

p.s.

Poyner Spruill^{LLP}
ATTORNEYS AT LAW

Everything Really Is Bigger in Texas

The Lone Star State Amends Law to Require 50-State Breach Notification

09.26.2011

Jessica M. Lewis

Elizabeth H. Johnson

Texas recently enacted [House Bill 300](#) (the Law). Its primary purpose is to add significant privacy requirements to the Texas Medical Records Privacy statute, but lurking among those provisions are amendments to Texas's breach notification law which, if triggered, purport to require notice in all 50 states.

The Law applies Texas's breach notification requirements to organizations "conducting business" in the state of Texas. The Law does not define what "conducting business" in Texas means, but a business that maintains a physical presence in Texas or has regular commercial dealings with Texas residents likely will be covered by the Law.

If a covered business suffers a breach, the Law requires that breach notification be given to affected residents of Texas and affected residents of "another state that does not require [breach notification]." If the other state's law also requires breach notification, then the Texas requirements are deemed satisfied when notice is provided to the other state's residents in keeping with the other state's law. If the other state's law does not require notification, but Texas law applies (i.e., the business operates in the state, etc.) and would require notice, then breach notification will have to be provided to residents of the other state following Texas requirements for notification. The result is that breaches affecting residents of other states will have to be analyzed under both the law of the state where an affected person resides and Texas law to

p.s.

POYNER SPRUILL publishes this newsletter to provide general information about significant legal developments. Because the facts in each situation may vary, the legal precedents noted herein may not be applicable to individual circumstances. © Poyner Spruill LLP 2010. All Rights Reserved.

RALEIGH

CHARLOTTE

ROCKY MOUNT

SOUTHERN PINES

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

determine if breach notification is required.

An important difference between Texas's breach notification law and the notification laws of other states involves the type of data covered. Like most states, Texas's breach notification requirements cover "sensitive personal information," including an individual's name accompanied by the individual's Social Security number, driver's license number, government-issued identification number, or financial account number with any information that would permit access to the same. Unlike most states, Texas's requirements also cover "personally identifying information relating to an individual's physical or mental health or condition, health care provided to such individual, or payment therefore."

So if there are affected persons in Texas and other states, how do you compare laws to decide whether Texas requires breach notification in other states, even if those states would not require it? Factors to consider in that analysis may include:

- *Whether the affected state has a breach notification law* - If it does not, and Texas would have required notification in its own jurisdiction, then notification may be required in the affected state despite the absence of a breach notification law.
- *Whether the affected state covers the same type of personal information as Texas* - While the vast majority of states have breach notification laws, only a minority of those laws apply to breaches involving health or medical information. Thus, in most circumstances where health information is affected, the affected state will not cover health information, but notification may be required since Texas does cover health information.
- *Whether the stated harm thresholds (if any) are equivalent* - State laws on breach notification vary with regard to the level of risk or harm associated with the breach that triggers a notification obligation.
- *Whether the definitions of a breach are equivalent* - State laws vary in describing the types of incidents that require notification.

- *Whether HIPAA Breach Notification Rule requirements apply* - The HIPAA Breach Notification Rule does not preempt state breach notification laws if it is possible for covered entities to comply with both. As a result, in most cases, HIPAA-covered entities addressing a breach of health information must analyze and comply with multiple breach requirements, and Texas requirements will now often be relevant.
- *The impact of any required (or optional) consultation with law enforcement* - States vary in these requirements, such as by requiring consultation with agencies prior to deciding whether notice is due and/or requesting a delay related in notification as a result of a law enforcement investigation.

The Law becomes effective on September 1, 2012, and carries financial penalties for violations. A covered business may be subject to penalties for violations if the business “fails to take reasonable action to comply.” Such failures are penalized at a rate of \$100 per affected person, per day that the failure persists, up to a maximum of \$250,000 per breach. At this rate, the maximum penalty would be reached relatively easily – a breach affecting just 250 people, accompanied by a failure to take reasonable action for 10 days, adds up to a \$250,000 penalty.

The practical outcome is that any entity conducting business in Texas will have to analyze Texas breach notification requirements in essentially every potential breach affecting U.S. residents to determine whether Texas law dictates that notification is due, even in cases where information about Texas residents was not implicated in the incident.