PUBLICATION

The Trend of Stricter State Data Breach Laws Continues with Florida [Ober|Kaler]

2014: Issue 19 - Focus on HIPAA/Privacy

Florida's new Florida Information Protection Act, Fl. Stat. § 501.171, became effective July 1, 2014. The new law repeals and replaces Florida's existing data breach notification requirements (Fl. Stat. § 817.5681) with more expansive reach and enforcement in this area. The Florida Information Protection Act (FIPA) continues a trend of states enacting their own data breach and notification laws that expand beyond the scope of the federal requirements under the Health Information and Portability Act (HIPAA.).

The new law applies to *covered entities* which include all businesses and government entities that acquire, maintain, store or use personal information. The definition of *personal information* is broader than it was under the predecessor breach notification statute, as it includes not only personal identifiers and other financial information, but also health care information and health insurance policy identifiers. Further, personal information now includes "a user name or email address, in combination with a password or security question and answer that would permit access to an online account." The term *online account* is not defined and therefore may reach beyond financial or health care related accounts. Arguably it could incorporate any "account" from online retail to social media accounts.

Breaches are defined as the unauthorized access of personal information in electronic form; however, there is an exception for good faith access provided the information is not further used for an unauthorized purpose. In the event of a breach, covered entities must provide individuals with notice that meets the statute's requirements within 30 days after the determination of a breach or reason to believe a breach occurred. There is, however, an exception to the notice requirement as well as "deemed compliance." If the covered entity, after investigation by and consultation with relevant law enforcement agencies, determines that the breach has not and will not likely result in identity theft or any other financial harm to the individual, no notice to the individual is required. Further, a covered entity's notice to the individual pursuant to the rules of its "primary or functional federal regulator" is "deemed compliance" with the requirements for individual notice under FIPA. Accordingly, notice provided by a HIPAA covered entity should amount to compliance with FIPA's notice requirements to individuals. Interestingly, because HIPAA gives covered entities 60 days to provide notice, the question raised is whether HIPAA covered entities in Florida continue to have the 60-day time frame or 30-day time frame. Answering that question requires a determination of whether HIPAA's longer notice period would be pre-empted by FIPA's more stringent 30-day time frame.

This exception and "deeming" method do not apply to the requirement for notice to the Attorney General. In all circumstances, covered entities must provide notice to the Department of Legal Affairs in the event of any breach affecting 500 or more individuals within Florida. This notice must be provided within the same 30-day time period. In addition to notice to the individual and Attorney General, notice must be provided to credit reporting agencies if notice is required to more than 1,000 individuals at a single time.

FIPA does require covered entities and their third parties to institute reasonable security measures; however, the law does not go into much detail as to what constitutes reasonable measures. Regardless, those covered entities covered by HIPAA will need to adhere to HIPAA 's security requirements, while covered entities outside HIPAA's jurisdiction will have more discretion until further guidance is issued.

While FIPA does require certain compliance by a covered entity's third party agent, it does not go so far as to make the third party individually labile under FIPA, as business associates are under HIPAA. The third party must provide notice of any breach to the covered entity within 10 days; however, the notice requirements and obligations remain with the covered entity. Even if the third party agrees to provide the notices on behalf of the covered entity, failure to properly do so amounts to a violation by the covered entity, not the third party. Notwithstanding, FIPA specifically states that a third party may be subject to a deceptive trade practice claim, under Florida's Deceptive Trade Practices Act, Fl Stat. § 501.201, *et seq*. , for its involvement in the breach.

On the topic of violations, FIPA penalties for failure to provide proper notice are assessed per breach and not per affected individual. While HIPAA does not impose penalties per individual affected either, it will also take into account the specific facts of each situation in assessing the total penalties. It is not clear from the language of the law whether FIPA allows state regulators to do the same. Under FIPA, penalties are assessed per day the violation of the notice requirement continues. Regardless of the size of the breach, (i.e., whether it affects 1 individual or 10,000), or circumstances in which the breach occurred, as are considered under HIPAA, (e.g., the covered entity acted reasonably v. acted with willful disregard), covered entities are fined the same. Specifically, $1,000 per day is assessed for the first 30 days of the violation, $50,000 for each subsequent 30-day period up to 180 days, and additional amounts, not to exceed $500,000, in total, are imposed for violations lasting more than 180 days. Keep in mind these penalties are for violations of the notice requirement only. Covered entities, as well as third parties, as referenced above, may be subject to other penalties related to the practices causing the breach if such amounts to a deceptive trade practice under state law.

FIPA continues a trend among states, such as California, Texas and Massachusetts, in creating notice obligations and penalties associated with improper disclosures of personal information that not only include personal and financial information (name, Social Security number, bank account numbers) but also that include health information. If such a trend continues, so may the discussion as to a national standard. Entities that are subject to both HIPAA requirements and state disclosure requirements, or requirements of multiple states for entities that conduct business in or serve residents of multiple states, and such requirements applying to the same information may push for clarity in the form of one national standard. Until then, such businesses should take the time to review each applicable state's requirements and how those requirements overlap, abbreviate or supplement the business's obligations already imposed under HIPAA.