TEXAS
e-HEALTH
ALLIANCE

Health Information Exchange
Privacy and Security Considerations

Nora Belcher, Executive Director

Texas e-Health Alliance

April 15, 2010

Senate Health and Human Services Committee

TEXAS eHEALTH ALLIANCE

Privacy and Security Considerations

- Access to personal health information
- Security of personal health information
- Protection against marketing to consumers
- Patient consent

TEXAS eHEALTH ALLIANCE

Access to personal health information

- Federal law allows individuals to choose to withhold personal health information related to services that they paid for personally.
- Individuals can request a list of all disclosures of their personal health information.
- Individuals must be notified if they are affected by a security breach.

TEXAS eHEALTH ALLIANCE

Security of personal health information

- Individuals who knowingly access, use, or disclose personal health information for improper purposes are now subject to criminal penalties.

- Existing federal law has been extended to health information exchanges.

TEXAS eHEALTH ALLIANCE

Protection against marketing to consumers

- Companies cannot use personal health information to market directly to consumers without the consumer's consent.

- Companies cannot be paid for personal health information that is shared without the consumer's consent.

TEXAS eHEALTH ALLIANCE

Importance of Consent in HIE

- The consent model selected for electronic exchange, as well as the determination of which types of health information to exchange, affects many stakeholders (e.g., patients, providers, and payers).
- These decisions also have consequences for national policy goals, such as improving the quality of healthcare, promoting public health, engaging patients in their health care, and ensuring the privacy and security of personal health.

TEXAS eHEALTH ALLIANCE

Core Consent Options

- **No consent.** Health information of patients is automatically included—patients cannot opt out;
- **Opt-out.** Default is for health information of patients to be included automatically, but the patient can opt out completely;
- **Opt-out with exceptions.** Default is for health information of patients to be included, but the patient can opt out completely or allow only select data to be included;
- **Opt-in.** Default is that no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out; and
- **Opt-in with restrictions.** Default is that no patient health information is made available, but the patient may allow a subset of select data to be included.

THSA Privacy and Security Workgroup

- **Angelyn Estwick**, Department of State Health Services. State agency representative.
- **Archibald Alexander, MD, JD, LLM**. Independent health law consultant.
- **Robert (Bud) P. Thompson, Jr. MD, FACS, PA**. Physician representative.
- **Celine Fynes**, Dell Perot Systems. Health information technology vendor representative.
- **Christy Rodgers**, Senior Director of Information Security, Tenet Health System. Hospital representative.
- **Deborah Peel, MD**, Founder and CEO, Patient Privacy Rights. Consumer representative.
- **Derek Kang, JD**, Director Compliance Services and Privacy Officer, Texas Children's Hospital. Hospital representative.
- **Diana Resnik**, Senior Vice President of Community Care, Seton Family of Hospitals. Regional health information exchange representative.
- **Edward Renteria Jr.**, Blue Cross Blue Shield of Texas. Health benefit plan representative.
- **Jennifer Reck**, Maximus. Health information technology vendor representative.
- **John Quinn**, Accenture. Health information technology vendor representative.

THSA Privacy and Security Workgroup

- **Josh De Jong**, Symantec. Health information technology vendor representative.
- **Julian Armstrong, MD**, President and Chairman of the Board, Sandlot, LLC. Regional health information exchange representative.
- **Lorraine Fernandes,** Initate Systems. Health information technology vendor representative.
- **Michael Gerleman**, Availity. Health information technology vendor representative.
- **Pamela McNutt**, Senior Vice President and CIO, Methodist Health System. Hospital representative.
- **Peter MacKoul, JD**. Health law consultant.
- **Sloane Cody**, Centene Corporation Superior Health Plan. Health benefit plan representative.
- **Susan Fenton, PhD**, Assistant Professor at Texas State University. Health information management representative.
- **Terry Turner**, Director of Information Security and HIPAA Security Officer, Harris Co Hospital District. Hospital representative.
- **Tracy Wade**, HIM Director, CHRISTUS St. Michael Health System. Hospital representative.

TEXAS
e-HEALTH
ALLIANCE

Appendix

TEXAS eHEALTH ALLIANCE

HIPAA Privacy Rule

- Applies to health plans, healthcare clearinghouses, and health care providers (i.e. "covered entities") who conduct certain financial and administrative transactions electronically that are subject to the transactions standards adopted by HHS.
- Requires covered entities to protect individuals' health records and other identifiable health information by requiring appropriate safeguards to protect privacy, and by setting limits and conditions on the uses and disclosures that may be made of such information.
- Gives individuals certain rights with respect to their health information.
- Permits a covered entity to disclose Personal Health Information (PHI) to a business associate, or allow a business associate to create or receive PHI on its behalf, so long as the covered entity obtains satisfactory assurances in the form of a contract or other agreement that the business associate will appropriately safeguard the information.
- The contract between a covered entity and its business associate must establish the permitted and required uses and disclosures of PHI by the business associate.

Additional Privacy Protections Added in the HITECH Act

- Allows individuals to request specific restrictions of the disclosures of their personal health information.
  - For example, a patient can specify that only certain health care professionals can have access to her mental health records when an individual has paid out of pocket in full for services.
  - Covered entities must honor a patient's request to withhold personal health information (PHI) from a health plan if the patient paid for the medical care.
- Extends the rights of individuals to an accounting of disclosures of health information to include electronic health records for a period of up to 3 years. Previously, the accounting requirement only extended to paper-based records.

TEXAS eHEALTH ALLIANCE

Additional Security Provisions Added in the HITECH Act

- Expands HIPAA privacy and security requirements to health information technology (HIT) entities. Previously, it was not clear that they were covered.
- Extends the HIPAA security provisions and penalties to Business Associates of covered entities.
- Mandates that health care providers enforce encryption and audit controls over all business processes involved with data transfers.
- Requires covered entities to have a business associate agreement with entities that provide data transmission of protected information, such as Regional Health Information Organizations, Health Information Exchanges, e-prescribing gateways, etc.
- Requires that covered entities must limit use or disclosure of Personal Health Information to a “limited data set” or, if needed, to the minimum necessary to accomplish an intended purpose.

Breach Notifications in the HITECH Act

Significantly strengthens breach notifications:

- Requires covered entities to notify individuals whose unsecured information (paper or electronic) has been breached; and requires business associates to notify covered entities about breaches. The notification must be provided by mail, and if urgent, by telephone.
- If more than 500 individuals are affected by a single breach, DHHS and the media must be notified. If fewer than 500 individuals are affected by a breach, that information must be included in a log submitted annually to DHHS.

Penalties Added in the HITECH Act

- Prohibits covered entities from receiving payment for communicating with patients for marketing purposes without the specific authorization of the patient (including fundraising solicitations).
- Increases civil penalties for HIPAA violations and creates different tiers for unintentional, reasonable causes and willful neglect that result in a breach or noncompliance.
- Subjects employees of covered entities or other individuals who knowingly access, use, or disclose PHI for improper purposes to criminal penalties.

Penalties Added in the HITECH Act

- Allows state Attorneys General to bring civil action on behalf of a state's residents for HIPAA violations.
- Increases civil penalties for violations under HIPAA, depending on the conduct. The federal government must impose penalties if the violation of the conduct was willful. State attorneys general (most of whom already have the jurisdiction to prosecute under state privacy laws) are authorized to prosecute and seek civil penalties.
- Requires periodic audits to ensure that covered entities and business associates are in compliance with the requirements of the HITECH Act.