Information Security – Keeping Secrets from the Backyard to the Board Room

We all learned how to keep a secret in the backyard as a small child – "Do not tell anyone." If you intentionally or unintentionally divulged another's secret, then you were subject to their wrath. The lessons of our youth get more complicated as we have to communicate with others for legitimate reasons and such communications have to be kept secret. Now that we are grown up, we call it keeping information in confidence; therefore, we develop procedures and policies to keep information confidential. Today, we must not only know how to keep information confidential but we have to demonstrate that we have procedures in place to ensure confidentiality.

What is Non-Public Personal Information?

Secrets can be in many forms, but knowledge of a person's financial secrets, which can be used against them, provides the holder of such information a great deal of power. Congress recognized the need to outline standards for protecting financial information and in 1999 they passed the Gramm-Leach-Bliley Act ("GLB"). GLB required certain protections for Non-Public Personal Information ("NPI") in the hands of certain companies. In order to protect NPI, one must understand what it is and where it is.

Non-public Personal Information: personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. NPI includes first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers.

This definition of NPI is rather broad in that two or more pieces of publically available information can be collected with the intention of influencing a consumer credit decision and be considered NPI. If you have an individual's name or address, that does not amount to NPI. Add the fact that that individual is involved in a real estate transaction and it becomes NPI. As you can see, most information that one would handle in a real estate transaction will rise to the standard when viewed collectively.

What is Gramm-Leach-Bliley Act (GLB)?

GLB was first enacted for the financial sector. If you were a financial institution and collected NPI from consumers, then you were required to comply. GLB goes on to include restrictions on businesses that receive NPI from covered financial institutions. If you fell into this category, your activities would be limited to the collection, use, storage, and disposal of NPI. The requirements of GLB basically extend to all parties that are providing "financial services." Section 4(k)(6) of the Bank Holding Company Act extended these privacy rules to all financial activities, specifically including "providing real estate settlement services."

ALTA Best Practice #3:

> **Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.**

The stated purpose of ALTA Best Practice #3 is as follows: "Federal and state laws (including the Gramm-Leach-Bliley Act) require title companies to develop a written information security program that describes the procedures they employ to protect Non-public Personal Information. The program must be appropriate to the Company's size and complexity, the nature and scope of the Company's activities, and the sensitivity of the customer information the Company handles. A Company evaluates and adjusts its program in light of relevant circumstances, including changes in the Company's business or operations, or the results of security testing and monitoring."

There are three basic steps required to comply with and fulfill the purpose of ALTA Best Practice #3:

1) Have a written information security program;
2) Include in your written information security program all of the necessary elements; and
3) Adhere to your written information security program.

What Should Be in the Written Information Security Program?

a. ***Risk Assessment.*** In order to tailor any Information Security Program to a specific office, a candid and critical assessment of the risks facing that particular office should be performed. These risks could include any or all of the following:

- Who has access to NPI?
- How is NPI transmitted?
- How and where is NPI stored?
- How is NPI used in the workplace?
- How vulnerable is NPI to loss due to data corruption or natural disaster?
- How is NPI decommissioned, destroyed or discarded?
- How is NPI vulnerable to internal and external threats?
- How many third parties (e.g. IT professionals) have access to NPI?

The most important thing is to take the time and complete a very HONEST risk assessment. Remember, the risk assessment is for internal use. Once it is complete, then the findings should be appropriately prioritized.

b. ***Privacy Officer.*** For any process or procedure in an office, someone has to take ownership of it if it is going to see a successful completion. In a small office, this could be just another title for the principal of the company. In a larger office, this responsibility may find that a committee is needed to effectively implement and monitor an Information Security Program.

c. ***Authorized Personnel Only.*** Access to NPI should only be granted to authorized employees who have the requisite training to be allowed to handle NPI.

Regardless of who you permit to access NPI in your care, you should perform adequate employee training which conveys the importance of NPI, ensures the protection of NPI from internal and external threats, and requires the trainee to acknowledge receipt and comprehension of the Information Security Plan. Additionally, before you allow any employee access to your office and NPI, you should perform a criminal background check. Subsequent checks every three years (going back five years) are also part of this process.

Finally, when an employee leaves your employ, their access to the office and the computer should be terminated immediately. In the old days, we would simply ask for the key to be returned. Today, we need to get that key, but also need to terminate their passwords and change the alarm code.

d. ***Physical Security.*** While we may think that the entire cyber world is harder to understand and conquer, it is the truly “old school” security protections that may be the hardest change in our everyday work environment. Changing old habits is invariably harder to accomplish than learning new things altogether.

Physical security begins with securing the building in which NPI is stored. Old school precautions such as a lock and burglar alarm are a good starting point. Most people already employ these trusted precautions. The next step is implementing a “Clean Desk Policy.” Simply put, a clean desk policy is securing documents containing NPI such as open files, closed files, bank statements, applications, unrecorded loan documents, mail, and basically any printed material

concerning a transaction whether it is located on the desk, in the file, on the printer, or even in the trash can.

One point about "*physical*" security that may often get confused with "*digital*" security is the physical custody of computer equipment. Making sure that your server, backup data, laptops, smart phones, and all other forms of "*portable*" media containing NPI are secure, is of utmost importance. Keeping information secure on the device is digital security. If someone loses their laptop, no matter how password protected or encrypted the data may be, a cyber-criminal – given enough time – will be able to get to the NPI.

e. ***Digital and Electronic Security aka Network Security.*** As mentioned above, digital security refers to keeping the NPI safe *on* the digital or electronic device. The first and easiest protection is to password protect data on all digital devices. Every password should be "complex." The acceptable standard for "complex passwords" is that they are at least 8 characters long, contain upper and lower case letters, at least one number, and are changed at least every 90 days.

Additional efforts to digitally protect NPI include having an up-to-date virus protection program that updates at least every day. The network should be located behind a digital firewall that protects the network from outside threats.

Digital storage and transmission of NPI should be encrypted. This includes email. All email should be a hosted or internal solution that is domain specific. The use of free email accounts (such as Gmail, AOL, Yahoo or Hotmail) may not provide the security needed for the transmission of NPI. Additionally, the transmission of email containing NPI should be encrypted so that it is safe from the initiation of the transmission, through the length of the transmission, to the receipt of the transmission.

Finally, there needs to be a protocol in place to protect digital media from being transported on portable media devices. An entire office's collection of NPI can be stored on a portable media device (e.g. cd, USB drive, jump drive, back-up tape) and removed from the office for improper purposes. While these devices are convenient, they need to be used in a controlled environment to prevent unauthorized release.

f. ***Disposal and Decommissioning of NPI***. When examining where and how we store NPI, we must consider how we dispose of it. If we protect it right up until the point that we put it in the garbage can on the curb, all of those efforts may be wasted if the right criminal were just waiting for you to hand deliver NPI to them. Generally, we think of shredding or burning paper files containing NPI; however, we have to expand our thinking and include any digital device that once contained NPI. These devices (e.g. computers, smart phones, portable drives, and even copiers) need to be decommissioned and wiped clean prior to disposal.

g. ***Disaster Management Plan.*** Protecting NPI from external threats that may use the NPI for improper purposes is not the only reason that one must protect NPI. NPI must be protected for the basic reasons of business continuity. Simply put, a disaster management plan includes a backup plan that protects NPI from loss.

h. ***Oversight of Third-Party Service Providers.*** When dealing with third-party providers, it is important to understand their procedures and policies when they handle your NPI. If your NPI is stored off-site, it is important to ensure it is secure in that environment. An example of this vulnerability is the IT professional that you have assisting with your network. Given the access that IT professionals have to the NPI in your network, they should be chosen with care and understand your obligations to protect NPI.

i. ***Notification of Security Breaches.*** When that unfortunate day comes and someone has a security breach, the first impulse is to minimize the event and think that it cannot be that big a deal. If you are the unfortunate victim of a security breach and an unauthorized release of NPI, it

is important to work with your affected customers/clients and appropriate law enforcement. Hopefully, if you take the steps outlined above, you will minimize the likelihood of having to face this difficult circumstance.

j. ***Audit Procedures and Oversight.*** At the end of the day, you can put all of the appropriate procedures in place, but if they are not effective, then they have been a waste of time and money. To oversee your Information Security Program, you need to make sure that your virus protection is actually updating, that your back-up is actually running, and that your NPI is actually being shredded. This is an ongoing process, and you should monitor the process that you took time and money to put in place to make sure that it is effective.

Can You Demonstrate that You Can Keep a Secret?

The stakes of keeping a secret have been raised since our days on the playground. Now, we not only need to keep secrets, we also need to demonstrate that we know how to keep a secret. We used to think of our threats as being all internal to our physical borders – employees, partners, thieves that enter the office. In today's world, we must reevaluate that line of thinking and think that anyone with internet access could be a threat because anyone with an internet connection is a potential target to those trolling the internet for vulnerable security systems. You do not have to be a big company to get hacked, you just have to be unprepared.