Proskauer

# Texas Raises Stakes on Health Care Privacy

**August 30, 2011**

In May, Texas enacted a far-reaching new health information privacy law that will take effect on September 1, 2012. The new law has received limited attention to date. Entities dealing with health information, however, are well advised to take note, as the law both applies to persons to whom HIPAA does not apply and imposes requirements that go above and beyond HIPAA.

The new law applies to "covered entities" ("CEs") as that term is defined under Texas law. Texas' definition of CE includes any person who assembles, collects, analyzes, uses, evaluates, stores, transmits, or comes into possession of protected health information ("PHI"), and any employee or agent of such entities. HIPAA applies only to health care providers, health insurers, health care clearinghouses, and their business associates. Thus, the new Texas law applies in a number of circumstances where HIPAA does not. For example, potentially, the Texas law could be applied to governmental entities that come into possession of health information, schools and universities who receive health information about students such as immunization information provided in connection with enrollment, sports teams, and other employers who receive health information from an employee (but not in connection with their provision of health services or administration of a group health plan).

Notably, by its terms, there is no limit on the application of the law to persons doing business in Texas or handling the health information of Texas patients. Rather, on its face, the law appears to apply to any CE. It remains to be seen whether Texas will seek to apply the law in such an expansive manner. Such broad enforcement could give rise to challenges to Texas' jurisdiction and to the constitutionality of the law. Absent guidance, however, businesses dealing with health information, even if they do not have operations in Texas, will have to comply with the law or face the risk of enforcement.

The costs of compliance could be substantial. Among other things, the new law imposes a requirement on CEs to provide compulsory training on the law and on HIPAA to employees every two years. New employees must receive training within 60 days of their date of hire. Employees must sign a statement verifying their attendance at the training, and CEs must maintain such written verification. Although many entities provide HIPAA training, HIPAA imposes no such requirement.

The Texas law's training requirement, on its face, appears to require CEs to provide training to all employees regardless of whether they have access to or deal with the health information of Texans. This has important ramifications. First, businesses with limited exposure to health care could be required to provide training to all of their employees. For example, an information technology provider with a single client that deals with health information could be required to provide training to its entire staff, including personnel who do not provide services for the health care client. Similarly, businesses with national or international operations could be required to provide training to their entire work force. Again, without guidance, businesses that fail to comply with the broadest interpretation of the law risk adverse enforcement action.

The new law also requires CEs to provide notice to individuals for whom they create or receive PHI if the individual’s PHI is subject to electronic disclosure. The notice may be posted on a web site or in the CE's place of business. In addition, CEs cannot electronically disclose an individual's electronic health information without written authorization from the patient, except to another CE for the purposes of treatment, payment, health care operations, for the performance of insurance functions, or as required by law.

Notably, the limitation on electronic disclosures does not appear to allow disclosures pursuant to a subpoena or in connection with a litigation or investigation unless the requesting party is a CE. HIPAA allows for such disclosures (with certain limitations). Accordingly, CEs who receive government subpoenas seeking health information in electronic form may be faced with the uncomfortable task of telling the government that they cannot comply with the subpoena. Presumably, CEs may produce hard copy records under such circumstances, however, as the limitations on disclosure only apply to "electronic disclosures."

The new law includes an expansive breach notice provision that requires providers to provide breach notice even to non-Texas residents if the affected individual's state does not require breach notice. Thus, this provision may require any company doing business in Texas to provide breach notice in every state for any event that qualifies as a breach in Texas.

Finally, the Texas law provides the Texas Attorney General with broad enforcement authority. Among other things, the Texas Attorney General can institute an action to impose civil penalties of up to $1.5 million per year for violations. In addition, Texas licensing agencies are authorized to take action against entities that violate the law, including license revocation.

In sum, Texas has imposed substantial new requirements on entities that deal with health information. These requirements apply broadly to any person who comes into possession of protected health information. In addition, although its jurisdictional reach is questionable, many of these requirements can be construed as applying even to entities that do not do business in Texas, and as imposing company-wide requirements on companies with only limited Texas operations.

For the latest information on privacy law, read our Privacy Law Blog.

**Related Professionals**

- **Jeffrey D. Neuburger**
  Partner