HIPAA Law Alert

Legal developments affecting HIPAA and medical privacy

A publication of Nixon Peabody LLP

JULY 21, 2011

New Texas health care privacy law more stringent than HIPAA

By Linn Freedman and Christopher Browning

Texas House Bill 300 (HB 300), recently signed into law by Governor Rick Perry, mandates new patient privacy protections and harsher penalties for privacy violations related to electronic health records (EHR). The requirements of the Texas law are more stringent than those of its federal counterpart, the Health Insurance Portability and Accountability Act ("HIPAA").

Under the Texas law, covered entities (health care providers, health insurers, and health clearinghouses) must provide customized employee training regarding the maintenance and protection of electronic protected health information (PHI). Covered entities are required to tailor the employee training to reflect the nature of the covered entity's operations and each employee's scope of employment as they relate to the maintenance and protection of PHI. New employees must complete the training within 60 days of hire and all employees must complete training at least once every two years. Covered entities must maintain training attendance records for all employees.

The Texas law requires covered entities to provide patients with electronic copies of their EHR within fifteen days of the patient's written request for the records. This provision of the Texas law reduces the timeframe a covered entity has to produce EHR following a patient's request from thirty days under HIPAA. The law charges the Texas Health and Human Services Commission with establishing a standard format for releasing patient EHR that is consistent with federal laws.

HB 300 also requires the Texas Attorney General (AG) to establish and maintain a website that states and explains patients' privacy rights under Texas and federal law. The website will list the state agencies that regulate covered entities, and provide the agencies' contact information and each agency's complaint enforcement process. Under the new law, the AG must issue an annual report regarding the number and types of complaints pertaining to patient privacy issues.

In a provision that mirrors provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the new law prohibits covered entities from selling PHI except to another covered entity for purposes of treatment, payment, health care operations, insurance functions, or any other reason not prohibited by applicable federal law. The sale cost may not exceed the cost of preparing and transmitting the data.

The new law contains severe civil penalties for violations of the law. Penalties can range from $5,000 up to $1.5 million per year for unlawful disclosure of a patient's PHI. In determining an appropriate penalty, the statute allows a court to consider five factors: the seriousness of the violation; the entity's compliance history; the risk of financial, reputational, or other harm to the affected patient(s) caused by the violation; the amount necessary to deter future violations; and any efforts taken by the covered entity to correct the violation.

If a violation is found to be negligent, it can cost up to $5,000 per violation each year the violation persists. Knowingly or intentionally violating disclosure laws can cost $25,000 per violation each year it persists. If the violation is known or intentional and produces financial gain, the penalty can reach $250,000 per violation each year that it persists. If the court finds that the violations are a "frequent pattern of practice," a covered entity can face up to $1.5 million dollars in fines as well as license revocation, civil action from the AG, and the AG can request an audit by HHS. These penalties are in addition to the similar penalties that can be assessed by HHS under HITECH, so a covered entity could be facing fines up to $3 million per year for the same violations under state and federal law.

HB 300 also requires any business in Texas that handles PHI to provide notification to individuals of a breach of their personal information. This is consistent with the requirements of HITECH. Failure to notify individuals may result in a $100 penalty per individual each day the notice is not sent, but not to exceed $250,000. It may also be treated as a class B misdemeanor. The Texas law requires any business, not only covered entities, operating in Texas and handling PHI to provide notice to Texas patients upon discovery of an unlawful disclosure of their PHI.

The law is effective September 1, 2012, though covered entities are encouraged to begin training and implementing the new rules as soon as possible. Texas health care entities should be aware of the new law and its requirements, which are more expansive than HIPAA or HITECH. Although entities have a little over one year to work on compliance, it is prudent to commence updating policies and procedures, Notice of Privacy Practices, and employee training to ensure full compliance in advance of the deadline.

For more information, please contact:

- Linn Freedman at 401-454-1108 or lfreedman@nixonpeabody.com
- Christopher Browning at 401-454-1006 or cbrowning@nixonpeabody.com