Data Theft and State Law

When Data Breaches Occur, 34 States Require Organizations to Speak Up

Thirty-four states currently require that organizations notify individuals whose personal data have been exposed in a security breach. Healthcare entities should have policies and plans in place.

by **Alan S. Wernick**, Esq.

You can hardly pick up a newspaper or visit a major online news source without reading about an incident involving a data breach. Laptops are stolen, private information is mistakenly exposed on public Web sites, and employees access data for illegal purposes.

Healthcare organizations are not immune. Providers and payers obtain, organize, analyze, copy, and distribute data around the clock. Data copied and distributed without authorization can result in legal complications that include violation of a data breach notification statute, identity theft, loss of employment, financial damages, and damages for breach of a legal statutory duty or obligation.

The time to prepare for responding to a data breach is now, not after it occurs. An organization's preparedness in knowing applicable laws, developing appropriate policies, monitoring

those policies, and having an appropriate response team assembled in advance will help manage the legal risks and minimize the potential liabilities and costs, both in dollars and in trust.

The States with Notification Laws
As of October 15, 2006

Arizona	Georgia	Maine	New York	Tennessee
Arkansas	Hawaii	Minnesota	North Carolina	Texas
California	Idaho	Montana	North Dakota	Utah
Colorado	Illinois	Nebraska	Ohio	Vermont
Connecticut	Indiana	Nevada	Oklahoma	Washington
Delaware	Kansas	New Hampshire	Pennsylvania	Wisconsin
Florida	Louisiana	New Jersey	Rhode Island	

What Are the Data in a "Data Breach"?

Data are protected by several state and federal statutes against unauthorized access, use, copying, and distribution. By way of example, and not limitation, these statutes include HIPAA, the Financial Services Modernization Act (otherwise known as Gramm-Leach-Bliley), and the Sarbanes-Oxley Act. Congress currently is considering data breach and related legislation. By way of example, the Identity Theft Protection Act (S 1408) and the Federal Agency Data Breach Notification Act (HR 5838) were under consideration in Congress in late 2006.

On the state level, more than 30 states currently have adopted data breach notification laws requiring organizations to notify consumers whose personal information have been exposed in a data breach (see list at right). Notification is intended to alert consumers about the potential for identity theft that occurs as a result of a breach. Data breach and other privacy laws can also help improve data security and privacy practices for the organizations complying with them.

Many of the state laws treat data as "personal identifiable information," or PII. Depending on the applicable statute, PII may include data stored on paper, a computer, or other media such as CD-ROM, DVD, flash memory drive, and PDA.

Depending upon the particular state's law, PII includes, by way of example and not limitation, an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security number
- Account number or credit or debit card number, or an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Financial information
- Medical information
- Passport number
- Alien registration number
- Employer identification number
- Taxpayer identification number (other than the individual's Social Security number)
- Medicaid account number
- Food stamp account number
- Insurance policy numbers
- Utility account number
- Mother's maiden name
- Employment history
- Biometric data including, without limitation, fingerprints, facial scan identifiers, voiceprint, retina or iris image
- Deoxyribonucleic acid (DNA) profile
- Digitized or other electronic signature
- Any professional, occupational, recreational, or governmental license, certificate, permit, or membership number

Two Strong State Laws

The California data breach notification law, effective July 1, 2003, is one of the first of such statutes in the United States, and the one other states and Congress have considered in the drafting of similar legislation.[1] The California data breach notification law defines "personal information" to mean

> any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.

For purposes of triggering a data breach notification, personal information in the California law means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number
- Driver's license number or state identification card number
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

Personal information under this section of the California statute does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Another example of a recent data breach notification law is the one adopted in Illinois, which became effective on January 1, 2006, and closely follows the California statute.[2] The Illinois data breach notification law, known as the Illinois Personal Information Protection Act (PIPA), defines personal information in the same terms as the California law (also excluding information publicly available and lawfully disclosed by a government agency).

When organizations consider what data are subject to notification in the event of a breach, they should also note that applicable state law may provide that data other than customer data trigger a notification requirement in the event of a data breach (e.g., employee data). Further, depending upon the residence of each of the

Data Breach: A Common Occurrence

A partial listing of data breaches notifications in the health services sector, August–September, 2006

Date of Public Announcement	Name and Location of Health Organization	Type of Data Breach	Number of Personal Information Records Lost or Stolen
September 24, 2006	Erlanger Health System, Chattanooga, TN	Records of hospital employees disappeared from a locked office on September 15, 2006. The employee records were stored on a USB jump drive. Information was limited to names and Social Security numbers (SSNs).	4,150 current and former employees
September 16, 2006	Michigan Department of Community Health, Detroit, MI	A flash drive was discovered missing August 4, 2006, and likely stolen from a department office. The drive contained names, addresses, phone numbers, dates of birth, and SSNs of participants in a scientific study.	4,000 Michigan residents
September 15, 2006	Mercy Medical Center, Merced, CA	A memory stick containing patient information was found July 18 on the ground at the county fairgrounds near the hospital's information booth. It was returned to the hospital four weeks later. Data on the memory stick included names, SSNs, birth dates, and medical records.	295 patients
September 9, 2006	Cleveland Clinic, Naples, FL	A clinic employee stole personal information from electronic files and sold it to her cousin, the owner of Advanced Medical Claims, who used it to file fraudulent Medicare claims totaling more than $2.8 million. Information included names, addresses, SSNs, birth dates, and other details. Both individuals were indicted.	1,100 patients
August 31, 2006	Labcorp, Monroe, NJ	During a break-in June 4 or 5, a computer was stolen that contained names and SSNs. It did not include birth dates or test results.	Unknown
August 29, 2006	Valley Baptist Medical Center, Harlingen, TX	In late August 2006, a programming error on the hospital's Web site exposed names, birth dates, and SSNs of nonstaff healthcare workers who contract with the hospital. It is not known how long the personal information was accessible.	73
August 25, 2006	Compass Health, Everett, WA	A laptop containing personal information, including SSNs, was stolen in June 2006. The agency serves people who suffer from mental illness.	"A limited number of people"
August 22, 2006	Beaumont Hospital, Troy, MI	A home healthcare nurse's vehicle was stolen in Detroit on August 5, 2006. A laptop in the car contained patient names, addresses, birth dates, SSNs, medical and personal health information, and medical insurance information of home healthcare patients served over the preceding three years. The laptop was returned on or about August 22 by a local resident who heard news reports about the incident.	28,000+
August 17, 2006	HCA, Inc., Hospital Corp. of America, Nashville, TN	Ten computers containing Medicare and Medicaid billing information and records of employees and physicians were stolen from one of the company's regional offices. Thousands of patient records in hospitals in eight states were affected. Names and SSNs of about 7,000 employees and physicians in four states were on the computers.	"Thousands of files"
August 11, 2006	Madrona Medical Group, Bellingham, WA	On December 17, 2005, a former employee accessed and downloaded patient files onto his laptop computer. Files included patient name, address, SSN, and date of birth. The former employee was arrested June 8, 2006.	6,000+
August 4, 2006	PSA HealthCare, Norcross, GA	A company laptop was stolen from an employee's car. The computer contained personal information on current and former patients, including names, addresses, SSNs, and medical case information.	51,000

Source: portions used with permission of the Privacy Rights Clearinghouse, www.privacyrights.org.

individuals whose data are the subject of the breach, more than one state's law may apply.

Notification laws generally require that the organization provide prompt notification as soon as it either discovers or is notified of a breach, or if it reasonably believes that the personal information may have been acquired by an unauthorized person.

The disclosure notification typically must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and

confidentiality of the data system. However, depending upon the applicable law, some constraints on the timing of the notice may include consideration of the legitimate needs of law enforcement if a notification might impede a criminal investigation and the need to take reasonable measures to determine the scope of the breach and restore reasonable integrity to the system.

The specific contents of the notice depend both on the applicable law and the facts of the breach. Generally, however, the contents of the notice may include, in addition to other relevant disclosures:

- A general description of the data breach
- What has been done to protect the personal identifiable information from further unauthorized access
- The type of personal identifiable information involved in the data breach
- What the individuals can do to protect themselves from identity theft (e.g., providing contact information and Web sites for the major credit reporting agencies and the Federal Trade Commission)
- Assistance the organization can provide (e.g., providing a Web site, e-mail address, or toll-free number for further information and assistance)

Depending on the applicable data breach notification law, a safe-harbor provision may exist for those organizations that, in advance of a data breach, have developed and maintained their own notification procedures as part of their information security practices for treatment of personal information, provided that such procedures are otherwise consistent with the notice timing requirements of the applicable data breach notification law. Thus, if an organization's notification procedures comply with the applicable data breach notification laws, then pursuant to the statutory safe-harbor provision, those procedures may be followed in lieu of the applicable statutory notification framework.

Be Prepared: Strong Security, Thorough Response Plans

Data privacy and security are closely intertwined. A fundamental principle of information and data stewardship is that organizations collecting or managing individuals' personal information should use reasonable security safeguards to protect that information against unauthorized access, use, disclosure, modification, or destruction. Protecting personal identifiable information requires more than just a strong physical structure to house the data; it includes appropriate data security considerations, data handling policies, and monitoring of those policies.

One example of a data security standard is ISO 17799 ("Information technology—Security techniques—Code of practice for information security management"), second edition (2005). It covers topics including:

- Security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Some questions to consider in reviewing your organization's risk for managing personal identifiable information include:

- Has the integrity of the database been tested by a third party?
- Does the company segregate critical PII data (e.g., PII subject to applicable laws) from other data?
- Does the company restrict employee access to the critical PII data?
- Does the company have written procedures for identifying if, when, and how a data breach has occurred?

- Does the company prescreen employees who have access to critical PII data?
- Does the company provide regular periodic training to employees concerning the handling of PII data?
- Does the company allow third-party access to PII data?
- Does the company have one or more individuals to whom any and all reports of a data breach are directed?
- Does the company have established contacts with the appropriate law enforcement agencies for reporting the data breach?
- Does the company have preliminary drafts of correspondences (e.g., letters, e-mail, e-faxes, etc.) regarding notice of a data breach?
- Has someone in the company been identified as the media contact for handling media inquiries regarding a data breach?
- Does the company "salt" the data so as to more easily identify the database or records in the database in the event of a breach?

While these questions may help you evaluate some of the data breach risk within your organization, it is not meant to be an exhaustive list. Each organization has different people, structures, and needs regarding the PII it manages.

Insurance coverage is available for data breach and varies according to policy purchased. Not all insurance policies provide the same coverage. For instance, for privacy injury liability and identity theft, coverage may be limited to specific activities (e.g., "e-commerce activities" or "Web site activities") or specific laws (e.g., HIPAA). A policy may exclude claims related to use of cookies, spyware, keystroke loggers, or other invasive devices or methods. It may or may not cover costs for regulatory defense, public relations, and notification expenses. Organizations should review policies in light of the applicable data breach and privacy law as well as the technology.

The bottom line is that when your organization experiences a data breach, your preparedness in knowing the applicable laws, developing appropriate policies, monitoring those policies, and having an appropriate response team assembled in advance (including knowledgeable legal counsel) will assist in compliance to manage the legal risks and minimize the potential liabilities and costs. These liabilities and costs include the financial costs of responding to the breach, and they include the impact on the organization's good will in the community and the impact on the time of the organization's professionals, management, and staff.

In the context of today's evolving technology, privacy concerns, and data breach notification laws, Ben Franklin's centuries-old advice still rings true: an ounce of prevention is worth a pound of cure. ❖

Notes

1. California Codes §1798.80, et seq.
2. Illinois Compiled Statutes, Act 530.

Alan S. Wernick (alan@wernick.com)

EM: ALAN@WERNICK.COM
T: 847.786.1005
URL: WWW.WERNICK.COM
LinkedIn: www.linkedin.com/in/alanwernick