



THE INFORMATION MANAGEMENT DIGEST

Our Business, Is Keeping Your Business - Your Business!

A Service of WesTex Document, Inc.

August 2011

PRIVACY LAWS AND RECORDS MANAGEMENT

Privacy is defined in a 1997 article by Ronald Standler as “the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. Information is interpreted broadly to include facts, images (e.g., photographs, videotapes), and disparaging opinions.”

Modern privacy law in the United States traces its roots to the 1977 Restatement of Torts where four principles of privacy were defined: 1) unreasonable intrusion upon the seclusion of another; 2) appropriation of a person’s name or likeness; 3) publication of private facts; and 4) publication that places a person in a false light – similar to defamation. We have come a long way since the Restatement of Torts but it is clear that these fundamental principles are still very much at the center of controversy.

Identity Theft

There is a common axiom that “on the Internet you can be anybody”. Unfortunately, this also extends to misappropriation of the identity of another person, or Identity Theft. This type of crime is exploding in the United States. The Federal Trade Commission conducted a study in 2003 and reported the following findings:

- 27.3 million Americans have been the victims of identity theft in the last 5 years
- 52 percent of identity theft victims discovered they were victims by monitoring their accounts



- 49 percent of victims did not know how their information was obtained
- Identity theft losses to businesses and financial institutions in 2003 was \$47.6 billion – losses to consumers was \$5 billion.
- Losses to business and consumers per victim averaged \$10,200.

In 2010 the Federal Trade Commission received 250,854 complaints regarding identity theft, making it the single largest source of consumer complaints received by the agency in that year.

Government Response

Where the issue of privacy rights is concerned, the government has responded on multiple fronts. In 1996 Congress passed HIPAA, which in part deals with the maintenance of privacy where protected health information is concerned. Health and Human Services has now completed issuing both the HIPAA Privacy Rule and the HIPAA Security

Rule. One absolute requirement of HIPAA is the confidential disposal of Protected Health Information. Health and Human Services issued its "Breach Notification Rule" in 2009. Additional requirements passed as part of the HITECH Act in February, 2009, include provisions to extend many requirements of HIPAA to Business Associates of Covered Entities. While the HITECH Act includes financial incentives for covered entities to convert to electronic health records, there continues to be hesitation on the part of many health care providers until more uniform systems and approaches are agreed. Two methods for protecting health information from the risks associated with data breach have been identified and are being widely applied: the confidential destruction of protected health information; and the application of NIST-certified encryption technology for digital records, including computer backup and recovery media held offsite.

Additionally, the government responded to privacy protections necessary for financial information. In 1999 Congress passed the Financial Services Modernization Act legislation more commonly referred to as Gramm Leach Bliley. Although similar to HIPAA, the scope of this act is actually much broader than is commonly understood. While banks and financial services companies are obvious targets of the act, the privacy provisions also extend to any business that collects financial information for installment loan purposes, etc. This could include jewelry stores, used car lots who finance, and pawn brokers if they pass the "significant engagement" test. Title V of the act is exclusively devoted to privacy concerns but the specifics are contained in rulemakings of agencies charged with implementing Gramm Leach Bliley. Effective May, 2003, the Federal Trade Commission's rule making on financial information privacy took effect. This rule making can be found at 16 CFR 314. Of particular concern to records managers is § 314.3 and § 314.4 (b) which contains this description of responsibilities required under GLB: "(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- (1) Employee training and management;
- (2) Information systems, including network and

software design, as well as information processing, storage, transmission and disposal; and

- (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures."

FACTA

In December, 2003 President Bush signed Public Law 108-159, the Fair and Accurate Credit Transactions Act, (Also known as the FACT Act or FACTA.) The purpose of this legislation was to permanently extend federal preemption provisions of the Fair Credit Reporting Act to provide uniform national consumer protection standards. FACTA requires consumer information to be appropriately destroyed. Confidential destruction through shredding is identified as one acceptable method that complies with the requirements in FACTA.

RED FLAGS RULE

In addition to FACTA, the Federal Trade Commission also introduced its "Red Flags Rule" which applied to creditors. Implementation of the rule was delayed on several occasions, but following amendment, the rule took effect on January 1, 2011. This rule requires an organization to establish an identity theft prevention program within their organization. As a part of that program potential points of failure, or "red flags", must be identified and mitigation strategies designed to help prevent, detect, and respond to any breach or other event, which could lead to identity theft.

STATE PRIVACY LAWS

More than 40 states now have their own version of data breach notification laws. In addition, all states afford their citizens privacy-related protections through various laws. The Electronic Privacy Information Center offers a quick checklist of all states that identifies which types of privacy laws exist in that state: <http://epic.org/privacy/consumer/states.html>. More detailed information regarding state privacy laws can be found at the National Conference of State Legislatures website at <http://www.ncsl.org/default.aspx?tabid=13463>.

CONGRESSIONAL EFFORTS CURRENTLY UNDERWAY

High profile data breach events are driving Congressional activity on issues related to privacy protection. Numerous bills have already been introduced in the House and Senate to address privacy issues and further expand requirements for data breach notification. The Consumer Privacy Bill of Rights, cosponsored by Senators Kerry and McCain,

is one such bill that provides for enhanced data breach reporting requirements, requires enhanced protections for personal data, and allows consumers the right to “opt out” of data collection on the Internet.

CONCLUSION

Personal privacy of data has evolved to one of the most important aspects of risk management within the organization. Records and information managers must be constantly aware and mindful of various regulatory requirements. Data breach events can cripple an organization with costs for

notification and credit monitoring moving beyond \$100 per individual record breached. As a result, records managers find themselves working closely with IT professionals to design systems that provide information to the organization, when needed, while at the same time restricting access through enhanced IT protections and more substantive use of training and information governance management policy creation. More than at any other time since the creation of the profession, records and information managers are uniquely positioned to play a central and strategic role in the information governance of the enterprise.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS



Last month, Texas Governor Rick Perry <http://governor.state.tx.us/signed> a health privacy bill <http://www.capitol.state.tx.us/tlodocs/82R/bill-text/pdf/HB00300F.pdf> into law (see the attached copy of the final language) that imposes re-newed obligations exceeding the requirements in the HIPAA Privacy Rule. The law, which will become effective on September 1, 2012, incorporates the expanded definition of the term “covered entity” in Texas’s existing health privacy law and could have a broad impact on many non-HIPAA covered entities.

Several years ago the legislature passed legislation to make health privacy in Texas more stringent than HIPAA and the following year special interest groups caused the legislature to gut the law - but the “covered entity” language of any entity that engages in “assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information,” as well as any entity that “comes into possession of” or “obtains or stores” protected health information (“PHI”) - remained. They simply gutted the penalties and enforcement language. Now the current legislature has put the teeth back into the law, recognizing the seriousness of the continuing breaches of privacy (not to mention the fact that our Texas state government actually sells medical lists to anyone that wants to fork over the money to get them) as led to more identity theft threats to the citizens of Texas.

Notably, the new Texas health privacy law:

- Requires all employees of covered entities to undergo training on HIPAA and Texas’ health privacy law within 60 days of hiring (and at least once every 2 years);
Bans the disclosure of PHI for remuneration, except that covered entities may disclose PHI to other covered entities for treatment, payment, health care operations, insurance or HMO functions, or as authorized or required by federal or state law;
- Requires covered entities to provide notice to individuals that their PHI is subject to electronic disclosure and obtain authorization for any electronic disclosure of PHI (apart from disclosures of PHI to other covered entities for treatment, payment, health care operations, insurance or HMO functions, or as authorized or required by federal or state law);
- Mandates that health care providers provide individuals with access to their PHI within 15 days of their request;
- Authorizes the Texas Attorney General, Texas Health Services Authority or Texas Department of Insurance to conduct compliance audits of covered entities that have consistently violated the Texas law; and
- Obligates the Texas Health Services Authority to develop privacy and security standards for the electronic sharing of PHI.

We can provide free training to assist in compliance and also help you develop a destruction/storage policy that will help you meet minimum necessary rules.

DO YOU HAVE A DISPOSAL CONTRACT?

Sec. 72.004. DISPOSAL OF BUSINESS RECORDS CONTAINING PERSONAL IDENTIFYING INFORMATION.

- (a) This section does not apply to:
- (1) a financial institution as defined by 15 U.S.C. Section 6809; or
 - (2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.
- (b) When a business disposes of a business record that contains personal identifying information of a customer of the business, the business shall modify, by shredding, erasing, or other means, the personal identifying information so as to make the information unreadable or undecipherable.
- (c) A business is considered to comply with Subsection (b) if the business contracts with a person engaged in the business of disposing of records for the modification of personal identifying information on behalf of the business in accordance with that subsection.
- (d) A business that disposes of a business record without complying with Subsection (b) is liable for a civil penalty in an amount not to exceed \$500 for each business record. The attorney general may bring an action against the business to:
- (1) recover the civil penalty;
 - (2) obtain any other remedy, including injunctive relief; and
 - (3) recover costs and reasonable attorney's fees incurred in bringing the action.
- (e) A business that in good faith modifies a business record as required by Subsection (b) is not liable for a civil penalty under Subsection (d) if the business record is reconstructed, wholly or partly, through extraordinary means.
- (f) Subsection (b) does not require a business to modify a business record if:
- (1) the business is required to retain the business record under another law; or
 - (2) the business record is historically significant and:
 - (A) there is no potential for identity theft or fraud while the business retains custody of the business record; or
 - (B) the business record is transferred to a professionally managed historical repository.



Stress from too much Paper?

Then relax, there is a better electronic way.

Improve performance with instant file access.

Increase efficiency with automated workflow

"The labor savings were immediately apparent. We can index and input a couple thousand documents in just minutes."

Digital imaging, microfilm, storage and destruction.



Westex Document, Inc.

Amarillo and Lubbock

www.westexdocument.com

(806) 885-2906

