Managing Health IT Security and Privacy Risk

Integrated Compliance Management

Overview

Maintaining the privacy and security of patient's protected health information (PHI) is a challenge for every health care organization and a concern of every person. The health care industry relies on private, sensitive data whose access should be limited to only those who need it for patient care. However, because there are many activities and services within the health care industry that use PHI, this increasingly opens up the opportunity for a data privacy or security breach.

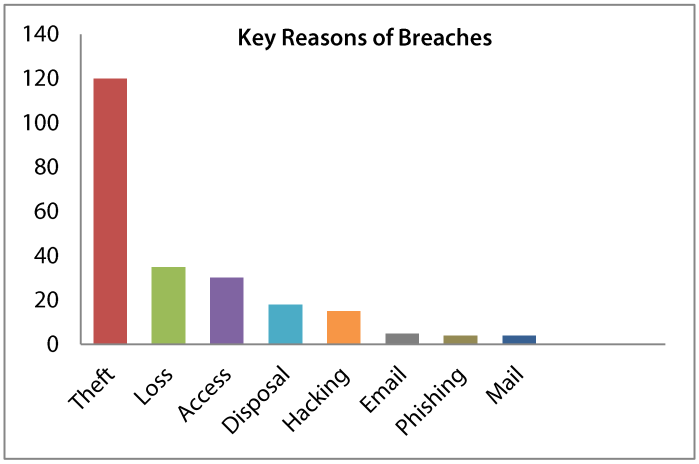
PHI is transferred from computer servers to laptops, USB drives, and smart phones. Information is copied into spreadsheets, databases and emails. Simply by its use and transmission, PHI can be at risk of unauthorized or unlawful disclosure. PHI carries a significant price tag for collection, protection, storage, and maintenance. It also carries a significant potential dollar and reputation cost if it is misused or lost. Consider the major data loss recently suffered by a large health maintenance organization. To deal with the event, required postal notification and one year of credit report monitoring to be provided to almost 300,000 customers whose PHI was compromised.

The health care industry is affected by data fraud and identity theft as it creates, collects, and stores billing records. This has unfortunately led it to be the leader in the number of data. The increase in data breaches has been attributed to gaps in federal privacy regulations, lack of enforcement of existing legislation, increased automation, use of social media, human curiosity, and the potential of financial gain through misuse of PHI.

It wasn't until 2010 that breaches were publicly reported to the U.S. Department of Health and Human Services (HHS). Initial breach statistics have identified human error as a leading cause of data breaches. Thus, stronger policies and procedures and on-going compliance can make a significant difference for any organization.

The Facts on Breaches

Since the enactment of the Health Insurance Portability and Accountability Act (HIPAA) in April 2003, the Department of Health and Human Services (HHS) has investigated over 20,000 violations. Since the enactment in September 2009 of the Breach Notification Rule, over 21 million individuals have been affected by data breaches. Over 70% of the breaches reported were by health care providers. The major causes of the breaches were theft, loss of media containing PHI, and unauthorized access. Hacking, which is often thought to be the major cause of data breaches, was identified as the cause of less than 10% of all PHI breaches. From a hardware and records viewpoint, most breaches occurred from laptops, desktops, and paper reports.

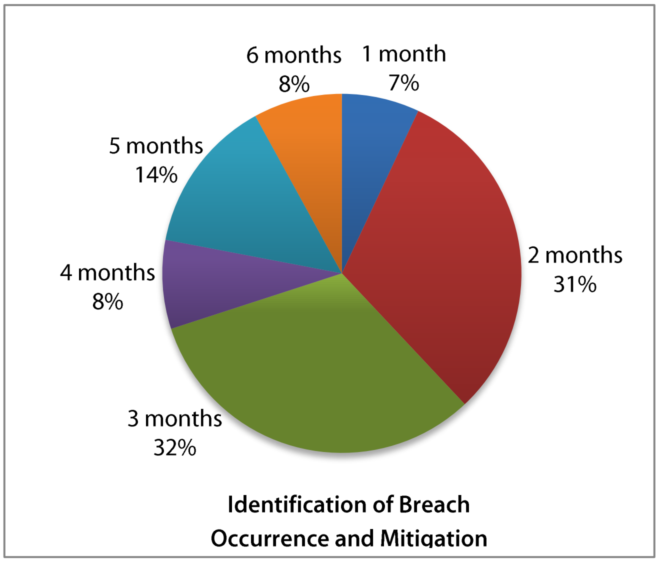


Source: HHS Statistics

The negative consequences of data breaches can be significant; monetary penalties, damage to reputation, and lost revenues. The total annual economic impact of data breaches on U.S. hospitals alone is estimated in the billions. Still most health care organizations have little or no protection in place to prevent, monitor, or remedy data breaches. At the same time, organizations have only committed limited funding to implement privacy and security safeguards. As the healthcare industry moves towards the increased accessibility provided by electronic health records (EHR), even more data will be at risk.

Theft and misuse of sensitive data such as SSNs, insurance identification numbers and payment information is often undetected for long periods of time. PHI can be vulnerable to a breach in any of the recognized data states:

- Data in Motion – data moving through a network
- Data at Rest – data that resides in databases, file systems, external media
- Data in Use – data in the process of being created, retrieved, updated or deleted
- Data Disposed – discarded paper records or recycled electronic media



Source: HHS Statistics

Current State of the Industry

According to health care industry and technology analysts, the current state of security and privacy readiness is poor.   Key causes include limited internal resources, lack of internal control over patient information, lack of upper management support, outdated policies and procedures, and inadequate training.

Based on a summer 2012 survey of hospital compliance officers, almost 75% were not in full compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH). It is no surprise that reported breaches continue to increase resulting in 41% of hospitals now having 10 or more data breaches annually. According to a fall 2011 Healthcare Information and Management Systems Society (HIMSS) Security Survey, over 50% of health care executives reported that information security expenditures are less than 3% of their IT budget. While security awareness continues to increase, the corresponding organizational readiness has not.

A 2012 HIPAA compliance sample of covered entities (CEs) (i.e. health care providers, health care clearinghouse, and health plans) showed that a majority had not performed a risk assessment nor had documented standards and procedures in place. Risk assessments that were present were out of date and/or missed critical risks.   Staff negligence and incomplete security policies were identified as two top causes of data being at risk. Compared to providers, business associates (BAs) (those organizations that receive PHI from health care providers) (i.e.   legal and accounting firms, medical transcription and translation firms, shredding companies, etc.) are behind in all areas of HITECH awareness despite new criminal and civil penalties applying to most BAs.

HHS issued the Privacy Rule to implement the requirements of HIPAA. The Privacy Rule standards discuss the use and disclosure of individual health information known as PHI. The security rule specifies a series of administrative, physical and technical safeguards for covered entities to ensure the confidentiality, integrity and availability of electronic PHI. The rule originally only affected CEs.

The HIPAA Security Rule operationalized the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that CEs must implement to secure individual PHI. The HITECH act also expanded this requirement to BAs. Lastly, the HITECH Act requires CEs and their business associates to provide notification following a breach of protected health information.

What is a breach? A breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational or other harm to the affected individual. CEs and BAs have the burden of proof to demonstrate that the use or disclosure of unsecured PHI did not constitute a breach or if it constitutes a reportable breach, all required notifications have been provided.

It can be difficult to meet the expanded HIPAA requirements as data security can at times be considered time consuming, disruptive, and restrictive. Additionally, responsibility has shifted to providers to manage the downstream security and privacy of PHI processes by BAs and other third parties.

The potential for health plan privacy and security breaches is substantial. Many health plans have outdated privacy and security practices and do not have control of third party PHI use.   The ever increasing government mandates and requirements are adding additional IT risk and making an already difficult task even more so.

The push toward 90% EHR adoption rate, implementation of HIPAA 5010, and ICD-10 is likely to increase outsourcing and subcontracting of various data processing activities. Third parties that provide these services may use outdated procedures or be less demanding in terms of privacy, security policies, and procedures than CEs. Complicating matters is that some outsourcing partners operate off-shore where

HIPAA requirements are unenforceable.

So What Should You Do

It is extremely important that security and privacy considerations and risks not be forgotten. What is needed is a comprehensive and rigorous security program that focuses on managing risk and reducing the potential for a PHI/data privacy breach. Simply launching an emergency or once a year compliance project may help you pass an audit but it is not providing your organization with protection against data breaches, hacking or employee negligence and fraud. You need a security based approach that:

- Considers critical organization priorities and technology risks
- Combines multiple regulatory and contractual requirements into one effort
- Considers servers, workstations, laptops, mobile devices, and non-electronic data
- Integrates compliance into daily operations instead of a standalone project
- Maintains compliance over time

The HITRUST or HHS ONC security frameworks can be used as a basis for a strong organization security posture but it is just a framework. In order to reduce your organization's risk, *a structured, repeatable process that is straight forward and efficient is required.*

You probably have talented individuals in your organization with many of the skills required to put an effective security and privacy program in place. You'll want to implement a repeatable process to identify current risks, mitigate the gaps identified and train responsible staff to continuously monitor and maintain the environment.

Putting a strong compliance foundation in place will reduce the potential for a breach and help avoid a costly fire drill when a breach or security incident occurs. It will also make any audits go smoothly with minimal disruption to your organization. Described below is an integrated security and privacy compliance readiness process.

Readiness Approach

Process Area	Objective	Benefits	Activities
Risk Assessment	Identify and assess data and security risks	Allow organizations to make effective decisions on security remediation priority	• Perform organizational risk assessment • Assess current business processes, systems and external factors for risk
Risk Mitigation	Determine and implement corrective actions to remediate security and privacy gaps	Reduces risk of data breach or security problem that could cause revenue and reputational loss	• Develop action plan to remediate gaps and mitigate identified risks • Create security and privacy policies and procedures • Develop and perform security awareness training • Implement data encryption, user and role based access and identity management to manage secure access to PHI
Security & Privacy Governance	Develop risk management organization responsible for monitoring and maintaining compliance	Creates baseline standards for secure handling of patient information. Creates organization wide awareness of data privacy and security policies	• Implement compliance organization structure and key activities • Perform project management and status reporting • Conduct regular internal and third party security audits • Perform regular security awareness training
On Going Compliance	Perform on-going risk monitoring, identifying and remediating gaps and weaknesses and coordinating resources	Reduces organizational risk, creates customer confidence in an organizations protection of PHI. Reduces potential for financial penalties due to negligence	• Monitor and log adherence to security and privacy policies and procedures • Perform on-going identification and remediation of gaps

Conclusion

Data privacy breaches continue to be a concern. The new health care IT environment will be information driven, connected and transparent exposing organizations and patients to increased privacy and security risks. Unfortunately, unless addressed, with the proliferation of data and mobile computing we will also see an increase in the number of breaches. Since the majority of breaches occur from theft and data loss, enhanced policies, procedures, and training can make a difference.

Organizations should act now to prevent compromising sensitive patient data, preserve brand value, and avoid substantial financial penalties for violations. Most organizations are still in a reactive mode. Implementing an integrated compliance framework will reduce the risk of breaches, limit the effect on day to day operations of security and privacy fire drills, and provide auditors and regulators the compliance information they require.

How We Can Help

To have a deeper discussion about managing health IT security and privacy risks, please contact:

Robert Zimmerman
rzimmerman@qipsolutions
301-802-1925

Eric Hummel
ehummel@qipsolutions.com
703-980-3378

qipsolutions.com