



Health Care Data Breaches: Steps To Take When Prevention Fails

By James P. Walsh and Thomas R. Burke

[May 2006]

Despite elaborate plans and safeguards, private health care information is finding its way outside security systems in ways that threaten personal privacy. Just yesterday, the Department of Veterans Affairs announced that data on more than 26 million veterans was stolen off of an employee's laptop and external drive. These health care data breaches, such as thefts of laptop computers containing patient health care and financial information, are occurring more frequently. These security breaches also come at a time when both federal and state laws are expanding to protect against identity theft and public exposure of personal information of all kinds, in particular health care information.

A security breach is an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business. Personal information is a person's name, social security number, driver's license or state identification number, or account number, credit card number or debit card number in combination with any required security code, access code or password that provides access to an individual's account.

This outline is intended for those responsible for protecting private health care information when the security system, for one reason or another, fails.

I. The Problem

Security breaches have affected over 50 million people in the United States in the last few years. No company is immune, particularly from the theft of laptop computers. Here are some prime examples:

- Recently, an employee of a large Florida health insurance company pled guilty to Federal Court charges of stealing electronic information about 27,000 company employees in order to see how his pay compared to others.
- A college researcher at the University of California—Davis had his computer stolen that contained the name, age, gender, race, and HIV status of individuals using a local clinic.
- A woman trying to help a boyfriend in a custody battle obtained confidential patient information from her mother, an employee at a hospital. The patient information was then used in a mediation to show the unfit character of one of the contesting parties.
- Other events in the news include California, Oregon and Washington health care companies that suffered theft of computers storing health and other private patient information on thousands of individuals.

Despite every reasonable precaution, security breaches have occurred and will continue to occur.

II. The Legal Background in Brief

A. Federal Law

The Health Insurance Portability and Accountability Act (HIPAA) requires the Secretary of HHS to promulgate standards to protect private health information. Health care providers (hospitals, clinics, etc.) and health insurance plans must comply with the standards. 42 U.S.C. § 1320d-2; 45 C.F.R. Parts 160 and 164 (HIPAA Enforcement Final Rule) (71 Fed.Reg. 8391-8433 (Feb. 16, 2006)). HIPAA has created a Privacy Rule, for protection of health information and to deal with violations, and a Security Rule, for standards to guard electronic information.

A violation of the HHS Privacy Rule regulations may result in a civil penalty of \$1,000 per incident. Wrongful disclosure of individually identifiable health information is subject to criminal penalties of a fine of up to \$50,000 and a jail term of up to one year, or both. The criminal penalties increase significantly (up to \$100,000) if the disclosure is committed under false pretenses and with intent to sell, transfer, or use protected information for personal gain (\$250,000 and imprisonment of not more than 10 years). Multiple penalties involving both the Privacy Rule and the Security Rule are possible.

Under the Privacy Rule, a covered entity must mitigate, to the extent practicable, any harmful effect of an improper disclosure. Notice to the affected individual is one element of mitigation. A covered entity must also have and apply sanctions to those employees who violate HIPAA requirements.

HIPAA does not create a private right of action for persons whose health information is compromised. However, it also does not foreclose any other legal remedies an individual may have under either federal or state law should disclosure of private health information lead to damage or other injury. In addition, HIPAA sets standards that could provide the basis for civil law suits seeking damages.

B. State Law

1. Confidentiality of Medical Information Act

The California Confidentiality of Medical Information Act, Cal.Civ.Code § 56.10, prohibits disclosure of patient information without the permission of the patient, with some exceptions. Any patient whose medical information is disclosed and sustains an economic loss or personal injury is entitled to recover compensatory damages, punitive damages (not to exceed \$3,000), attorneys' fees (not to exceed \$1,000), and the costs of litigation. Cal.Civ.Code § 56.35.

Medical information is broadly defined as any individually identifiable information regarding a patient's history, mental or physical condition, or treatment. Among other exceptions, medical information may be disclosed to any person or entity responsible for paying for health care services to the patient. Other disclosures require written consent from the patient in a particular form.

2. California Data Protection Statute

In 2002, California was the first state to enact a data security law creating duties on the part of businesses when a security breach occurs. The statute applies to any person or business that conducts business in California and "owns or licenses computerized data" that includes personalized information. Calif.Civ.Code § 1798.82. The law applies to release of unencrypted information.

The data protection statute requires that persons and businesses “shall implement and maintain reasonable security procedures and practices” to protect personal information from unauthorized access, destruction, use, modification or disclosure. Calif.Civ.Code § 1798.81.5. However, this provision does not apply to entities covered by the Confidentiality of Medical Information Act or HIPAA, which contain essentially the same requirement. However, health care entities are subject to the data breach notification requirements in § 1798.82.

In the event of a security breach that compromised personal information, prompt notice must be given to any affected state resident. The notice must be:

- written and sent by mail; or
- by an electronic notice in conformity with the Federal Electronic Signatures Act; or
- if the costs of providing notice will exceed \$250,000, or if more than 500,000 consumers are affected, or if the business does not have sufficient contact information, by substitute notice through e-mail, website publication, or major state-wide new media; or
- in conformity with the business’s or institution’s own notification system, if it meets the timeliness requirements of the security breach notification laws.

The California data breach statute authorizes a private right of action for damages, which is in addition to any other remedy provided by law. Calif.Civ.Code § 1798.84(b). An injunction is also available to prevent further breaches. A waiver of any of the rights provided in the statute is unenforceable.

C. Possible Civil Causes of Action for Data Breaches

As experience with data breaches and new laws has grown, so have attempts to expand liability for data breaches, in particular through class action law suits. A good example is the case of *Eric Parke, et al. v. Cardsystems Solutions, Inc., et al.*, Case No. CGC-05-4426254, California Superior Court for the County of San Francisco (filed Jul. 5, 2005). The case is about a hacker attack on credit card databases for 40 million credit card holders. The breach allegedly occurred in May 2003 and was not disclosed publicly until July 2005. In addition to violations of the California data breach statute, the complaint alleges a variety of other causes of action, including negligence, unfair business practices under Business and Professional Code §§ 17200, and declaratory relief. The case has yet to reach a decision point.

The California Confidentiality of Medical Information Act has also been the subject of litigation. In *Colleen M. v. Fertility and Surgical Associates of Thousand Oaks*, 132 Cal.App.4th 1466 (2005), a woman patient sued for invasion of privacy and infliction of emotional distress because a clinic had given information to her ex-fiancée about her vitro fertilization. She had used her ex-fiancée’s credit card to pay the cost of the services. The Court of Appeal ruled that disclosure by the clinic was authorized as an exception under the statute to someone who was responsible for payment of a patient’s health care costs.

In other cases around the country, data breach or identity theft cases are being dismissed early because plaintiffs failed to prove that identity information has in fact been transferred to an unauthorized person. *Guin v. Brazos Higher Education Service Corporation, Inc.*, Case No. 05-668 (RHK/JSM), (D.Minn. 2006); *Stollenwerk v. Tri-West Healthcare Alliance*, Case No. 03-0185, 2005 WL 2465906 (D.Ariz. Sept. 6, 2005).

III. What to Do When the Security System Fails

Prevention is the very best way to avoid the consequences of a security breach. But if a security breach does occur, several steps are recommended, depending on the circumstances surrounding the breach. There is, of course, no perfect plan. And it is important to keep in mind that applicable notification laws are not entirely clear and often overlap.

A. Conduct An Investigation of the Incident

A single person should be put in charge of investigating the data breach incident, reporting to a senior company official. A decision should be made whether to include the company's in-house or outside attorneys in the process. Insurance coverage should be examined.

Thought should be given to issues such as attorney-client privilege and confidential communications, particularly if criminal violations are possible.

It may be necessary to hire computer or security experts to assist. Documents and information should then be gathered and safeguarded. Once the parameters are reasonably known, decision-makers should be informed of the results of the investigation.

B. Disclosures

Disclosure of a security breach may be required to various groups and entities, including the board of directors, stockholders, shareholders, employees, state and federal enforcement officials, government regulators, auditors, the public, and, of course, those whose information has been released. For each category, there should be an analysis of what disclosures may be required by law or policy.

The manner of disclosure is sometimes spelled out by statute and/or regulation and sometimes not. Care must be taken to meet all requirements to give notification. If in doubt, the broadest possible disclosure is probably appropriate.

Timing will be a big issue. Law enforcement may play a role in deciding when to announce a breach. Under the California data breach statute, disclosure must be accomplished in "the most expedient time possible and without reasonable delay." Disclosure should only happen after the incident is fully understood. Care should be taken in developing and implementing a disclosure plan.

The disclosures must be carefully crafted to avoid complicating the problem. To those affected, it should provide basic information about what happened, who might be affected, measures taken to avoid the problem in the future, and general guidance on what an individual should do to protect themselves.

The company should be prepared to provide responses to those who call in or otherwise contact the company for more information and guidance.

C. Fixing the Problem

Steps should be taken immediately to fix the problem that caused the data breach. This may include new computer security systems, additional training, or new company policies. Remedial measures should begin as soon as possible.

D. Contacting Government Agencies

The need to disclose a data security breach may require reports to various state and federal agencies, including law enforcement, licensing and regulatory agencies. Each should be approached with care and each contact documented. Success in handling relationships with these agencies can mean that the problem will not get bigger than mere notification. However, it is possible that further government investigation could be triggered.

■ Contact Information



James P. Walsh
San Francisco, California
(415) 276-6556
budwalsh@dwt.com



Thomas R. Burke
San Francisco, California
(415) 276- 6552
thomasburke@dwt.com

This Health Law Advisory is a publication of the Health Law Group of Davis Wright Tremaine LLP. Our purpose in publishing this Advisory is to inform our clients and friends of developments in health care law. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.

Copyright 2006 | Davis Wright Tremaine LLP