Florida Information Protection Act (FIPA) of 2014: A Game Changer for Information Security

Being a Florida resident and business owner, I'm glad to see that our legislatures are taking a careful look into data security. With identity theft on the rise and the number of breaches involving personal information skyrocketing, it is refreshing to know that action is being taken to curb this activity. *But….is it enough*?

Overview

Let's take a look at the new Florida Information Protection Act (FIPA) that was unanimously passed and signed into law June 20, 2014. FIPA went into effect July 1st and covers a wide range of organizations. In basic terms, any company (including a governmental entity) that 'acquires, maintains, stores, or uses personal information' is governed by this law.

Personal Information

It is important that we define *personal information* since FIPA expands this in comparison to other related privacy and security regulations such as the Health Insurance Portability and Accountability Act (HIPAA). FIPA defines personal information as an individual's first name (or first initial) along with their last name in **combination** with any or more of the following data elements of the individual:

- A social security number;
- A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- A financial account number/credit/debit card number, in **combination** with any required security code (password) that is necessary to gain access to the account;
- Any information about the individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; **OR**
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

In addition, FIPA defined personal information to be a user name or e-mail address, in **combination** with a password or security question/answer that would permit access to an online account.

Exception of Personal Information

A major point to note about the definition of personal information is that information that is encrypted, secured, or modified by some method or technology to remove personally identifiable elements of an individual (or otherwise render the information unusable) is **NOT** considered personal information.

Unfortunately, the law doesn't go into any detail on what is acceptable encryption, security, or modification to information. As information security experts know, not all encryption is the same; nor is security standardized across all industries. In fact, the Department of Health and Human Services has issued 'Guidance Regarding Methods for De-identification of Protected Health information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule" (November 26, 2012) and also refers to FIPS140-2 standards for acceptable encryption; however, FIPA doesn't reference any such guidance for covered entities to follow.

Approach: Reactive vs. Proactive

FIPA appears to be intended to address the security of confidential personal information, but the legislatures are taking a *reactive* approach to this concern as opposed to being *proactive* in protecting our personal information. Instead of covered entities proving that they are performing their due diligence when it comes to protecting their customer records, FIPA basically addresses breach notification requirements. This notification is 'after-the-fact' when something went wrong or a company fell victim to a breach (i.e. reactive) as opposed to FIPA requiring certain actions to be taken to sure up a covered entities systems to prevent something bad from happening. FIPA could have required covered entities to: perform risk assessments; implement certain administrative, physical, and technical mitigating controls; perform independent testing/audits/evaluations; develop information security/privacy policies/procedures; require assignment of these security responsibilities to an officer of the company; require incident response plans/procedures; require verification that companies meet a certain level of security; perform log monitoring and active surveillance of a covered entities' systems; etc.

I realize that the law requires each covered entity, governmental entity, or third party agent take *reasonable measures* to protect and secure data in *electronic form* containing personal information, but *what does this really mean*? The law doesn't provide any definition of 'reasonable' and *what standards do we address*? *NIST*? *PCI*? *FISMA*? *ISO*? *Other*? In addition, this section of the law only addresses data in electronic form; albeit, *customer records* are defined in FIPA as any material regardless of the physical form on which personal information is recorded or preserved. (A special note here is that customer records also include 'spoken words', but there isn't any mention in FIPA on how this is taken into consideration.)

Breach Notification

To continue our analysis, FIPA requires that a covered entity provide notice to the **Department of Legal Affairs** of any breach of security affecting **five hundred (500) or more** individuals in the **State of Florida**. This notice needs to be provided as expeditiously as practicable, but no later than **thirty (30) days** after the determination of the breach or reason to believe a breach occurred. A *breach of security* (i.e. *breach*) is defined as unauthorized access of data in electronic form containing personal information. It is also defined as an employer or agent of a covered entity that uses personal information for other than business purposes or for further unauthorized uses. (Note: this definition indicates 'in electronic form', but as we already indicated, personal information could be maintained in paper form or through spoken words. *Will this law not apply to a 'breach' of personal information involving other mediums of data*?)

As it relates to the time allotted for notification, those of us familiar with the HIPAA/HITECH regulations will note that thirty (30) days upon determination may be less strict than the sixty (60) days upon discovery. The concern I see is the time between an incident that occurred, being discovered, and then actually being determined that the incident constitutes a breach under the law. Those in the information security industry have already seen where there are time lapses when responding to an incident.

As an example, let's say that a covered entity had their customer database accessed by an unauthorized person. This database contained personal information. Without certain controls implemented, the covered entity may not even know that this database was accessed by someone. In addition, this unauthorized person could possibly gain complete access to this system over an extended period of time. For argument sake, let's say the unauthorized access was *discovered*. Under HIPAA, the 'clock' starts running at this point for notification purposes; however, no formal investigation has begun. The covered entity brought in a forensic expert to review exactly what happened. It took the expert forty-five (45) days to come to a conclusion that someone got into the database three (3) months back and over time, copied all the customer records out of the database. Under HIPAA, the covered entity has fifteen (15) days to make notifications to affected individuals. Based on the results of the expert, the incident was reported to law enforcement. If the law enforcement agency takes the experts opinion 'at face value', the *determination* of a breach might be made at this point and the clock would start for FIPA notification; however, if the law enforcement agency wants to conduct their own investigation, a *determination* might not be made (or there could be a delay due to a criminal investigation being underway). In either case, individuals' personal information is controlled by someone other than the covered entity that could be utilized for malicious and criminal activities (i.e. identity theft). If the covered entity doesn't fall under HIPAA regulations, the individuals affected in this breach haven't even been notified that their personal information is out there somewhere.

Department of Legal Affairs Notice

FIPA requires certain written notice to the **Department of Legal Affairs** that must include: a synopsis of the event; number of individuals affected; services being offered to affected individuals (without charge); a copy of the notice provided to individuals (*we'll talk about this in just a second*); and contact information for an employee or agent of the covered entity for additional information on the breach.

Be aware, FIPA indicates that the Department of Legal Affairs could request and the covered entity must provide upon its request the following:

- A police report, incident report, or computer forensic report.
- A copy of the policies in place regarding breaches.
- Steps that have been taken to rectify the breach.

Of course, a covered entity can provide additional information regarding a breach at any time and if the covered entity is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, they can post the notification information on an agency-managed website as opposed to making written notice to the Department of Legal Affairs.

Notification for HIPAA Covered Entities

For those covered entities that are considered covered entities (or business associates) under HIPAA/HITECH and make the requisite notifications to individuals pursuant to the HIPAA/HITECH Breach Notification Rules, they are deemed to be in compliance with the individual notification requirements under FIPA.

Other Covered Entities

For non-HIPAA covered entities (or business associates), a written notice must be sent by mail or e-mailed to affected individuals that includes, at a minimum, the following items:

- Dates of the breach (or estimated date or date range)
- Description of the personal information that was accessed or reasonably believed to have been accessed
- Contact information of the covered entity to inquire about the breach

Substitute Notification

FIPA allows for substitute notification in the case of notification costs exceeding **$250,000** due to the number of individuals affected (i.e. exceeding **500,000**) or if the covered entity **doesn't** have e-mail or mailing addresses for the affected individuals. A covered entity could post a notice on the Internet website and provide notice in print and to broadcast media where the affected individuals reside.

Credit Reporting Agency Notification

If more than **one thousand (1,000)** individuals at a single time were affected by a breach, the covered entity will need to notify, without unreasonable delay, all **consumer reporting agencies** that compile and maintain files on consumers nationwide. The notice must include timing, distribution, and content of the notices.

Third-Party Notifications

Risks are growing to third-party service providers as more companies rely on their services and these service providers maintain covered entities' customer records. If a third-party falls victim to a breach, they are required to notify the covered entity as expeditiously as practicable, but no later than **ten (10) days** following the determination of the breach of security or reason to believe the breach occurred. Once the third-party notifies a covered entity, the covered entity needs to provide the requisite notices to individuals, Department of Legal Affairs, and the credit reporting agencies accordingly. Now, the third-party service provider could provide notice on behalf of the covered entity, but if they **fail** to do so, any **violations come back on the covered entity**.

In essence, covered entities have a responsibility to ensure that their service providers are doing what they are supposed to in protecting personal information. Covered entities must also ensure that notifications are appropriately made if necessary. Service providers have a tight deadline to make notifications, but unlike the HIPAA Omnibus Rule making these service providers directly liable for certain regulations, the onus is on the covered entity to ensure notifications are made.

For those covered entities under HIPAA/HITECH that just updated their business associate agreements in reference to the Omnibus Rule changes, you may want to consider the changes FIPA now brings about for those covered entities (and third-party agents) that operate in Florida. Although a business associate agreement always indicates that a third-party must notify the covered entity, I've always recommended to my clients they add the specific time frame of notification. In Florida, you may want to consider updating this notification requirement accordingly. You will also want to ensure you address the responsibility for notifying individuals. Even though the agreement might indicate a third-party is responsible for notification, under FIPA, the covered entity may still be held liable for a third-parties' failure to notify.

Law Enforcement Investigations

A caveat to making a notice to affected individuals is that if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, it is reasonably determined that a breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed, **no notification is required**. This determination must be in writing and maintained for at least **five (5) years**. The covered entity must also provide this written determination to the Department of Legal Affairs within **thirty (30) days** after the determination.

This caveat makes me a little nervous. Being a former law enforcement officer, I know that cybercrime investigations aren't normally a part of officers' training, especially at the local law enforcement level. Although I actually pursued training in this area when I was on the force, I found that law enforcement agencies were way behind in this area of investigations. Now that I work in the information security industry, it is apparent that these agencies may not be equipped to handle such investigations as seen through the rise in identity theft crimes and the low number of arrests of cybercriminals. These types of investigations could be highly complex/technical and unless the investigators are trained/skilled in these specific investigations, I'm not sure how they can make an *accurate* determination of a breach. I'm not even sure if law enforcement agencies have the resources to handle the influx that may come about from investigating these breach incidences. (I suppose they could call on experts in the field to assist, like me, but I digress.) *Will additional resources be provided to these agencies*? *Will additional training be provided to these investigators*? *What type of equipment and software will be needed to perform these type of investigations*? FIPA doesn't address these questions.

For covered entities under HIPAA/HITECH, the federal regulations still presumes a breach occurs unless there is a low probability of a compromise of the protected health information utilizing a four (4) factor analysis. This analysis may (or may not) align with a determination of a breach under FIPA so you will want to ensure you consider this in your determinations if you are a HIPAA covered entity.

Disposing of Customer Records

FIPA requires that covered entities and third-party agents take reasonable measures to dispose, or arrange for disposal of customer records within their custody when no longer needed. FIPA is a little wide open with disposal in that shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means is a little vague. As security experts, we know that unless you utilize a cross-cut shredder, perform certain wiping activities utilizing specifically approved software, or physical destruction of paper/media, the information could possibly be retrieved. FIPA lacks the appropriate guidance for proper disposal of personal information. FIPA could have easily referred to the *NIST SP 800-88: Guidelines for Media Sanitization* to offer up guidance by which these disposal methods could be better followed and enforced.

Enforcement

No law is fully complete without having some *teeth* to back it up. A violation of FIPA is treated as an unfair or deceptive trade practice. **Civil monetary penalties** can be imposed against a covered entity or third-party agent not to exceed **$500,000**. Civil penalties can be assessed as follows:

- **$1,000** for each day up to the **first thirty (30) days** following a violation, and
- **$50,000** for each subsequent **30-day period** thereof for up to **one hundred eighty days (180)**
- If violation continues for more than one hundred eighty days (180), amount is not to **exceed $500,000**

Unlike HIPAA that has penalties assessed on a **PER VIOLATION** basis, civil penalties under FIPA are on a **PER BREACH** basis (and not based upon the number of individuals affected). In addition, there is **no private cause of action**.

It is interesting to note that any penalties collected under FIPA will be deposited into the General Revenue Fund. I'm curious to note why these penalties might not be utilized in other ways to promote covered entities in making their systems more secure or establish grant funding opportunities to provide expert resources to assist covered entities in their security efforts. (*Maybe this is planned for the future*?)

Although I can appreciate the steep penalties in an attempt to obtain compliance of covered entities, I believe there should be a private cause of action. At the end of the day, we are talking about the rights of an individual to keep their personal information private and the failure of a covered entity to properly protect/secure this information. Covered entities, in their performance of certain services or under contract to their customers, have an obligation to protect this personal information. It is ultimately going to be the individual that is at risk or will fall victim to identity theft in the case of a breach. It has already been shown that victims of identity theft spend thousands of dollars to recover from the damages caused by this type of crime. Unless the legislatures were counting on individuals affected by a breach taking up personal legal actions against covered entities, I'm not sure why these *victims* would not be entitled to a private cause of action. We are already finding that the judicial system is not very supportive of individuals taking actions against companies to protect their information unless they can show specific damages caused by a breach. I argue that the damage has already occurred when an individual's personal information *has been* breached. Once the information is out, it can't be taken back. Individuals have the right to be private in their information.

Summary

Although Florida may be taking a lead in getting a handle on security issues by passing FIPA and I applaud them for their efforts, there is still a lot more that needs to be done in this area. Information security is ever evolving and ongoing. New technology along with the criminal elements that may find ways of utilizing this technology in nefarious ways will always outpace the regulations designed to curb this activity. I believe the intent of the law is honorable, but as discussed, there are several areas that it could be improved. I'm optimistic that the law will be taken seriously by covered entities, enforced fairly, and raise the level of concern over security that may be lacking in many organizations as opposed to being just another revenue generator. I guess time will tell.

Disclaimer

The material presented in this whitepaper is provided for informational purposes only and does not constitute legal advice. This material is intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. This whitepaper is offered only for general informational and educational purposes. It is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained in this whitepaper without first seeking the advice of an attorney.

Author

John "Jay" Trinckes, Jr., CISSP, CISM, CRISC - President/CEO of Eagle Trace Security Consulting, Inc. and author of "The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules". http://www.EagleTraceSecurity.com . Jay is an industry thought leader and subject matter expert in the area of information security and HIPAA compliance.