PUBLICATION

Texas (and California) Increase Privacy Requirements [Ober|Kaler]

2012: Issue 1 - Focus on HIPAA/Privacy

By now, most providers are well aware that national privacy and security obligations exist on at least two levels. Federal statutes and regulations get the most publicity and dominate most providers' compliance programs, but state obligations often exist in addition to the more familiar federal structure of HIPAA and HITECH. Providers who do business in multiple jurisdictions must remain vigilant for changes in these state laws, which often require compliance responses unique to the state at issue, particularly in terms of timing, content and basis for notices to individuals that their personal information has been disclosed improperly. In 2012, new statutes in Texas and California will require precisely this sort of state-specific updating to existing compliance programs and procedures. The changes made in Texas are described below. An analysis of California's new law is available in "California (and Texas) Increase Privacy Requirements."

Texas's new statute (H.B. No. 300) imposes requirements on “covered entities” as that term is defined by Texas law. The statute also creates several new government task forces and tasks several existing governmental and quasi-governmental entities with additional responsibilities related to making recommendations and reports on the state's existing procedures for handling protected health information. The new Texas law takes effect September 1, 2012.

Breach Notification

Texas's breach notification provisions apply more broadly than those imposed by HIPAA. Under Texas law, a breach notification is required of any “person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information.” Breach notification requirements, accordingly, apply to a broader class than is described by the Texas (or federal) definitions of *covered entity*. *Sensitive personal information* is defined (in Texas's Business & Commerce Code) to include:

an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

social security number;

driver's license number or government-issued identification number; or

account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

information that identifies an individual and relates to:

the physical or mental health or condition of the individual;

the provision of health care to the individual; or

payment for the provision of health care to the individual.

Accordingly, Texas law applies breach notification requirements to both entities and information (such as drivers' license numbers) that would otherwise lie outside the purview of federal breach notification law. An entity may be subject to Texas's breach notification requirements, for example, even if that entity is not a covered entity or a business associate under federal law and even if the information breached is not considered protected health information.

HB 300 makes several important changes to Texas's existing breach notification requirements. The existing law, requiring that notice be issued "as quickly as possible," remains unchanged. HB 300 expands the class of persons to whom such notices must be issued, however. Previously, Texas's notice requirement extended only to "residents of the state," but HB 300 expands this class to include residents of *other* states where that state does not "not require a person [as described] to notify the individual of a breach of system security." Entities that do business in Texas, therefore, must remain aware of not only Texas's breach notification requirements, but also those of *every other state*. A company doing business in Texas that, for instance, learns of a breach that implicates records of customers who reside in Alabama (which, as of this writing, has no breach notification requirements), is obligated *by Texas law* to notify breach victims in *Alabama*.

HB 300 also increases the penalties associated with a failure to make appropriate breach notifications. In addition to the existing injunctive relief and civil penalties available to the state attorney general ($2,000 to $50,000), HB 300 provides for additional civil penalties of $100 per individual, per day that an entity "fails to take reasonable action to comply." These civil penalties are capped at $250,000 *per breach* (not per year). Further, HB 300 provides that a failure to comply with Texas's breach notification requirements is a Class B misdemeanor *unless the information breached is considered protected health information under Texas law*. In that case, a failure to conform to the state's requirements is to be considered a "state jail felony."

Ober|Kaler's Comments

Existing Texas definitions, combined with the changes made by HB 300, cast an extraordinarily wide net. *Any* entity that does business in Texas should consider the extent to which it holds *any* personal information and ensure that policies and procedures are in place to comply with the law's strict requirements.

New Obligations For Covered Entities

HB 300 does not change the existing definition of a *covered entity* under Texas law. The existing definition, however, is already broader than the federal HIPAA definition. Under Texas law, an entity is a *covered entity* and thus is subject to the state's privacy rules where it:

for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;

comes into possession of protected health information;

obtains or stores protected health information under this chapter; or

is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

The Texas definition, importantly, includes even entities that merely store protected health information *even if those entities are not health care providers and do not transmit that information electronically*. The new Texas requirements, accordingly, may apply to many entities that do business in Texas even though those entities may not be considered either "covered entities" or "business associates" of covered entities under federal law.

HB 300 takes specific note of this difference, providing that "covered entities as defined by 45 C.F.R. Section 160.103" are required to follow the federal HIPAA requirements while "covered entity, as that term is defined [by Texas law]" must follow the requirements of Texas law (including the changes made by HB 300). Under HB 300, those requirements have been expanded in several ways.

First, HB 300 requires that all covered entities provide all employees with training regarding both federal and state privacy requirements. Training must specifically address both the entity's "particular course of business" and each trained employee's "scope of employment." Training must be completed not later than the 60th day following a new employee's hire, and must be repeated at least once every two years. Employees must, when they attend training, execute a signed statement (electronically or in writing) stating that they attended the training program, and this signed statement must be "maintained" by the covered entity (though HB 300 does not specify for *how long* the statement should be maintained).

HB 300 also provides for consumer access to electronic health records in a time frame *shorter* than that provided by HIPAA. Under HB 300, a health care provider using an electronic records system "capable of fulfilling the request" must provide a person with an electronic copy (unless the requesting individual accepts an alternate form) of the person's electronic health care record *within 15 business days* of receiving a written request. HB 300 also provides that the Texas executive commissioner, in consultation with the Texas Medical Board and the Texas Department of Insurance, may recommend a standard electronic format for the release of requested health records.

Under HB 300, covered entities are prohibited from disclosing protected health information for direct or indirect remuneration. An exception is made only for those disclosures that are made to another covered entity (as defined under Texas law) for purposes of treatment, payment, health care operations, performing an "insurance or health maintenance organization function" (as described under Texas law) or for disclosures "authorized or required by state or federal law."

Finally, HB 300 provides specific requirements regarding the notice and authorizations required for the electronic disclosure of protected health information. In terms of notice, HB 300 provides that all covered entities must provide notice to individuals whose protected health information is "subject to electronic disclosure." Notice may take the form of a posting to the entity's website, in the entity's place of business, or "in any other place where individuals…are likely to see the notice."

In terms of authorizations, HB 300 requires that covered entities obtain a unique authorization *for each and every electronic disclosure of an individual's protected health information*, with several exceptions discussed below. Authorizations may be written or electronic and may even be oral, provided the entity documents any oral authorization in writing. Authorizations, however, are not required for disclosures made to another covered entity (as defined under Texas law) for purposes of treatment, payment, health care operations, performing an insurance or health maintenance organization function (as described under Texas law) or for disclosures "authorized or required by state or federal law." HB 300 provides that the Texas attorney general "shall adopt a standard authorization form for use in complying" with this requirement by January 1, 2013.

Importantly as well, this section of HB 300 does *not* apply to a covered entity (as that term is defined in Texas Insurance Code – (a definition slightly different than that cited above) unless that entity is *also* considered a covered entity under federal law. It presumably *does*, however, apply to covered entities (as defined by Texas's Health & Safety Code) which are not considered covered entities under federal law.

Ober|Kaler's Comments

Many of the HB 300 provisions track policy decisions made in the federal HITECH Act. Regulations implementing much of HITECH have not yet been issued (though they are expected soon). Providers, however, should note that they may be subject to Texas law even if they are not considered covered entities under federal law, and take appropriate steps to create and implement compliant policies and procedures.

New Penalty Provisions

HB 300 includes multiple new penalty provisions. Civil penalties for negligent violations have been increased to $5,000 per violation from $3,000. “Knowing or intentional” violations earn $25,000 penalties. A fine of $250,000 may be levied against a covered entity that “knowingly or intentionally used protected health information for financial gain.”

The total amount of the civil penalties levied against a covered entity with respect to “a violation or violations” may not exceed $250,000 annually, but only when the court finds that 1) the disclosure was made to another covered entity for a purpose that does not require an authorization; 2) the information was encrypted when transmitted; 3) the recipient did not use or release the information received; and 4) at the time of the disclosure, the covered entity had in place appropriate privacy and security policies and procedures and had properly trained the employees responsible for the information's security.

If, on the other hand, a court determines that violations have “occurred with a frequency as to constitute a pattern or practice” the court may itself assess a civil penalty not to exceed $1.5 million (annually). HB 300 provides extensive guidance regarding the factors that a court should take into account in determining an appropriate civil penalty amount.

Finally, HB 300 provides that, in addition to the above, any covered entity that is licensed by a state agency and violates the state privacy laws is also subject to investigation and discipline by the agency responsible for its licensure. HB 300 specifies that discipline for violations of state privacy laws may include the revocation of the covered entity's state license (including, presumably, professional licenses).

Ober|Kaler's Comments

Texas's new penalties follow a national trend towards increased penalties stepped to reflect the penalized party's state of mind. Entities subject to the Texas law should take note that documentation and robust procedures can serve as excellent evidence that a single noncompliant event was neither “knowing” nor part of a “pattern or practice.”

New Government Tasks (and Task Forces)

HB 300 contains several provisions tasking various parts of the Texas government with studying and making recommendations with regard to certain health information problems and creates at least one new task force. Providers may be interested in providing information to these government entities, assisting them with their

investigations, or reviewing the results of their work to get a better understanding of the Texas government's view of the state's information handling practices.

- HB 300 provides that the state Health and Human Services Commission (the "Commission") may:
  - Request that the United States Secretary of Health and Human Services conduct an audit of a covered entity (as defined by HIPAA regulations);
  - Periodically review the results of such audits;
  - Require (when an audit has revealed a pattern or practice or an egregious instance of noncompliance) that the covered entity submit to the Commission the results of a risk analysis conducted by the entity (as required under HIPAA regulations);
  - Request that the responsible licensing agency (if the covered entity is a licensed entity) audit the entity for compliance with Texas privacy laws; and
  - Report annually to the appropriate legislative bodies the number and results of audits performed and requested.
- The Executive Commissioner of Health and Human Services is tasked with reviewing amended federal HIPAA regulations (and definitions) and, taking into account the best interests of the state, determining whether the amended federal regulations should be adopted and referenced by state law. A final report of these determinations is to be provided to the legislature within 30 days of the determination.
- The attorney general is required to maintain a consumer website (to be created by May 1, 2013) that:
  - Lists the agencies that regulate covered entities along with the types of entities that each regulates;
  - Provides detailed information regarding each agencies' complaint procedures and enforcement process; and
  - Provides contact information for each agency.
- The attorney general is to provide an annual report to the legislature describing the number and type of complaints received by these agencies and the attorney general's office with regard to privacy, and the enforcement steps taken. Each listed agency is required to provide the same annual report to the attorney general with regard to the complaints it receives and the actions taken.
- The state-designated health information exchange entity (referred to in HB 300 as the "corporation") shall develop and submit to the Commission for ratification "privacy and security standards for the electronic sharing of protected health information." (HB 300 provides a series of requirements regarding these standards).
- Not later than December 1 of each year, the Commission must report to the legislature on any "new developments in safeguarding protected health information and recommendations for the implementation of the safeguards…."
- The Commission, in conjunction with the Texas Health Services Authority and the Texas Medical Board, shall review issues regarding the security and accessibility of protected health information maintained by "unsustainable covered entities" (meaning, covered entities who are no longer actively doing business). Not later than December 1, 2012, the Commission is to submit a report to the legislature including recommendations regarding:
  - The state agency to which protected health information should be transferred when a covered entity becomes unsustainable;
  - Methods to ensure security of the information at the unsustainable entity, in transit, and in storage;
  - How (and for how long) such information should be stored by the state;

  - Processes for individuals to retrieve their records when they are stored in this manner by the state; and
  - How such a program will be funded.
- HB 300 created a new task force on “health information technology.” The task force will be comprised of 11 members (at least: two physicians, two hospital representatives, one private citizen, one pharmacist, and three designated government representatives) appointed by the attorney general. The task force is to develop recommendations regarding:

  - Improvements in informed consent and authorization protocols regarding electronic exchange of protected health information;
  - Improvement of patient access to and use of electronic health information; and
  - Any other critical issues, as determined by the task force.
- The task force must submit its report to the legislature no later than January 1, 2014.

Ober|Kaler's Comments

State information technology policies and strategies often begin in task forces and similar state organizations. Providers and other interested parties who wish to have a voice in the formation of Texas' state policies should follow the workings of such groups closely and, to the extent possible, contribute in the conclusions they reach and the policies they recommend.