akerman

Practice Update

Florida Information Protection Act of 2014 - Florida Means Business When It Comes to Protecting Customers' Personal Information

July 10, 2014

By Robert Slavkin, Elizabeth Hodge, Alia Luria

On June 20, 2014, Governor Rick Scott signed into law the Florida Information Protection Act of 2014 ("FIPA"), which became effective July 1, 2014. FIPA expands the obligations of businesses and government entities that maintain data containing personal information of individuals to safeguard and provide notice of breaches of such information. As a result, Florida now has one of, if not the most strict breach notification statutes in the country.

The Act repeals § 817.5681, Florida Statutes, Florida's existing breach notification statute, and creates within Chapter 501, Consumer Protection, new statute § 501.171, Florida Statutes. While some of the language of § 817.5681 remains in the new law, FIPA makes significant changes as described below:

- FIPA expands the definition of "personal information" to include a person's first name or first initial and last name in combination with such person's health insurance information, medical information or financial account information, and now also includes a person's online account credentials.

Related People

Elizabeth F. Hodge
Robert E. Slavkin

Related Work

Corporate
Data Privacy and Security
Healthcare

Related Offices

Orlando
Tampa

- Thirty (30) day notice by covered entities to consumers after discovery of a breach or the belief that a breach occurred. Previously, businesses had up to forty-five (45) days to provide notice to affected individuals, unless, after appropriate investigation or consultation with relevant law enforcement agencies, the entity determines that the breach will not likely result in identity theft or other financial harm to any individuals. Third party agents of covered entities that have a breach must notify the covered entity no later than ten (10) days following discovery of the breach.
- In the event of a breach affecting 500 or more Florida residents, covered entities must provide notice to the Florida Department of Legal Affairs within thirty (30) days of the discovery of a breach or the belief that a breach occurred, even if the covered entity determines that a breach is not likely to result in identity theft or other financial harm to individuals. Covered entities must provide a copy of their breach policies if requested by the Department.
- Businesses and state government entities must take reasonable measures to protect data in electronic form, such as encrypting data or de-identifying the data. They must also dispose of records in a way that protects consumer information from being disclosed, such as shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.
- Entities that maintain, store, or process personal information on behalf of a covered entity or governmental entity must notify a covered entity of a breach of security no later than ten (10) days after discovering a breach or a suspected breach.
- Violations of FIPA will be treated as unfair or deceptive trade practices.
- In addition to the remedies provided under the Florida Unfair and Deceptive Trade Practice Act, a

covered entity that fails to provide notice of a breach is liable for a civil penalty for each breach of up to $1,000 per day for the first 30 days, and $50,000 for each subsequent 30-day period for up to 180 days. State governmental entities and their instrumentalities are not liable for these civil penalties for failing to timely report security breaches but are subject to notification requirements.

While the Act specifically states that it does not create a private cause of action for those affected by a breach, that does not mean there is no risk of litigation in the event of a security breach. The plaintiffs' bar is using common law theories such as negligence, breach of contract, unjust enrichment and restitution, and breach of fiduciary duty to sue for damages caused by data breaches.

What does this mean for health care entities?

In some ways, the language of § 501.171, Florida Statutes, parallels the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. For example, the threshold of 500 individuals being affected to trigger reporting to the Department of Legal Affairs is similar to the 500 individual threshold for sixty (60) day reporting on the Department of Health and Human Services breach website. Similarly, HIPAA covered entities, business associates, and subcontractors should already be familiar with the concepts of appropriately encrypting personal information and de-identifying personal information as "safe harbors" from enforcement activity.

However, there is ambiguity in FIPA as the act relates to entities that are subject to federal laws requiring breach notification. Currently, HIPAA provides covered entities up to 60 days to notify individuals of a health information breach and provides that covered entities may be able to avoid sending notice if they demonstrate that it is unlikely that the information has been compromised. Under

FIPA, to avoid notifying a patient, a health entity would first have to consult with law enforcement. There could be situations where FIPA may require notice but HIPAA does not, based on the covered entity's assessment that there is a low probability that patient information was compromised.

Also, FIPA states that if a covered entity complies with the breach notification rules and regulations of its primary or functional federal regulator, *i.e.*, HIPAA, the covered entity is deemed to have complied with the notice requirements of FIPA. However, this contradicts the requirements under FIPA that covered entities must timely provide notice of the breach to the Department of Legal Affairs, *i.e.*, within thirty (30) days of discovery of the breach or suspected breach. As implementation progresses, some of these ambiguities will be sorted out.

What does this mean for non-health care businesses?

This change does not just affect Florida healthcare-related businesses, but any business storing the information of Florida residents. All businesses doing business with Florida residents will be subject to the new, more stringent notification requirements in FIPA, and any business with a breach response plan will need to re-assess its internal compliance to make sure that it is capable of meeting the new, shortened response times required by FIPA.

What should entities conducting business with Florida customers do to comply with FIPA?

- Evaluate your current policies and security measures for electronic personal information and update them as necessary;
- Develop new policies or update existing policies for identifying breaches and providing appropriate notification to affected individuals.

- Ensure that your company is using proper methods to destroy or dispose of personal information;
- Review and update your agreements with third party agents who maintain or transmit electronic personal information to address the new requirements of § 501.171, Florida Statutes, regarding notification of breaches suffered by the third party agent and what precautions the third party agent takes to safeguard and properly destroy data.
- Review your liability policies to determine what coverage is available in the event of a breach. The cost to respond to a data breach continues to climb, and some insurers are revising their CGL policies to exclude coverage for data breaches. Separate cyber liability policies are available in the marketplace.
