Whitepaper

How Data Privacy and Protection Assists in Regulatory Compliance

February 2011

PIVOTGROUP
Armed with Information Security Knowledge

As an organization, do you know where company employees collect and store PII personally identifiable information? PII is primarily defined as pieces of information that can be used to distinguish or trace an individual's identity. These include a person's first name or initial of first name along with last name used in conjunction with a Social Security Number (SSN), credit or debit card account number, passwords, user ID's, medical records, health insurance information, bank account number and personal identification number (PIN). Identifying where PII is located can be a very daunting task for organizations as the proliferation of portable media devices continue to increase. Knowledge of where PII is on your network, computer hard drives, and portable media devices is critical in order to be in regulatory compliance and to be aware of when a security breach may have taken place.

The Risks of Identity Theft

The Federal Trade Commission (FTC) describes the risk of identity theft as the loss of one's good credit when someone else uses your identity through the use of their PII to procure credit cards typically for cash advances as well as to make purchases of jewelry, electronics, or other items that can easily be converted into cash. Once the bill comes, either one payment is made or no payments are made by these identity thieves. The result is that the person whose identity has been stolen begins to have their credit rating deteriorate and cause a great headache with regard to procuring credit in the future.

There are a number of risks associated with unprotected PII. One of the identity theft risks involves how an organization collects, uses, disseminates, and disposes of PII. Many news reports have claimed the exposure of numerous SSNs, credit card and debit card numbers, or medical information due to lost laptops, USB drives, or other portable media devices containing unencrypted PII. The use of e-mail to transmit PII without the use of encryption also provides an avenue for identity theft if this message is intercepted or sent to the incorrect e-mail address. Hacking into an unprotected computer is another avenue for identity thieves to procure access to your PII. Additionally, the physical thefts of credit card applications delivered through the mail or found in garbage have been used by persons attempting to capture or steal someone's identity. Improperly disposing of credit card applications, documents containing one's SSN, medical records or pharmacy receipts in the garbage without first cross-strip shredding them have also lead to identity theft.

The Regulations Pertaining to Data Privacy & Protection

There are laws in the United States as well as international laws that attempt to place the onus of protecting PII on the organization in possession of this information. PCI DSS (Payment Card Industry Data Security Standards) outlines security measures that must be implemented in regard to credit card information. HIPAA (Health Insurance Portability and Accountability Act) of 1996 imposes restrictions on healthcare providers to ensure that patient medical records remain confidential, private, and secure through the use of administrative, physical, and technical safeguards. GLBA (Gramm-Leach-Bliley Act) of 1999 Title V focuses specifically on privacy and the protections of financial customer data. Any non-public information in the possession of a financial institution must be protected from a security breach. NCUA (National Credit Union Administration) Reg 748 -

Appendix B to 12 CRF Part 748 - Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, (November 2005) requires credit unions to protect sensitive member information and to properly dispose of it. FACTA (Fair and Accurate Credit Transaction Act) Disposal Rule created by the FTC, NCUA, federal banking regulatory agencies have required appropriate disposal of credit reporting information or information derived from credit reports. The FACTA disposal rule requires that PII be burned, pulverized, or shredded. This rule also includes the proper destruction of electronic media containing sensitive data to ensure that the information contained therein cannot be read, reconstructed, or used. One of the most recent laws dealing with preparation of red flags to warn of identity theft was promulgated by the Federal Trade Commission in cooperation with many other United States regulatory agencies.

Red Flags Rule

As a result of the propagating identity theft market, wherein the stakes have been raised by organized crime entering the playing field, the FDIC drafted a supervisory policy on identity theft that was issued on April 11, 2007. On October 31, 2007, the FTC, FFIEC, FDIC, and NCUA sent the *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003* to the *Federal Register* for publication of the final rule. These red flags rule had a mandatory compliance date of **November 1, 2008** by all financial institutions. However, many non-banking creditors, such as car dealerships, finance companies, mortgage brokers, utility companies, and telecommunications companies, as well as non-profit and government entities who defer payment for goods or services, did not realize they too needed to comply with the Red Flags Rule. As a consequence, these non-banking creditors and state-chartered credit unions were given an extension to **May 1, 2009** to create and put into practice their written identity theft programs. However, this extension does not relieve them of any liability they may incur during this time period.

The Red Flags Rule requires financial institutions to implement a written identity theft prevention program and take specific steps to prevent identity theft. The financial institutions and creditors with covered accounts must track events to develop patterns of identity theft as an early warning system to proactively notify their customers and the appropriate authorities. Examples of specific events that should be monitored as possible indicators of identity theft are suspicious or unusual account activity that is inconsistent with previous account activity, consumer fraud alerts received from a consumer reporting agency, suspicious identification documents that appear to be altered or forged, and suspicious access to PII.

HIPAA and HiTECH ACT

HIPAA was enacted in 1996 and became fully effective in 2003 covers electronic protected health information (ePHI). The regulation identifies the types of security safeguards required for compliance:

- Administrative Controls
- Physical Controls
- Technical Controls

The security controls, how long to retain ePHI, and appropriate destruction procedures are required to insure the privacy of medical information. This information should be encrypted or securely destroyed to protect it. The impetus of this legislation and the HiTECH Act (Health Information Technology for Economic and Clinical Health) is to protect sensitive data from inadvertent exposure

HiTECH Act was enacted in **February 2010** to strengthen, enhance, and enforce the HIPAA provisions. The HITECH Act is the portion of the ARRA (American Recovery and Reinvestment Act of 2009) that provides for a federal breach notification of any unsecured PHI (protected health information). The main points of federal breach notification are:

- Impacts data in any format; paper, fiche, computerized, etc.
- Must notify if accessed, acquired, or disclosed
- The term ‘‘breach’’ means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

All notifications shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate.)

The HiTECH act also allows for enhanced penalties. There is a tiered penalty structure based on how bad the negligent behavior was and starts at $25,000 up to $1.5M for the worst cases. Where situations include willful neglect the penalties will be mandatory.

The HiTECH Act also creates explicit authority for the Dept. of Justice to pursue investigations and criminal cases against individual employees. True criminal acts such as identity theft will be a primary concern of Dept. of Justice. Healthcare organization may want to use these penalties and authority for enforcement as part of training to get attention of employees.

The Federal Security Breach Notification Law for healthcare and dramatically different than every other state law. There is not a risk of harm threshold which is included in most state data breach notification laws. There is no opportunity to evaluate whether there is any real risk of harm which will require reporting of a wide range of security breaches.

Any breach requires notification; it does not matter if it is a breach of SSNs applies to unsecured data. If encryption, or any other technology the government defines as secure, is implemented it would not be considered a breach. Extensions of the HIPAA obligations now apply to the vendors (business associates) under the HiTECH ACT which were not subject to terms under HIPAA Security Rules for business associates. Vendors now become covered entities under HIPAA Security Rules

Data Privacy Laws

The United States has a blended self-regulation approach to data privacy through the use of sectoral laws encompassing finance, healthcare, protection of children, and the protection of consumers' PII. The European Union on the other hand has data privacy laws that are all encompassing.

Nevada passed a privacy law during the fall of 2007 requiring that any e-mail containing PII must be encrypted. Nevada's law is the first data privacy law enacted that mandates encryption for the transmission of customer PII through electronic means other than via a fax or on an internal secured system. This law went into effect on **October 1, 2008**. Massachusetts implemented a similar law on **January 1, 2009** regulating PII of Massachusetts residents, whether or not that business maintains a presence within Massachusetts.

In the EU (European Union), data privacy is taken quite seriously. Their definition pursuant to the *European Commission's Directive 95/46/EC Article 2* is: "*Personal Data* shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

Canada takes the privacy of their citizens very seriously as well. PIPEDA (The Personal Information Protection and Electronic Documents Act) of 1998 covers all industries and protects the collection, usage, and disclosure of personal information. Similar to the European Directive, this law mandates a person's consent to allow their personal information to be used in any fashion barring criminal investigations.

The EU and Canada also have laws controlling third party transfers of data. Thus, data cannot be removed from European countries or Canada without complying with many stringent standards. A company that has satellite offices in European countries must obtain Safe Harbor certification prior to transferring any private data to any other country, including the United States. Safe Harbor certification is a laborious and expensive process. Employee data is the most sensitive data pursuant to the EU Data Directive. Performance evaluations, terminations, drug tests, and employment applications are also considered sensitive data. Supplier contact databases and contract information and third party access to sensitive data as well as customer databases and contract information are all forms of personal information in Europe and must be protected.

Data Security Breach Laws

California Senate Bill (1386) was the first data security breach notification law in the United States passed in 2003. As of February 2011, there were 46 states as well as the District of Columbia, Puerto Rico, and the Virgin Islands who have similar data security breach notification laws. These laws mandate if a company compromises the PII of anyone living in their state, including access by an unauthorized employee, that the affected individuals must be notified. There are severe monetary penalties ranging from $250 to $500 per PII exposed to a maximum of $750,000 in some states for not properly notifying those individuals whose PII was compromised.

Best Practice Tips on Preventing Identity Theft and Regulatory Compliance

The following best practice tips are not an exhaustive list but are critical ones to consider when complying with the various regulations and laws.

1. Only collect the PII/ePHI your organization needs to conduct business with the customer.
2. Ensure the protection of this collected PII/ePHI by only allowing access to those who require access to complete their jobs and the organization's transactions.
3. Being in possession of PII/ePHI does not give you authority to transfer it to a third party. This type of data should not be shared with third parties unless there is a business use necessary for disclosure of PII to complete a business transaction. There should also be a contract outlining how the third party will be protecting this information while it is in their custody.
4. A vendor management audit should be performed by an independent third party to ensure that the shared data is being adequately protected by appropriate security measures.
5. Encrypt PII/ePHI when it is in transit or at rest on computer hard drives or servers, even if it is not mandated by law.
6. Ensure that the information is securely protected even when at rest on the network.
7. Properly train all custodians of PII in the best practices of protecting this data while in their possession.
8. Destroy sensitive data when it is no longer needed. Immediate use of a cross-strip shredder that will pulverize the paper into unreadable form is best rather than relying on a service to shred it.
9. Never dispose of PII/ePHI in a public receptacle or in your own personal garbage without first shredding it with a cross-strip shredder. Post warning signs on trash receptacles to alert your customers that they should not dispose of their PII in your company's waste cans.
10. Pulverize, burn, or shred hard drives as well as paper documents. A sledge hammer or magnet can be extremely helpful when it comes to properly disposing of hard drives containing information.
11. Conduct regular risk assessments to identify where and how your company stores or transmits PII/ePHI.
12. Implement an intrusion detection system (IDS), intrusion protection system (IPS), and data leakage protection (DLP) technology to help detect and protect PII from being compromised.
13. Test your incident response policy regularly to make sure it is current and effective.
14. Review and assess your information security management program, policies, and procedures to ensure they are current and effectively communicated throughout your organization.
15. Be knowledgeable of the requirements of applicable data privacy protection laws and regulations.
16. Regularly monitor the results of your Data Privacy and Protections program to ensure they are meeting your business requirements and adjust accordingly.

Recommended Technologies

The following is a list of recommended technologies that can help keep PII and ePHI safe and assist in regulatory compliance.

1. Security Patch Management-Protection
2. Encryption for Data and Devices-Protection
3. Virus and Malware-Detection and Protection
4. Extranets/Secure File Transfers-Protection
5. Business Recovery-Protection
6. Secure Back Up-Protection
7. Secure Business and Operations Data Bases and Systems- Protection
8. Confidential and Ethical Walls-Protection
9. Vulnerability Management- Detection & Protection
10. Firewalls-Protection, Detection, Monitoring & Alerting
11. Log Management-Detection, Monitoring and Alerting
12. IDS/IPS- Detection, Protection, Monitoring & Alerting
13. Access Control & Authentication- Protection, Detection, Monitoring & Alerting
14. Web Activity Monitoring- Protection, Detection, Monitoring & Alerting
15. Data Loss Prevention- Detection, Protection, & Monitoring and Alerting
16. Portable Device Control – Detection, Protection, & Monitoring and Alerting
17. Governance, Risk, and Compliance- Management Reporting
18. Data Search and Inventory- Management Reporting
19. Risk Assessments-Management and Reporting
20. Penetration Testing-Management and Reporting

Conclusion

Data Privacy and Protection is an integral part of our day to day lives. The most successful compliance programs are not based upon developing a data privacy program around a compliance initiative, but rather developing an ERM (Enterprise Risk Management) program that is based on an appropriate standardized framework which is tailored to your organization's business model and available resources. The ERM framework is a combination of culture, policies, awareness, technologies, and risk appetite. When an ERM program is effectively implemented and maintained the compliance effort will be a natural output of the program. In addition, you will be serving your company and customers better because of your holistic view of protecting critical data and receiving the best ROI for your company. An effective ERM program will also provide you with the critical information you will need to manage risk from an enterprise perspective and your company will be in a more defensible position when a data breach or loss occurs.

Authored By
Jim Soenksen, CEO
Pivot Group, LLC

About Pivot Group
Pivot Group is an independent audit, assessment, and compliance firm that exclusively provides data privacy and protection services. Rather than selling or reselling technology, we redefine the InfoSec realm by tailoring solutions for each client. The consultant-based practice delivers the complete life cycle of security services that meet the business and resource requirements of its clients. If you require assistance with data privacy and security initiatives, please call Pivot Group at 888-722-9010 or visit us at www.pivotgroup.com.