ReedSmith

Even Data Privacy Obligations are Bigger in Texas

Author: John L. Hines, Jr., Partner, Chicago
Author: Paul Bond, Partner, Princeton
Author: Amy S. Mushahwar, Associate, Washington, D.C.
Author: Brad M. Rostolsky, Associate, Philadelphia
Author: Frederick Lah, Associate, Princeton

Publication Date: November 17, 2011

Earlier this year, Texas Governor Rick Perry signed into law Texas House Bill (H.B. 300), which presents more stringent requirements for health privacy, data breach notification obligations, and increased fines for violations. The law will become effective September 1, 2012.

The new law adds obligations to Texas Health and Safety Code § 181.001, *et al.,* the state's law on protecting patient health information. Texas' current law applies to "covered entities," defined as any person who "for commercial, financial, or professional gain, monetary fees, or dues [ ], engages [ ] in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information." The term includes any entity who maintains an Internet site that "comes into possession of protected health information" or "obtains or stores protected health information." This definition is much broader than the definition of a "covered entity" provided under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), which only applies to health plans, health care clearinghouses, and health care providers "who transmit[ ] any health information in electronic form in connection with a transaction covered by [HIPAA]." 45 C.F.R. § 160.103(ii)(3).

Under H.B. 300 (the new Texas law), all "covered entities" - as defined under HIPAA - must comply with HIPAA. In addition, H.B. 300 imposes a number of further requirements on "covered entities," as the term is defined by the existing Texas law. Each covered entity shall provide a training program to its employees on HIPAA and Texas' health law; and the employees must complete the training within 60 days after their date of employment and subsequent training at least once every two years. The law also requires covered entities to provide notice to individuals if their personal health information is subject to electronic disclosure. It imposes civil penalties up to $5,000 for violations of the chapter committed negligently, and up to $25,000 for violations committed knowingly or intentionally. Further, the law imposes up to $250,000 for each violation in which the information was used for financial gain. Penalties may be subject to an annual cap of the same amount where certain conditions are met. Repeated violations occurring with a frequency that constitute a "pattern or practice" may be civilly liable for up to $1.5 million.

H.B. 300 also bolsters Texas' already strong data breach notification law. Under the current law, Texas Business & Commercial Code § 521.053, *et al.*, any business that "owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Most states' breach notification laws define "sensitive personal information" as an individual's first name or first initial and last name in combination with the individual's (i) Social Security Number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card in combination with any required access code or password permitting access. Texas, though, is one of a handful of states that also includes protected health information (PHI) under its definition of "sensitive personal information." In addition to the above three elements, Texas includes in its definition of "sensitive personal information" information that identifies an individual and relates to (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

Under the new law, businesses in Texas will also have to comply with a new requirement. Those businesses that suffer a data breach of any of these types of "sensitive personal information" must provide notification now to "*any individual* whose sensitive personal information was, or is reasonably believed to have been acquired by an unauthorized person" (emphasis added). In effect, this means that in the event of a breach, the business must notify Texas residents, *as well as non-residents* if the non-resident lives in a state that does not require notification to be provided to the individual in the event of a data breach. The law also provides that for those individuals residing in states outside of Texas that have breach notification laws, entities would be deemed compliant with Texas law if they provided notification pursuant to their own laws, although it remains to be seen just how Texas interprets this provision. Only four states (Alabama, Kentucky, New Mexico and South Dakota) have not passed data breach notification laws.

Also important to note in H.B. 300 is the increased penalties for violations of the new breach law. Those businesses who "fail[ ] to take reasonable action" to comply with the law will be liable to the state for a civil penalty of up to $100 for each individual to whom notification is due for each consecutive day that the business "fails to take reasonable action to comply" with the law. Civil penalties are capped at $250,000 under this provision.

* * * *

We want to note that, in addition to the above changes to Texas law, California amended its data breach notification bill earlier this year. California's amended law, S.B. 24, mandates a number of additional requirements for those California businesses that suffer a data breach, including that the attorney general be notified in the event of a breach of more than 500 California residents, and that specific content be included in the notification. In addition, the law requires that the notification be written in "plain language." The explicit requirement that "plain language" be used is the first of its kind. The California amendments will become effective January 1, 2012.

Understanding state-level data privacy obligations can be a difficult task for any company, especially when states continue to alter and update their requirements. Reed Smith has helped advise a number of companies on their data protection obligations with regard to protecting PHI and data breach notification obligations. For any questions, please contact the authors.