.* at 25.

¹²⁹ *Id.*

¹³⁰ *Id.*

¹³¹ Consumer Partnership for eHealth, *Protecting Sensitive Health Information in the Context of Health Information Technology*, June 2010, available through <http://www.nationalpartnership.org>. The HIPAA Privacy Rule does not draw a distinction between sensitive health information (SHI) and other health information. The National Committee on Vital and Health Statistics, which is HHS’ public advisory body on health data, statistics and national information policy, has recognized certain defined categories of sensitive information. See generally National Committee on Vital and Health Statistics, *Correspondence to Kathleen Sebelius*, Nov. 10, 2010.

Although there has been considerable debate as to what constitutes SHI and whether it should be defined as a category distinct from other types of health information, SHI is generally considered to be information that carries with it unusually high risks in the event of disclosure.¹³² The sensitivity of data is often influenced by the context in which it appears.¹³³ Categories of health information often considered to be “sensitive” include information related to minors, domestic violence, genetics, mental health, reproductive care and health, substance abuse, or sexually transmitted diseases, including HIV/AIDS.¹³⁴

(c) Patient/Consumer Engagement: Segmentation policies should take into consideration the patients who will be making segmentation decisions. Patients who want to exercise their preferences for data sharing and segmentation are presumed to understand what is possible and the potential consequences of their decisions.¹³⁵ However, experts have voiced concerns about the capacity of patients to appreciate the nuances of data segmentation and articulate their preferences in a manner that could be honored by multiple diverse data holders in the health care environment.¹³⁶ Legitimate issues are whether patients have the capacity to make segmentation decisions, whether they are motivated to make such decisions, and finally whether they reasonably and logistically make the decisions.¹³⁷

(d) Provider Reluctance: Segmentation policies should also take into consideration the needs and concerns of providers as well as patients. Providers play a role in obtaining, documenting, and honoring patient preferences with respect to their personal health information. Providers also rely on the availability of accurate and relevant information to provide appropriate, quality care. Segmentation policies may compromise their concerns for ensuring safe and appropriate

¹³² *Protecting Sensitive Health Information*, *supra* note 130, at 2-3; *Correspondence to Kathleen Sebelius*, *supra* note 130, at 1.

¹³³ *Correspondence to Kathleen Sebelius*, *supra* note 130, at 1.

¹³⁴ *Protecting Sensitive Health Information*, *supra* note 130, at 2-3; *see also Correspondence to Kathleen Sebelius*, *supra* note 130, at 4-13.

¹³⁵ *Goldstein*, *supra* note 110, at 27.

¹³⁶ *Id.*

¹³⁷ *Id.* at 27-30.

delivery of health care and may raise liability and workflow implications.¹³⁸

5. *Examples of Systems Engaging in Data Segmentation:*

(a) *Patient-Controlled Segmentation Models:* At the present, only personal health record (PHR) systems offer patients the ability to apply segmentation preferences to copies of their own data and share data with specified providers.¹³⁹ Some PHR systems function as electronic repositories for medical records received from different providers, giving patients control over what records they want to share with new providers.¹⁴⁰ But, patients still do not have control over the original providers' records and documentation.¹⁴¹ Patients are not able to control the providers' documentation or the flow of information once patients release information to another entity.¹⁴² Microsoft Health Vault, Tolven, Inc., and Private Access, Inc. are examples of this type of model.¹⁴³

(b) *Provider-Controlled Models:* With this type of model, providers act as the patient's proxy in recording the patient's preferences for sharing data through the use of an EHR or other application.¹⁴⁴ Patients can communicate their preferences for segmentation, but ultimately it is left to the provider's discretion.¹⁴⁵ Some examples of this type of model include e-MDs and the Texas Department of State Health Services Clinical Management for Behavioral Health Services (CMBHS).¹⁴⁶ Some of these systems, such as the CMBHS system, operate as closed systems and do not allow for interoperable electronic exchange.¹⁴⁷

(c) *Organizational-Controlled and Hybrid Models:* With these types of models, an organization designs its policies and infrastructure to allow for standard data segmentation and

¹³⁸ Goldstein, *supra* note 110, at ES-1, ES-2.

¹³⁹ *Id.* at 39-43.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² Goldstein, *supra* note 110, at 39-43.

¹⁴³ *Id.* at ES-II, ES- III, 40-43.

¹⁴⁴ *Id.* at 44.

¹⁴⁵ *Id.*

¹⁴⁶ Goldstein, *supra* note 110, at 44.

¹⁴⁷ *Id.* at ES-III, 46.

patient consent options across all users and may execute those policies through the use of overarching or third-party application technology applied to data within the system.¹⁴⁸ Some systems utilize web-based, third-party services that offer data routing and management services while others may use third-party applications, such as consent management systems, that act as an outside rules or intelligence engine.¹⁴⁹ These models enable data segmentation with some degree of granularity through system-wide implementation of policies and procedures.¹⁵⁰ Pilot programs are in development to allow use of consent management systems to exchange health data between systems, including the Massachusetts ehealth Collaborative (MAeHC), Kaiser Permanente's system, KP Health Connect, and the Veterans Health Administration's system, Veterans Health Information Systems and Technology Architecture (VistA).¹⁵¹

6. *Are There Alternatives to Data Segmentation?*

Data segmentation not only supports patient autonomy, but it also fosters respect for patient privacy and trust--those critical elements necessary for securing patient participation in sharing their information.¹⁵² When patients lack trust in their providers, they tend to withhold information about their health.¹⁵³ Statistics from a nationwide study reveal that, nearly 50 percent of patients who know their information will be shared would either hide or

¹⁴⁸ *Id.* at 46.

¹⁴⁹ *Id.* 46, n.296.

¹⁵⁰ *Id.*

¹⁵¹ *Id.* at ES-III.

¹⁵² See generally, American Medical Ass'n, *Physician-Patient Relationship Topics: Patient Confidentiality*, <http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/patient-physician-relationship-topics/patient-confidentiality.page?>; American Medical Association Council on Ethical and Judicial Affairs, *Code of Medical Ethics* (2010-2011 ed.), available through <http://www.ama-assn.org>; see, e.g., Health IT Policy Committee, Privacy and Security Tiger Team, *Letter to David Blumenthal, Chairman of the Office of the National Coordinator for Health IT*, at 4, August 19, 2010, available at http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf (discussing the need for trust between patients and their providers as foundation to secure confidential exchange of information).

¹⁵³ See, e.g., California Health Care Foundation, *Consumers and Health Information Technology: A Nationwide Survey*, April 2010, available at <http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey>; see also additional survey results by the Markle Foundation on consumer views of health information technology found at <http://www.connectingforhealth.org/resources/surveys.html>; see also Consumer Partnership for eHealth, *Protecting Sensitive Health Information*, June 2010, at 4, available through <http://www.nationalpartnership.org/>.

consider hiding information from their physician.¹⁵⁴ Consumer organizations that focus on protecting electronic health data tend to promote solutions that would enhance patient trust generally and in the physician-patient relationship more specifically.¹⁵⁵ Data segmentation would offer a means of giving patients some control over sharing their health information and the potential for enhancing trust, and thus, autonomy and more engagement in their health care.¹⁵⁶

The alternative to data segmentation would be the exchange of the entire health record. This alternative could lead patients to engage in more protective behaviors, such as withholding “sensitive” but relevant information from their health care providers for fear that it would be shared.¹⁵⁷ Full disclosure enables a physician to diagnose conditions properly and to treat the patient appropriately.¹⁵⁸ Lack of full patient disclosure could ultimately compromise patient care.

B. Participant Indemnification Provision:

Some consideration should be given to whether an indemnification provision is desirable in a trust agreement for a Texas HIE. Parties engaged in business transactions that have inherent risks for liability exposure may typically attempt to protect themselves through the use of indemnification agreements. These agreements may serve as an effective tool for shifting risks among participants to the agreement.

1. What is an Indemnification Agreement?

In Texas, an indemnity agreement is legally defined as “[a] collateral contract or assurance, by which one person engages to secure another against an anticipated loss or to prevent him from being by the legal consequences of an act or forbearance on the part of one of the parties or of some third person.”¹⁵⁹ In simple terms, an indemnity agreement is a promise to safeguard or hold the indemnitee harmless against either

¹⁵⁴ See *Consumers and Health Information Technology: A Nationwide Survey*, *supra* note 152.

¹⁵⁵ *Id.*; Goldstein, *supra* note 110, at 4.

¹⁵⁶ Goldstein, *supra* note 110, at 4.

¹⁵⁷ See *supra* notes 152 and 153 and accompanying text.

¹⁵⁸ *Patient Confidentiality*, *supra* note 151; see also, *Code of Medical Ethics*, *supra* note 151

¹⁵⁹ *Dresser Industries, Inc. v. Page Petroleum, Inc.*, 853 S.W.2d 505, 508 (Tex. 1993) (citing Black's Law Dictionary 692 (5th ed. 1979))

existing and/or future loss, damage or injury liability.¹⁶⁰ A contractual indemnity agreement is given effect as any other contract.¹⁶¹

2. *The DURSA Excludes an Indemnification Provision:*

The DURSA expressly excludes an indemnification provision. Commentary in a draft version issued in January 2009, prior to issuance of the final version in November 2009, explained the absence of such a provision as a matter of fairness to all participants. The NHIN includes HIEs that are federal and state governmental agencies and other governmental instrumentalities. In almost all cases, governmental agencies and instrumentalities are prohibited by law from indemnifying third parties. The DURSA workgroup thought it would be unfair to ask nongovernmental HIEs to agree to indemnification when the governmental HIEs would not be subject to the indemnification provision.¹⁶²

3. *Should Indemnification Provision Be Included In Texas HIE?*

The DURSA Workgroup's rationale for not including an indemnification provision in the DURSA may need to be considered if the Texas HIE includes governmental agencies and instrumentalities. Not only would it seem unfair to ask nongovernmental entities to agree to indemnification while not requiring the same of governmental entities, but it stands to reason that, more than likely, these nongovernmental entities would not agree. Moreover, the inclusion of an indemnification provision that would apply to only nongovernmental entities would, more than likely, discourage nongovernmental participants from joining the HIE.

That said, however, the Arizona Model Health Exchange Participation Agreement¹⁶³ includes a mutual indemnification provision, under the terms of which both participants and the HIO mutually agree to indemnify and hold harmless each other for claims arising from the other party's breach of the agreement. An HIO is defined as a nonprofit or governmental organization in this model agreement. At this point, it is unclear whether any governmental entities have agreed to this Model Agreement.

¹⁶⁰ *Id.*; citing *Russell v. Lemons*, 205 S.W.2d 629, 631 (Tex. Civ. App. – Amarillo 1947, writ ref'd n.r.e.).

¹⁶¹ *Safeco Insurance Company of America v. Gaubert*, 829 S.W.2d 274, 281 (Tex. App. – Dallas 1992, writ denied).

¹⁶² NHIN DURSA Cooperative Workgroup, *Draft Data Use and Reciprocal Support Agreement*, January 23, 2009, available through <http://www.healthit.hhs.gov>.

¹⁶³ Arizona Health-e Connection, *Model Health Information Exchange Participation Agreement*, available through <http://www.azhec.org>.

C. Monetary Penalties Imposed Against Violators

Some consideration may be given to the issue of whether monetary penalties should be imposed upon violators of the trust agreement, as separate and apart from HIPAA and HITECH-imposed civil monetary penalties. The DURSA provides for a mandatory non-binding dispute resolution process as a means to resolve disputes between participants concerning unauthorized disclosures. Moreover, the DURSA provides for a suspension and termination due process procedure for: (1) participants that are in material default of a duty or obligation under DURSA, or (2) participants whose acts or omissions create an immediate threat or will cause irreparable harm to another participant or participant user, the NHIN, or individual whose information is exchanged through the NHIN. However, the DURSA does not provide for the imposition of monetary penalties which, if significant, could serve as a deterrent for violative behavior.

Neither draft versions of the Arizona Model Health Exchange Participation Agreement or the Florida Health Information Exchange Participation Agreement¹⁶⁴ reference or address monetary penalties or any other deterrent for violative behavior, other than the potential for suspension and termination from the HIE.

D. HIPAA Compliance Requirements and Business Associates Provisions

Although the DURSA cross-references HIPAA and couches all HIPAA-related compliance requirements under the definition of “Permitted Uses,” to avoid confusion and for added clarification, consideration may be given as to whether to specifically define and delineate HIPAA terms, such as “covered entity,” business associate,” “PHI,” in greater detail, especially since Texas state law defines “covered entity” more broadly than does HIPAA. Moreover, reference could be given to the Texas medical records privacy laws, both statutory and case law, as they pertain to protecting health care provider-patient confidential communications.

E. Designation of Management and Operational Committees

The DURSA grants the NHIN Coordinating Committee and the NHIN Technical Committee with a laundry list of oversight, management, and development functions. The THSA may wish to have similar designated responsibilities and authority in a Texas HIE agreement, consistent with Texas state law and Chapter 182 of the Texas Health and Safety Code. The Florida Health Information Exchange Participation Agreement, referenced above, designates and describes the responsibilities and oversight authority of the “Management Committee” as similar to that of the DURSA NHIN Coordinating Committee.

¹⁶⁴Draft Health Information Exchange Participation Agreement, *available through* <http://www.fhin.net/pdf/hiecc/Oct0110/ParticipationAgreementDraftTabE.pdf>.

KEY POLICY QUESTIONS

Should a Texas-specific model trust agreement be developed and provided for reference by HIEs in the development of their own multi-party trust agreements?

Should Texas or Texas' HIEs pursue means of data segmentation as a tool to enable enhanced patient control over disclosure of PHI or to fulfill applicable legal requirements with respect to certain PHI? If so, should the approach to employment of data segmentation in Texas HIE be reflected in a Texas model trust agreement, and if so, how?

If Texas adopts a Texas specific trust agreement, should it include an indemnification provision, provisions about specific laws, such as Texas medical records privacy laws, and/or monetary penalties for non-compliance?

How should technical and managing committees be structured? Should a single management committee be created as part of the Texas Health Services Authority? What authority should that management committee have to ensure compliance with the HIE participation agreement?

V. CONCLUSION

Trust is the cornerstone of an effective HIE. A trust agreement is an essential tool for supporting exchange of health data and for establishing and ensuring trust among the participants within an HIE. DURSA, the designated federal trust agreement for nationwide HIE through the NHIN, may serve as a model basis for Texas HIEs, but with some modifications and additional provisions. Aside from the essential core provisions in DURSA, an effective Texas HIE would need to address such issues as: whether and how to implement data segmentation; whether to include indemnification clauses; and whether to impose monetary penalties against violators of the trust agreement. Moreover, additional language could be added to clarify HIPAA compliance expectations for business associates and the designation and responsibilities of the managing and technical oversight committees for the HIE. Drafters of the trust agreement for Texas HIEs should take into account any policy considerations that may arise and effectively address such policy questions in the trust agreement.