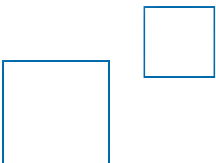




Low-Tech is the Path to HITECH

2	Introduction
3	Challenges Unique to the Healthcare Industry
5	Meeting the Challenges
6	Know Your Data: At Rest, in Use, and in Motion
7	Know Your Employees: Training and Communication
8	Know Your Partners: Third-party Risks and Responsibilities
9	Know Your Incident Response Plan: Comprehensive and Tested
11	Conclusion



Kroll strives to provide accurate, up-to-date information, but our materials should not be deemed as legal advice or counsel, but rather as supplemental material offered as an educational component to Kroll's services.

Introduction

The Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law in February 2009, as part of the American Reinvestment and Recovery Act (ARRA). Prior to HITECH, breach notification had been a somewhat murky subject, allowing data breaches at healthcare facilities to go unreported. Moving forward, this will not be the case. HITECH addresses gaps in the current HIPAA provisions – namely, that covered entities will generally be required to disclose to patients any security breach that exposes their Protected Health Information (PHI) to unauthorized persons. Furthermore, notification must be made no later than 60 days after “discovery” of the breach, or whenever the breach is known by either a third party vendor or the covered organization itself.

Patient-focused healthcare organizations will strive to implement policies and procedures to protect PHI and Personal Identifying Information (PII) as a measure to safeguard against data breaches and incidents of identity theft. This will require a complete understanding of the use, storage and access of all data, implementing employee training and communicating policies and procedures, recognizing the risks and responsibilities of third parties, and developing a comprehensive incident response plan.

An important caveat that healthcare organizations should remember: the path to HITECH compliance does not solely lead to the IT department. Though detecting and securing data through

technology is an important component, human error or malicious employees are problems that cannot be solved through technology alone. In 2008, over 88 percent of all data breach cases surveyed involved incidents resulting from negligence.¹ Per-victim cost for data breaches involving negligence cost \$199 per record, compared to malicious acts costing \$225 per record.²

A dependency on technology to “stop” a security breach promotes the dangerous (and often costly) assumptions that a breach is preventable and that technology is the key to compliance. In fact, survey data shows that when organizations have breached, training and awareness programs lead companies’ efforts to minimize their risk of future breaches.³

Even with the passing of the strictest privacy and data security legislation to impact the healthcare industry since HIPAA, one recent survey reveals that over half (53 percent) of surveyed respondents in the healthcare data security industry do not believe that their organization takes appropriate steps to protect the privacy rights of patients and comply with legislation and industry regulations.⁴

¹“2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.

²“2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.

³“2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.

⁴“Electronic Health Information at Risk: A Study of IT Practitioners,” October 2009, Ponemon Institute.

Challenges Unique to the Healthcare Industry

Is healthcare at a disadvantage as compared to other industries?

The healthcare industry is undergoing significant changes – providers are spending a considerable amount of time and money on updating and revising systems to accommodate electronic health records. This change, while important, will bring new burdens for security. Covered entities are already tasked with the double responsibility of safeguarding a client's PHI, as well as PII, such as names, addresses, Social Security numbers, credit card numbers, or other account numbers. Unlike other industries, healthcare will now be responsible for following both state and federal notification requirements for the first time.

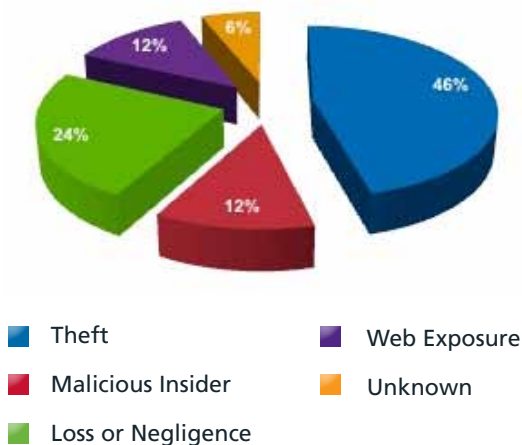
How prevalent is the problem of data theft and loss in healthcare?

Since January 2008, over 110 healthcare organizations have reported the loss of sensitive PII affecting in excess of 5,306,000 individuals.⁵ Over 46 percent of these reported data loss incidents were caused

by theft (stolen laptops, computers, or media/tapes). The remaining 24 percent were the result of loss or negligence by staff or third parties, 12 percent were caused by malicious insiders and 12 percent were caused by web exposure.

A recent study found the average value of a lost laptop for entities surveyed was \$49,246.⁶ However, the cost of a lost laptop varied by industry. The average cost of a lost laptop for a healthcare organization was \$67,873, and a pharmaceutical company averaged \$50,393.⁷

How Data is Lost



Cost of a Lost Laptop



- Lost Laptop (Avg.)
- Healthcare Organization
- Pharmaceutical Company

⁵ www.datalossdb.org, accessed 11/1/2009

⁶ "The Cost of a Lost Laptop," April 2009, Ponemon Institute.

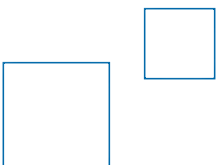
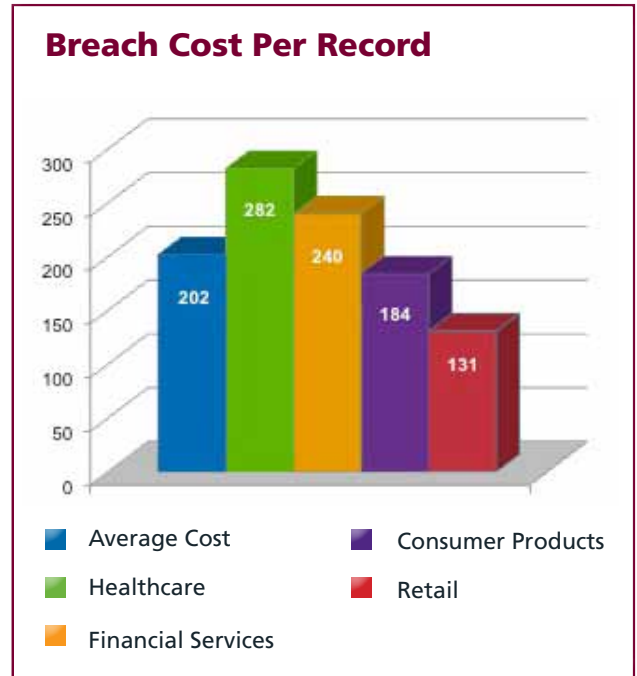
⁷ "The Cost of a Lost Laptop," April 2009, Ponemon Institute.

What is the effect on patient care and/or satisfaction levels?

While it is difficult to gauge the long-term effects of data loss or ineffective security on patient care, one telling aspect is that of consumer churn within healthcare. Healthcare organizations that have breached patient data have the highest average rate of consumer churn – 6.5 percent followed by financial companies with a churn rate of 5.5 percent.⁸ These high churn rates demonstrate that consumers are concerned enough about a breach of this data to terminate their relationship with an organization. Additionally, the average cost of a healthcare breach (\$282) is more than twice that of an average retail breach (\$131) and is 39 percent higher than the overall average cost of \$202.⁹ This is an indicator that consumers may have a higher expectation for the protection and privacy of their healthcare records and personal information.

⁸ “2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.

⁹ “2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.



Meeting the Challenges



Corn 1966
Euro 95020
Cattle 8640

Lumber 26840
US T-bond 9623
Flaxseed 2195

Wheat 4575
Nat. Gas 4967
Lean Hog 4967

Silver 4958
Franc 6165
Euro 3000

Mark 4889
Peso 95750

Silver 4958
Franc 6165
Euro 3000

Mark 4889
Peso 95750

Suber 866

Propane 866

Lumber 26840
US T-bond 9623
Flaxseed 2195

Gold 26840
Euro 97295

Corn 1966
Euro 95020
Cattle 8640

Know Your Data: At Rest, in Use, and in Motion

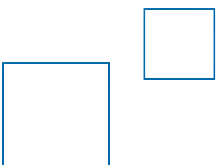
Healthcare providers are prime targets for a malicious or accidental breach because:

1. They are data-rich organizations: virtually everyone requires healthcare assistance at some point in life.
2. The patient, along with his or her data, moves through the healthcare system - in and out of the ER, changing insurance, pharmacies, and doctors.
3. Healthcare data has a high “touch-point” and is handled by many different people throughout the process.

With data moving in, out, and around a healthcare organization, the burden of protection includes data at rest (in an Electronic Health Record or on a paper chart), data in use (accessed at the point of care), and data in motion

(transferred from one location to the next). Stored data also frequently contains inactive patients, as well as those who are difficult to notify in the event of a breach, such as minors or decedents.

At the most basic level, healthcare organizations should inventory and map patient data flow, as well as coordinate and develop processes and procedures for sharing and protecting this data both internally and externally. A good place to start is by assessing various departments within the organization – ask basic data questions of employees within IT, human resources, the billing department, and catalog the responses to get a comprehensive picture. Encourage staff to detail the ways in which data is used, retained, or accessed to provide insight. This will help in identifying poor practices within the organization such as collection of unnecessary data, inconsistency in data handling, and improper storage.



Know Your Employees: Training and Communication

Providing excellent care starts with an organization's employees – every individual that a patient, or “customer” comes in contact with must be mindful of the role they play in safeguarding patient information.

In addition to building awareness of risk by balancing education, training and technology, healthcare organizations, as a best practice, should properly screen employees who potentially have access to patients and their data. Background screening is not a panacea for employee hiring and training, but a thorough background check performed by a reputable third-party can alleviate risk to patients and clients by detecting criminal histories, derogatory financial histories, and instances of professional misconduct. Screening for these “red flags” reduces the risk of a patient's exposure to negligence and fraud.

Train to Be the Best

When surveyed about how their organization attempted to secure and protect patient data, the majority (81 percent) of IT practitioners who responded identified “Policies and Procedures” as the top method followed by “Training and Awareness Programs” (67 percent).¹⁰ With such

emphasis placed on training, it is imperative that healthcare organizations make training part of the culture rather than just the “required” act of signing an agreement. In addition, as employees of healthcare organizations have widely varying responsibilities and points of touch with patient data, it is important to construct a training program that is relevant to job function and level of sensitive data handling.

Rather than creating excessive training, the goal should be to make necessary pre- and post-breach training a part of the overall program. For healthcare organizations, the primary focus should be on privacy and security breach prevention and detection. Healthcare employees must be trained to detect and report a breach as the notification 60-day “stopwatch” starts when they knew or “reasonably should have known” that a breach occurred. Furthermore, to encourage detection and escalation of an incident, a “whistleblower” hotline can facilitate and expedite breach reporting.

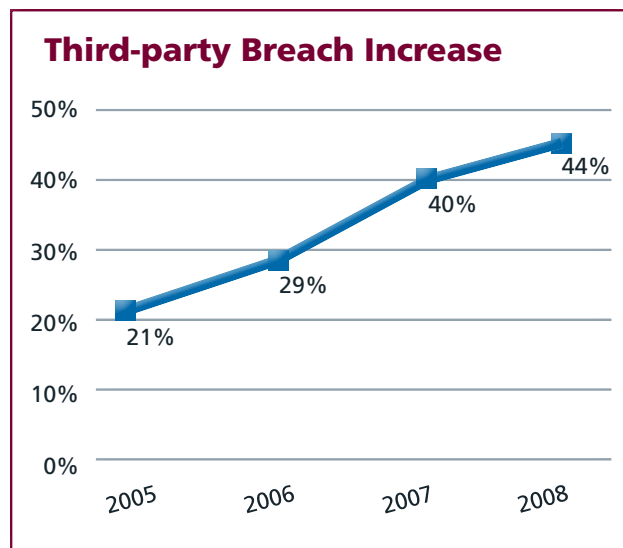
¹⁰ “Electronic Health Information at Risk: A Study of IT Practitioners,” October 2009, Ponemon Institute.

Know Your Partners: Third-Party Risks and Responsibilities

Healthcare organizations, or “covered entities,” are legally responsible for the oversight of their business associates. When a covered entity’s business associate discovers a breach of PHI or PII, they are only required to notify the covered entity of such a breach, including the identity of each individual whose information has, or is reasonably believed to have been, breached. In contrast, the covered entity is responsible for notifying those affected no later than 60 calendar days after the first day on which the business associate knew or reasonably should have known of the breach.

For this reason, it is imperative to perform “due diligence,” making sure partners’ or vendors’ privacy and security policies and procedures meet the healthcare organization’s requirements. Do they stringently screen employees? When a data breach occurs, do they have a method by which they can accurately scope the damage to ensure proper notification? Do they have an incident response plan in place to ensure client organizations receive notice of a security breach in a timely manner? The clock starts with their mistake.

According to the Ponemon Institute, breaches by third-party organizations such as outsourcers, contractors, consultants, and business partners were reported by 44 percent of respondents in 2008, up from 40 percent in 2007.¹¹ This upward trend continues to rise year after year. Per-victim cost for third-party breaches is \$52 higher (e.g., \$231 vs. \$179) than if the breach is caused by an internal source.¹²



¹¹ “2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.

¹² “2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.



Know Your Incident Response Plan: Comprehensive and Tested

Apart from employee training and proper screening for third-party vendors, all healthcare organizations that deal with PHI and PII are under pressure to develop and implement a breach preparedness and actionable incident response plan. Under HITECH, covered organizations that breach patient data have only 60 days to properly assess the scope of a data breach, and then thoroughly and accurately navigate the notification process. Similar state laws also encourage holders of sensitive data to be prepared to respond to a breach.

Response Plan

Responding involves knowing the full impact of the breach, properly notifying, and providing a comprehensive solution to those affected.

Scope

When the scope of a data breach is properly assessed, the affected organization will be able to appropriately service the needs of the impacted population. This includes recognizing and differentiating among the unique and sensitive populations that may be affected including minor children, decedents, and those living abroad.

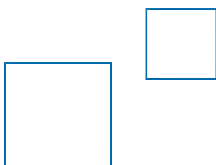
Notify

Notification is the next step after determining which individuals are at risk. HITECH mandates notification and has specific requirements as to what must be included within the notification letter.

However, HITECH is only one side of the legislative landscape. The Centers for Medicare and Medicaid Services (CMS), also requires notification, and any healthcare organizations can be subject to CMS through contracts, agreements, and partnerships. CMS holds entities to a contractual obligation to notify within a certain timeframe based on the type of incident; CMS must be notified as early as one hour, or as late as one week, after breach discovery.

Healthcare organizations that attempt to notify using internal resources often commit the costly mistake of foregoing compliance with state laws. It is important for organizations to remember that compliance with HITECH, CMS, and other federal regulations does not automatically negate the need to comply with state legislation. Because many states include health information in the definition of “PII,” HHS mandates that both federal and state laws must be followed. Healthcare organizations that breach both PII and credit card numbers, for example, must comply with both state and federal statutes.

Not having a comprehensive response plan that is suited to comply with both federal and state regulations can be detrimental. Not only will healthcare organizations be subject to federal sanctions, but they will also be subject to state fines for violations of non-compliance.



Communicate

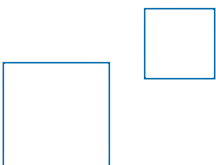
There will be both internal and external inquiries once the incident is known. An organization should designate a communications “team” and establish procedures for delivering a clear, concise, organized, and consistent message.

Remediate

Identifying the scope of a breach also involves understanding the potentially negative impact the breach can have on a healthcare organization’s brand, reputation, and patients. Due to the sensitivity of patient PHI and PII at risk after a healthcare data breach, simply notifying the affected is not enough to protect them from the risk of medical and financial identity theft. In order to truly safeguard data, organizations must make a shift in focus – the “caregiver” philosophy so prevalent within this industry must be extended to patient and employee PHI and PII.

Furthermore, with the risk of a 6.5 percent churn rate and additional data showing that lost business continues to dominate the cost of a data breach, accounting for 69 percent of data breach costs,¹³ a healthcare organization cannot afford to be unprepared. An organization’s remediation plan must match the risk of the data loss.

¹³ “2008 Annual Study: US Cost of a Data Breach (Understanding Financial Impact, Customer Turnover, and Preventative Solutions),” February 2009, Ponemon Institute.



Conclusion

It is important to know the risk factors – keep in mind that healthcare organizations are data rich and are prime targets for a malicious or accidental breach. If an organization is caught unprepared, they will now find themselves with 60 days to put a written incident response plan into action, assess the scope of the breach, and thoroughly and accurately navigate notification of the affected population.

Data security must be thought of as a long-term goal, rather than a stop-gap application. To enact a long-term plan and commitment to security and data, organizations must follow these key steps:

- Understand the what, where, and when of the data housed within the organization, and then determine how and why it is accessed, used, or transported.
- Recognize that hiring best practices are an important component in security, as is training and communication.
- Assess the importance of performing due diligence with third-party vendors and making them aware of their responsibilities in keeping patient data safe.
- Examine the steps needed to actively prepare, respond, and prevent (or minimize) the risk of a reoccurrence through a comprehensive and tested response plan.

Kroll Fraud Solutions
866 419 2052
www.krollfraudsolutions.com
www.kroll.com

