June 2011

Texas Health Care Providers and Insurers Face New Mandates and Increased Penalties Regarding Electronic Health Records

Texas health care providers and insurers face new mandates and increased penalties over the use of electronic health records (EHR) as a result of HB300, which was passed in the 2011 Texas legislative session and signed into law by Governor Perry. The Texas legislation expands privacy rights of patients beyond that contained in federal HIPAA legislation and regulation. The new law, which is not effective until September 1, 2012, is designed to better ensure the security and privacy of protected health information (PHI) that is exchanged via electronic means. However, the law will also increase mandates on covered entities (health care providers and health insurers), grant new enforcement authority to a variety of state agencies, establish standards for the use of EHR, and increase penalties for the wrongful electronic disclosure of PHI, including creating a new felony for the wrongful accessing or reading of EHR via electronic means. With the recently increased federal enforcement activity regarding patient privacy, covered entities in Texas can expect similar enforcement action from state agencies as well.

Covered Entities in Texas Must Conduct Patient Privacy Training

Covered entities (which include health care providers, health insurers and health care clearinghouses) will be required to provide training to their employees regarding state and federal law concerning PHI[1]. The training must be customized as to the entity's particular course of business and each employee's scope of employment. An employee must complete the training no later than the 60th day after the employee is hired, and such training must be repeated at least once every two years. Additionally, all covered entities must maintain records documenting each employee's attendance at training programs. Such records may be maintained either electronically or in writing.

This training requirement is an expansion of the duties placed on covered entities under the federal HIPAA legislation and corresponding HIPAA Security and Privacy Rules.

Increased Patient Rights and Remedies Over Electronic Health Records

The Texas Legislature granted patients additional rights and remedies concerning their EHRs. Covered entities must provide patients their EHRs in electronic format within 15 business days of receiving a written request[2]. The Texas Health and Human

1Section 181.101, Texas Health and Safety Code

2Section 181.102, Texas Health and Safety Code

Services Commission is to recommend a standard format for the release of EHRs that is consistent with federal law. Additionally, the Texas Attorney General is required to establish a website containing information for patients regarding patients' medical privacy rights under federal and state law, a list of state agencies that regulate covered entities, detailed information regarding each agency's complaint enforcement process and contact information for each such agency. The Attorney General must also report annually to the Texas Legislature the number and types of complaints received by state agencies regarding patient complaints over medical privacy.

HB300 also prohibits the sale of PHI, except for treatment, payment and health care operations, consistent with existing provisions in the federal HIPAA statute and privacy Rule, as amended by the 2009 HITECH Act[3].

Although the HB300 is not effective until September 1, 2012, covered entities should begin planning now to provide the required training for all of their employees. Such training will have to be customized to reflect each employee's scope of employment and the particular course of business of each entity. Covered entities will also have to provide notice to, and authorization from, patients of the electronic disclosure of their PHI, except in instances for treatment, payment or health care operations. The Texas Attorney General will adopt a standard for authorization of such disclosures, consistent with HIPAA and the federal Privacy Rule.

Increased Enforcement Penalties

The Texas Attorney General may institute penalties against covered entities that violate state laws regarding patient privacy. Penalties can range from $5,000 to $1.5 million annually for providers that wrongfully disclose a patient's PHI[4]. In determining the amount of penalty, the law provides that a court should consider:

- The seriousness of the violation;
- The covered entity's compliance history;
- Whether the violation poses a significant risk of financial, reputational, or other harm to the patient;
- The amount necessary to deter future violations; and
- The covered entity's efforts to correct the violation.

3Section 181.153, Texas Health and Safety Code

4Section 181.201, Texas Health and Safety Code

Additionally, the Texas Attorney General may request that the Secretary of the U.S. Department of Health and Human Services audit a covered entity's compliance with federal HIPAA and Privacy Standards. If the audit shows egregious violations that constitute a pattern or practice, a covered entity may be required to conduct a risk analysis as required under the Privacy Rule,[5] and submit the results to the Texas Health and Human Services Commission. The Texas Attorney General will also have to report annually to the Legislature the number of federal audits of covered entities.

Standards for Electronic Sharing of PHI

In earlier legislative sessions, the Texas Health Services Authority (THSA) was created as a public-private collaborative to implement state-level health information technology functions and to serve as a catalyst for the development of a seamless electronic health information infrastructure. HB 300 adds to the duties of the THSA by requiring it to develop privacy and security standards for the electronic sharing of PHI.[6] The THSA will also establish a process by which a covered entity can be certified for compliance with the standards it develops.

Notification Requirements

Under HB300, *any* business (not just a covered entity) that conducts business in Texas that handles PHI must provide notification to Texas residents if their PHI is wrongfully disclosed. This notification requirement is in addition to the notification required in HIPAA and the federal Privacy and Security Rules. Any business that fails to make the required notification is subject to state penalties that may not exceed $250,000 for a single breach. Moreover, HB300 makes it a state felony if an individual, without the consent of the patient, accesses, reads, scans, stores or transfers PHI via a scanning device or electronic payment card.

Covered Entities Should Begin Compliance Efforts Now

The new requirements placed on covered entities in Texas as a result of HB300 are numerous and extend beyond those requirements contained in HIPAA and the federal Security and Privacy Rules. Even though the effective date of the new law in not until September 1, 2012, covered entities (health care providers and health insurers) should begin now their efforts to develop and conduct employee training, change their notices of privacy practices and update policies regarding the security and privacy of patients' protected health information.

---

545 C.F.R. Section 164.308(a)(1)(iii)(A)

6Section 182.108, Texas Health and Safety Code