Updates to the Texas Medical Privacy Act: How Texas Covered Entities Should Prepare

By George R. Gooch, J.D., LL.M. candidate (Health Law)
grgooch@central.uh.edu

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to act as a floor for medical privacy upon which states may expand. As intended, federal enforcement has been limited; the Department of Health and Human Services issued its first penalty enforcement in February 2011. Texas was one of the first states to expand upon HIPAA protections by implementing a medical privacy bill of its own in 2001.

Since that time, the adoption of health information technology (HIT) has presented new challenges to keeping sensitive health information private, and out of the hands of those seeking to profit from the sale and purchase of protected health information (PHI). Texas reacted this past legislative session by passing House Bill 300, intended to respond to advances in HIT by greatly expanding patient protection of and access to sensitive health information, while increasing penalties for violations of the Medical Privacy Act. These provisions take effect on September 1, 2012. This paper should act as a guide to inform Texas covered entities on how to prepare for changes to the Texas Medical Privacy Act.

To Whom does the Texas Medical Privacy Act apply?

The Texas Medical Privacy Act applies to all “Texas covered entities,” a term more broadly defined than HIPAA’s covered entities. HIPAA covered entities include healthcare providers, healthcare clearing houses, health plans, and any of their business associates. Texas, on the other hand, defines a covered entity in several ways, the most encompassing of which states that a covered entity is “any person who . . . comes into possession of protected health information.” PHI generally includes any individually identifiable health information about a patient. Therefore, any business entity in Texas that handles PHI should at the very least be aware of updates to the Texas Medical Privacy Act.

3 Senate Bill 1754, 77th Leg., (Tex. 2001).
4 House Bill 300, 82d Leg., (Tex. 2011). (hereinafter “H.B. 300”)
5 Id.
6 Tex. Health & Safety Code §181.001(b); See also HIPAA, supra note 1.
7 See HIPAA, supra note 1.
9 See HIPAA, supra note 1.
10 See H.B. 300, supra note 4.
What exactly changed?

The 82nd Texas Legislature updated the Texas Medical Privacy Act in several ways. For purposes of this paper, however, only those provisions for which Texas covered entities need to change routine business practices will be addressed.\(^{11}\)

First, Texas health care providers will be required to provide a patient’s medical record in electronic format within 15 days of request.\(^{12}\) Please note that this does not apply to all Texas covered entities – only to health care providers, as that term is defined by HIPAA.\(^{13}\) This new timeline is only half the time currently allowed under HIPAA.\(^{14}\) The health care provider does not have to provide the patient’s record in electronic format if the patient requests it in another form, or if the provider does not have an electronic health record system capable of fulfilling the request.\(^{15}\)

Second, Texas covered entities will be required to provide a training program to their employees regarding state and federal medical privacy laws as they relate to the entity’s particular course of business and each employee’s scope of employment.\(^{16}\) At first glance, this seems as if it requires anyone who comes in contact with PHI to conduct an expensive training session on state and federal medical privacy law. However, because the training is tailored by the course of business (i.e., businesses that customarily handle PHI), most entities that this provision applies to are likely also HIPAA covered entities, and already have a training program in place for employees.\(^{17}\) Furthermore, because the training is tailored to the scope of employment, covered entities will not have to train every single employee (e.g., the janitor) on how to properly access PHI.\(^{18}\) Because the training should be specifically tailored by entity, and again by employee, a standard training program is not provided. However, providing employees who handle PHI with the updates to the Texas Medical Privacy Act and the current updates to HIPAA should be considered essential.\(^{19}\)

Third, Texas covered entities will be prohibited from selling PHI, except in limited circumstances.\(^{20}\) A Texas covered entity may sell a patient’s PHI to another covered entity for purposes of treatment, payment, health care operations, insurance functions, or any other purpose

\(^{11}\) Please note that this paper represents only the tip of the iceberg regarding updates to the Texas Medical Privacy Act. For more information please reference the Texas Legislature’s website, available online at http://www.legis.state.tx.us.

\(^{12}\) See H.B. 300, supra note 4.

\(^{13}\) See 45 C.F.R. §164.103; also, please note that any term not defined under the Texas Medical Privacy Act adopts the definition used under HIPAA. Because a “health care provider” is not defined in the Texas Medical Privacy Act, it automatically adopts the definition used under HIPAA.

\(^{14}\) See H.B. 300, supra note 4.

\(^{15}\) Id.

\(^{16}\) Id.

\(^{17}\) Id.

\(^{18}\) Id.

\(^{19}\) See H.B. 300, supra note 4; See also Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-05, tit. IV, §§ 4101-02, 123 Stat. 467, 467-68, 477-78 (codified at 42 U.S.C. §§ 1395w-4, 1395ww).

\(^{20}\) See H.B. 300, supra note 4.
authorized or required by state or federal law. Unless the sale of PHI under these limited exceptions is meant to cover the cost of transmitting the information for legitimate purposes for carrying out the health care needs of the patient. In all actuality, this provision should not change any essential business function of Texas covered entities already complying with HIPAA. Covered entities looking to profit from the sale of PHI, on the other hand, may want to be on the lookout.

Fourth, House Bill 300 will require Texas covered entities to provide notice to individuals for whom the covered entity creates or receives PHI if the individual’s information is subject to electronic disclosure. Texas covered entities may provide this notice by posting it in the covered entity’s place of business, on its website, or any other conspicuous place where patients are likely to see the notice. There are limited exceptions to this authorization requirement identical to the provision banning the sale of PHI.

Finally, Texas covered entities should be aware of updates to Texas breach-notification laws. Currently, a person who conducts business in Texas and owns or licenses computerized data that includes sensitive personal information must disclose any breach of system security, after discovering or receiving notification of the breach, to any Texas resident whose sensitive personal information was, or was reasonably believed to have been, acquired by an unauthorized person. House Bill 300 changes this provision to require Texas covered entities to provide notification of a breach to any individual whose sensitive personal information was, or was reasonably believed to have been, acquired by an unauthorized person. To clear up any confusion between the breach-notification laws of different states, Texas covered entities may satisfy Texas breach-notification law by complying with either Texas breach-notification laws or the breach-notification laws of the state in which the person whose PHI has been breached resides.

Increased Penalties: Civil and Criminal

Texas covered entities should be aware of the above-listed provisions, and ready to change current business models to comply with those provisions. Increased penalties, on the other hand, should not change any day-to-day business, but Texas covered entities should still be aware of them.

Increased Civil Penalties

Currently, the Texas Attorney General may assess a $3,000 civil penalty against Texas covered entities for each violation of the Texas Medical Privacy Act. Once House Bill 300 takes effect, tiered penalties may be implemented as follows: $5,000 for each violation.

---

21 Id.
22 Id.
23 Id.
24 Id.
26 See H.B. 300, supra note 4.
27 Id.
committed negligently; $25,000 for each violation committed knowingly or intentionally; and $250,000 for each violation committed knowingly or intentionally for financial gain.  

While these increases may seem steep, they are coupled with several caps and mitigating factors. For example, violations under the first two tiers are capped annually, meaning the cap remains the same, regardless of how long the violation continues within one year. Furthermore, all the penalties listed above may not exceed $250,000 if the covered entity meets certain criteria showing it instilled proper measures to safeguard PHI. Finally, when assessing penalties, the court must consider several mitigating factors such as the seriousness of the violation, the covered entity’s compliance history, the risk of harm to those whose PHI are involved in the transaction, whether the Texas Health Services Authority has certified the covered entity for standards regarding the electronic exchange of PHI, the amount necessary to deter future violations, and efforts to correct the violation. So, while penalties have the potential to get much higher than before, good actors may shield themselves from excessive liability by implementing policies and procedures to safeguard PHI.

**Increased Criminal Penalties**

In addition to increased civil penalties, House Bill 300 also increases criminal penalties for identity theft involving PHI. Currently, a person using a scanning device or re-encoder to access, read, scan, store, or transfer information encoded on the magnetic strip of a payment card without the consent of an authorized user of the payment card and with intent to harm or defraud another is subject to a Class B misdemeanor. After House Bill 300 takes effect, a person committing this same act to access PHI will be subject to a state jail felony.

**Conclusion**

Advancements in health information technology increase ease of access to PHI not only for those who should have access to the information, but also for those who should not. Increased vulnerability of health information requires increased protection. The Texas Attorney General will now be much better equipped to combat those mishandling patients’ sensitive health information. Texas covered entities have nearly a year to prepare for the updates to the Texas Medical Privacy Act that go into effect September 1, 2012. Be prepared or be ready to go to court.

---

29 See H.B. 300, supra note 4.
30 Id.
31 Id.
32 Id.
33 Id.
34 Id.
36 See H.B. 300, supra note 4.