

Identity Theft Awareness and Coverage for the Healthcare Industry



William Gallagher Associates
Phone: 888.261.8884
www.WGAins.com

Data breaches cost the U.S. economy an estimated \$45 to \$50 billion annually. The highly publicized breach at TJX Companies (parent of TJ Maxx, Marshall's, etc.), compromised more than 100 million credit and debit cards and has already cost \$65 million in litigation settlements. When the dust finally clears, costs to TJX could exceed \$250 million. And while this case is not specific to the healthcare industry, it does give some evidence of the scope and size of the issue facing organizations that capture and retain a great deal of personal data.

According to statistics presented at the 2008 *American Society for Healthcare Risk Managers* Conference recently held in Boston, there has been a six fold increase in the number of incidents reported between 2004 and 2005. There has also been a more than double the number of incidents per week from 2005 to the latest reports in 2008. According to a recent study by the Identity Theft Resource Center, 15% of **all** data breaches were in the healthcare/medical industry. Another interesting note, of all the known data breaches, only 20% were from outside hackers.

William Gallagher Associates, a leading provider of insurance brokerage, risk management and employee benefits services to firms with complex risks, within industries that include high technology, life sciences, financial risks, healthcare services, energy, and environmental services. WGA has offices in Boston, MA; New York, NY; Hartford, CT; Princeton, NJ; Columbia, MD; Atlanta, GA; and Paris, France.

Many cases of identity fraud are not detected for months. In testimony before the U.S. Senate, a director within the Federal Trade Commission recently stated that an average of twelve months elapsed between the commission of a crime and the victim's actual detection. Within the healthcare industry, there is significant exposure to an organization given the extent of the non-public data and private information they retain. This fact makes it critical for healthcare organizations to address the issue of data integrity and security.

Recent Cases

In April 2008, the University of Miami reported a theft that occurred in March of more than 2 million medical records involving 47,000 patients. The records from the university's medical school were on six backup tapes that were being transported by a van for off-site storage. When the data was written to the tapes, it was coded by means of proprietary compression and encryption tools, so there is reason to believe that the thieves may fail to decode the tapes. Personal data stored on the tapes included Social Security numbers, patient names, addresses, and health information. The theft is presumed to be a random event.

Recently Blue Cross & Blue Shield of Louisiana compromised the personal data of about 1,700 insurance brokers via an e-mail, exposing information such as Social Security numbers, phone numbers and addresses. The data was accidentally attached to a general e-mail being sent out to brokers notifying them of a software upgrade. The company is now offering free credit monitoring to the affected brokers for twelve months.

The TJX case, which occurred from mid-2005 through 2006, remains the largest loss of data records ever reported. TJX was charged by the FTC with failure "to provide reasonable and appropriate security for sensitive consumer information." Although the agency didn't fine the retailer, it did impose conditions on the company, including system audits.

In 2008 alone, there have been over 15 million records either lost or stolen. The largest single case consisted of over 2.2 million records at the University of Utah Hospital and Clinics. In this case, a courier simply failed to deliver billing records to a storage facility. The breach contained over 1.6 million social security numbers from patients over the past 16 years. Other instances occurred in Brevard County in Florida and Harris County Hospital in Texas.

According to the Privacy Rights Clearinghouse, in 2005, a disgruntled Kaiser Permanente employee posted information on her blog noting that Kaiser Permanente included private patient information on systems diagrams posted on the Web. This resulted in a \$200,000 fine from the State of California for the exposure of confidential health information.

A more mundane but equally troubling example of this is a Pennsylvania hospital that discharged an employee who had access to patient records in the course of her work. When the employee was fired, her access to patient records was not restricted. In leaving her job, the employee took several patient records and left them on a local park bench. The employee then called the local newspaper to report “the theft”. The news headlines that were generated by this breach cost the Pennsylvania hospital millions in recovering the records and securing that the patient data was not used in an identity theft crime.

In a similar case, thousands of medical records were discovered in a Nevada storage unit that had been purchased for only \$25. This example demonstrates the low cost that is paid on the “black market” for such a large number of files and records.

Scope

Based on these and other data theft cases, experts say that data security is no longer an option for companies, regardless of size. Several experts have expressed doubts that there will be full compliance with recognized payment card security systems at the point-of-sales level any time soon. Compliance isn't likely to reach deep into the ranks of smaller entities. Health Care Organizations (HCO) with legacy systems may also be reluctant to make costly changes in their programs, especially when they must integrate with other, third party computer systems and software. Many have not used encryption for data flowing between their point-of-service payment processes and their system servers because the process requires too much computing power, capacity not found in many environments. Organizations without encryption software capability remain at risk for identity theft and fraud.

HCOs are affected each time there is a data breach of their non-public data and private information. There are direct and indirect costs associated with computer and network system breaches and identity theft. For example, there are the costs of investigation and forensic analysis; remediation and/or system upgrades; reputational damage; management time; business interruption; retraining employees; providing notification to law enforcement, business affiliates, service providers, state agencies, and customers; public relations; the possible insurance premium increases; payment card association-initiated or government fines; class action lawsuits; and legal fees and expenses.

There are several federal laws that require providers to protect non-public data. One of the most important of them is HIPAA. Other federal laws of importance to the healthcare industry are the Sarbanes-Oxley Act for publicly traded companies and the Identity Theft & Assumption Deterrence Act.

Forty-four states have adopted data breach laws that require the victimized company or institution to take remedial action and/or steps to mitigate losses. Massachusetts recently passed two of the most aggressive state responsibility laws to deal with data breaches and document destruction. Most state data breach laws require that the affected entity provide notification as soon as practicable. The new Massachusetts laws, which cover data disposition and destruction of personal information and biometric indicators, require that companies create and maintain policies regarding:

- Constructing and enhancing data security;
- Incident response time;
- Data breaches; and
- Data destruction.

Health Insurance Portability & Accountability Act (HIPAA) of 1996 (P.L. 104-191)

HIPAA requires that entities that handle medical data – including banks that may be contracted to process medical account data – assure the integrity, confidentiality, privacy, and availability of protected health information during collection, maintenance (including storage), use, and transmission. Covered firms, including healthcare providers, health plans, and healthcare clearinghouses, must have contingency plans that establish policies and procedures for responding to emergencies that may damage systems that contain electronic health information.

Section 244 of HIPAA makes it illegal for any person to knowingly and willingly falsify, conceal, or cover up a material fact, or to make any materially false, fictitious, or fraudulent statements or representations, or to make or use any materially false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry in connection with the delivery of or payment for healthcare benefits, items, or services.

HIPAA [Section 262 (1177 and 1179)] makes it a criminal offense for a person – knowingly and wrongfully – to disclose individually identifiable health information. A person who wrongfully uses or causes to be used a unique health identifier (of another person), obtains individually identifiable health information relating to an individual, or discloses individually identifiable health information to another person is subject to fines and a prison term. The penalties increase substantially if the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. It is not wrongful to use appropriate information for payment or medical treatment purposes.

Identity Theft & Assumption Deterrence Act of 1998 (P.L. 105-318; Title 18 USC §1028)

This law makes it illegal to “knowingly transfer or use without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”

Insuring the Risks

Data breaches and identity theft have been the subjects of much discussion in the insurance industry. Most insurers will now provide some financial protection for these hazards, either in stand-alone policies or through endorsements to other liability policies and riders to a crime bond. William Gallagher Associates is actively following the insurance markets for appropriate policies to address loss of data, breaches of security, loss or compromise of data storage hardware (including laptops), loss of paper files with confidential or privacy information, identity theft, identity fraud, extortion, destruction of records, and property losses.

Insurance is available for most computer network system risks including electronic storage; Internet, satellite, or wire transmissions; network database losses; theft of data during transmission; employee fraud; and malicious mischief. Coverage is also available for denial of service attacks and damage to software and hardware.

Healthcare providers are at risk of extortion if their databases, networks, or computer systems suffer a security breach. Providers have legal responsibilities to fully secure private and non-public data, including employee medical records. If a breach does occur, one or more insurance products will help ease the financial pain.

Insureds shouldn't overlook coverage for extortion, terrorism, and reputational remediation costs. Coverage, especially for drug companies, should include loss or infringement of intellectual and proprietary property, e.g., patents, trade and process secrets, and trade and service marks. Insureds should have coverage for losses associated with the use of employee data bases to instigate harassment, and data breaches – including paper records – to obtain private medical information or to obtain personal information, such as email addresses, without authorization.

Insureds should include coverage for any off site hardware systems, back-up media, the transportation of data storage media to and from off premises sites, and off site records retention. Include any records that are retained for business reasons or regulatory compliance.

Insurers generally will cover any data losses caused by a computer system breach. Typical coverage includes network breaches, laptop losses, and loss of or damage to paper records and storage media. When purchasing insurance for data breaches, the insured will want broad coverage, including unauthorized additions to or deletions from the database, and the corruption or destruction of records. Insureds that have international exposures need worldwide coverage, not only for the location where an insured event may take place, but also for litigation by foreign parties in foreign jurisdictions.

Losses associated with violations of regulations that mandate privacy data protection are usually covered by the policy, but there may be exceptions, limitations, and exclusions. Insureds need to look at federal and state requirements regarding notifications of a breach of data security or an unauthorized disclosure of private information. Many insureds will also need to ensure that there is coverage for violations of foreign statutes, regulations, and common law regarding breaches of privacy and data theft. Some insurers provide limited coverage for other violations, such as unfair competition or anti-trust activities.

Please contact Peter Reilly, Leader of WGA's Healthcare Practice, should you have further questions regarding identity theft coverage at preilly@WGAINS.com or at (609) 228-1607.

