

Don't Mess with Privacy in Texas - A Summary of the New Texas Privacy Laws Concerning Health Information

11.01.11

In May of 2011, Texas passed House Bill 300, which amends the Texas Health and Safety Code and contains privacy requirements that are more stringent than the federal privacy requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In particular, the new Texas law imposes requirements regarding (i) training; (ii) electronic health records access; (iii) sales of protected health information; (iv) notice and authorization for electronic disclosures; (v) enforcement and disciplinary actions; and (vi) audits of covered entities. This new Texas law is effective on September 1, 2012.

By way of background, currently the Texas Health and Safety Code contains an expansive definition of a "covered entity," which is broader than HIPAA's definition. Under HIPAA, a covered entity is a health plan; health care clearinghouse; or health care provider who transmits any health information in electronic form in connection with a transaction.¹ In addition, the Health Information Technology for Economic and Clinical Health Act resulted in business associates, as defined under HIPAA, having to comply with many of the HIPAA privacy and security requirements in the same manner as covered entities.²

Under Texas law, a covered entity includes any person who for financial gain engages in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information.³ This term includes business associates, health care payers, governmental units, computer management companies, schools, health researchers, health care providers, and internet site providers; who come into possession with or obtain or store protected health information; as well as their employees, contractors or agents.⁴ As a result, a broad array of people and companies, beyond those directly covered by HIPAA, are subject to the Texas law, which is summarized below in more detail.

Training

According to the new Texas law, each covered entity must train its employees on state and federal laws regarding protected health information no later than the 60th day after the employee is hired.⁵ All employees must receive this training at least once every two years.⁶ Each employee must sign a statement verifying the employee's training.⁷ The covered entity must maintain these signed statements.⁸ Although HIPAA requires covered entities to train their employees on privacy and security, HIPAA does not provide specific timelines for such training.

Consumer Access to Electronic Health Records

The new Texas law requires a health care provider that uses an electronic health records system to provide, within 15 business days of a written request, a record in electronic form to the individual, to whom the record relates, unless such individual agrees to accept the record in another form.⁹

Sale of Protected Health Information

Under the new law, a covered entity may not disclose an individual's protected health information to anyone in exchange for remuneration.¹⁰ However, there are exceptions. A covered entity may disclose in exchange for remuneration an individual's protected health information to another covered entity for the purpose of (i) treatment; (ii) payment; (iii) health care operations; (iv) performing an insurance or health maintenance organization function; or (v) as otherwise authorized or required by state or federal law.¹¹

Notice and Authorization Required for Electronic Disclosures of Protected Health Information

If the individual's protected health information is subject to electronic disclosure, the new law requires a covered entity to provide notice of such electronic disclosure to the individual, who is the subject of the disclosure.¹² The notice may be posted (i) via a written notice in the covered entity's place of business; (ii) on the covered entity's internet website; or (iii) in any other place where the individual, whose protected health information is subject to electronic disclosure, will likely see the notice.¹³

In addition, a covered entity may not electronically disclose protected health information without obtaining an authorization from the individual or the individual's representative.¹⁴ The authorization may be in written, electronic, or oral form; if the covered entity documents it in writing.¹⁵

There are exceptions to this requirement. The authorization for electronic disclosures is not required if the disclosure is made to another covered entity for the purpose of (i) treatment; (ii) payment; (iii) health care operations; (iv) performing an insurance or health maintenance organization function; or (v) as otherwise authorized or required by state or federal law.¹⁶ Sound familiar? In the future, the Texas Attorney General will be adopting a standard form of authorization, which must comply with these Texas requirements as well as HIPAA.¹⁷

Enforcement and Disciplinary Actions

The new Texas legislation changed the amount of civil penalties for violations of the original Texas privacy law. For example, civil penalties for each negligent violation increased from \$3,000 to \$5,000 and up to \$25,000 for each knowing or intentional violation.¹⁸ If the violations occur with a frequency as to constitute a pattern or practice, the court will be able to assess a civil penalty of up to \$1.5 million annually.¹⁹ Prior to the new Texas law, the total penalty could not exceed \$250,000.²⁰

Currently, a covered entity is also at risk for disciplinary proceedings, probation, or suspension by a licensing agency, as well as revocation of its license for a violation of the Texas law.²¹ However, under the new law, a violation also may result in the referral of the covered entity's case to the attorney general for potential civil penalties.²²

Audits of Covered Entities

Finally, the new Texas law provides that the Commission of Health and Human Services (the "Commission"), in coordination with the Texas Attorney General, the Texas Health Services Authority, and the Texas Department of Insurance (i) may request the U.S. Secretary of Health and Human Services to conduct audits of various covered entities to determine compliance with HIPAA; and (ii) shall monitor and review periodically the results of such audits.²³ In addition, if the Commission merely has "evidence" that a covered entity committed violations of the Texas law that are egregious and constitute a pattern or practice, the Commission may require the covered entity to submit to the Commission the results of a risk analysis conducted by the covered entity (if such risk analysis was required under the HIPAA Security Standards); or request a licensing agent, as applicable, to conduct an audit of the covered entity's system to determine compliance with the Texas law.²⁴

So, not only is the new Texas law more stringent than HIPAA, it requires Texas agencies to coordinate privacy and security law enforcement efforts with federal agencies. As a result, organizations subject to HIPAA and/or the new Texas law have a number of new compliance steps to implement by September of 2012 or else face enforcement by both state and federal agencies.

Cheryl Camin Murray is a Shareholder in Winstead's Healthcare Industry Group as well as the Corporate, Securities/Mergers & Acquisitions Practice Group. Her practice focuses on health care matters, advising providers and businesses on entity formation and structural, contractual and regulatory health care issues. Cheryl's experience includes counseling clients on fraud and abuse, illegal remuneration, HIPAA, the HITECH Act, and Stark Law matters as well as compliance with other state and federal health laws. She speaks and trains clients on technology, HIPAA privacy and security, and compliance. Cheryl has authored and co-authored numerous publications on health law, HIPAA compliance and e-health issues.

Disclaimer: *Content contained within this news alert provides information on general legal issues and is not intended to provide advice on any specific legal matter or factual situation. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel.*

¹ 45 C.F.R. § 160.103.

² Under HIPAA, a business associate is defined as a person or entity who, on behalf of a covered entity, but other than in
winstead.com

the capacity of a member of the covered entity's workforce, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information (or in other words protected health information). 45 C.F.R. § 160.103.

³ Texas Health and Safety Code, Section 181.001(b)(2).

⁴ *Id.*

⁵ Texas Health and Safety Code, Section 181.101.

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ Texas Health and Safety Code, Section 181.102.

¹⁰ Texas Health and Safety Code, Section 181.153.

¹¹ *Id.*

¹² Texas Health and Safety Code, Section 181.154.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ Texas Health and Safety Code, Section 181.201.

¹⁹ *Id.*

²⁰ *Id.*

²¹ Texas Health and Safety Code, Section 181.202.

²² *Id.*

²³ Texas Health and Safety Code, Section 181.206.

²⁴ *Id.*