Developing Robust Data Management Strategies for Unprecedented Challenges to Healthcare Information

Latasha Blake
Prairie View A&M University

Vanessa Francis
Prairie View A&M University

Janice Johnson
Prairie View A&M University

Muhammad Khan
Prairie View A&M University

TaShauna McCray
Prairie View A&M University

Healthcare organizations face unprecedented challenges of developing robust data management strategies to safeguard against the loss of consumers' personal, medical, and financial information. Although experts have developed frameworks to decrease the risks of breaches, organizations and consumers remain vulnerable. Based on a review of the literature the authors concluded that healthcare organizations and government officials must take the necessary steps to bridge gaps posing significant risk to the electronic health information of consumers. This paper explores data breaches in healthcare based on the sources of breaches, governmental regulations, financial impact, while recommending improvement tactics focused on detection, mitigation, and prevention.

INTRODUCTION

Technology has shaped the world as we know it today. From computers to tablets to cell phones, technology is readily available and has changed the phenomenon of convenience forever. With just a few clicks of a button, consumers can quickly purchase goods, pay bills, learn about a new medical diagnosis, and view their electronic health records. While consumers enjoy the electronic amenities that improve efficiencies, productivity, and effectiveness, it is assumed that the electronic exchanges are private and secure, but are they really? The answer in many instances is no, which leaves many consumers vulnerable, thus exposing their personal identifiable information to data breaches.

A security or data breach is described as the "compromise of the security, confidentiality, integrity or loss of electronic data resulting in unauthorized attainment of sensitive personal identifiable information" ("Legislative Language," n.d., p. 1). Sensitive personal identifiable information (i.e., social security numbers, addresses, phone numbers, etc.) is valuable to cyber criminals and is considered expensive on the black market. One small error can lead to breaches that affect millions of consumers. With thousands of employees having access to consumers' personal identifiable information, is a challenge to ensure that this information is secure. Studies show that employee error, both intentional and unintentional, is a leading cause of data breaches (Neray, 2011; Willison & Warkentin, 2013). Federal laws and regulations are in place that require entities to secure personal information, but compliance has been inconsistent.

The healthcare industry sees high volumes of data breaches due to cybercrimes. Interestingly, cybercrimes are now considered the new healthcare crisis (PR Newswire US, 2015). Threats attributed to cybercrimes include hacker attacks, staff negligence, third parties (i.e., physician offices, insurance companies, and outsourced vendors), and loss or unsecure devices such as laptops, tablets, cell phones, and media storage (Eddy, 2014). Additionally, federal regulations requiring healthcare providers to migrate to electronic health records and healthcare exchange systems have made the healthcare industry more of a target (Eddy, 2014).

Data breaches in the healthcare industry have a tremendous cost. McMillan (2015) suggests that enterprises incur many direct costs for breaches, including costs associated with "discovery, response, investigation, and notification" (p. 46). To add to this cost, the Office for Civil Rights (OCR) has increased the fines applied to "willingful neglect" from $25,000 to $1.5 million per violation (Chaput, 2014, p. 22). Consequently, industries spend millions of dollars on data security efforts to prevent data breaches. The problem lies in the fact that many enterprises inadequately budget for electronic data management security efforts due to lack of understanding of risks (McMillan, 2015). This paper will explore the exposure, risk, regulations, reporting, financial impact, and preventive measures for healthcare data breaches.

HEALTHCARE DATA BREACHES: EXPOSED

The federal government has developed strategies to automate patient health records to improve quality, safety, efficiency, and the overall cost-effectiveness of care delivery. With these changes came increased threats of data breaches and cybercrimes (Merisalo, 2015; Neray, 2011). In fact, from 2010 to 2015, healthcare organizations have seen a 125% increase in security breaches (Khan & Hoque, 2015). In 2015 alone, approximately 10 million patient health records were compromised due to security breaches (Flower, 2016). Likewise, in the first half of 2016, the number of compromised patient health records increased to 11 million (Flower, 2016).

Risk of Exposure

The risk of data breaches has increased immensely due to the lack of robust data security plans and systems (Merisalo, 2015). The challenges that the healthcare industry faces are often compounded by limited resources and reach (Chaudhary & Ward, 2014). The healthcare sector is considered a late adopter of electronic data exchange, in comparison to other industries such as finance and retail (Chaudhary & Ward, 2014). However, recently efforts have been made to align with other industries.

Exposure of Data on the Bottom Line

The root causes for data breaches sustained by healthcare organizations included hacker attacks, lost or stolen electronics, accidental employee disclosures, third-party glitches and data leakages, and system malfunctions (Aldhizer & Bowles, 2011; Beeskow, 2015; Free, 2014; Merisalo, 2015; Neray, 2011). The industry must realize and accept that there is a problem before the problem can be solved. Protecting valuable customer information should be of the highest importance at all levels of an organization (Klie, 2015). Nevertheless, to mitigate the risk of data breaches associated with technological advancements, healthcare organizations should conduct detailed data security risk assessments; evaluate processes, policies, and procedures centered around privacy and security and patient health information; install database security and activity monitoring technology; and develop a robust training plan for frontline staff (Free, 2014; Merisalo, 2015; Neray, 2011).

Whether by way of cyberattacks or government fines, data breaches in the healthcare industry have a significant financial impact on individuals and organizations. Interestingly, breaches expose hundreds of patient records and have cost the healthcare industry an estimated $6.2 million overall, with more than one breach occurring per month within the last two years (Higgins, 2016). According to 2015 and 2016 data breach studies, the average cost of data breaches in other industries, such as retail or education, is $154 per record; however, data breaches cost healthcare organizations $363 per record (Khan & Hoque, 2015; Ponemon Institute, 2016). Nonetheless, identity theft cases dropped when states adopted data breach and notification laws (Sullivan & Maniff, 2016). The federal government has sued and levied fines against large healthcare institutions for inadequacies noted in data security frameworks and failure to notify consumers timely when data breaches occurred.

Preventing Data Breaches: A Deep Dive

The United States is facing a growing concern with cybersecurity beyond government, financial, and educational institutions. According to the Ponemon Institute's *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data*, approximately 90% of healthcare service providers have experienced a data breach (Ponemon Institute, 2015). In *Follow the Data: Analyzing Breaches by Industry. Trend Micro Analysis of Privacy Rights Clearinghouse. 2005–2015 Data Breach*, the Forward-Looking Threat Research (FTR) team discussed data trends for breaches between 2005 and 2015 (Huq, 2015). The report explores many variables, including industry, method of breach, and the type of records breached. The author identified the increasing frequency of breaches across industries and noted a major shift in the number of healthcare breaches since 2010 (Huq, 2015). Also, Huq (2015) noted that the most frequently reported breach method was not malicious hacking or fraud; rather, two-thirds of the breaches resulted from the loss or theft of portable devices, backup drives, files, laptops, office computers, and other devices.

Dynamic Regulations

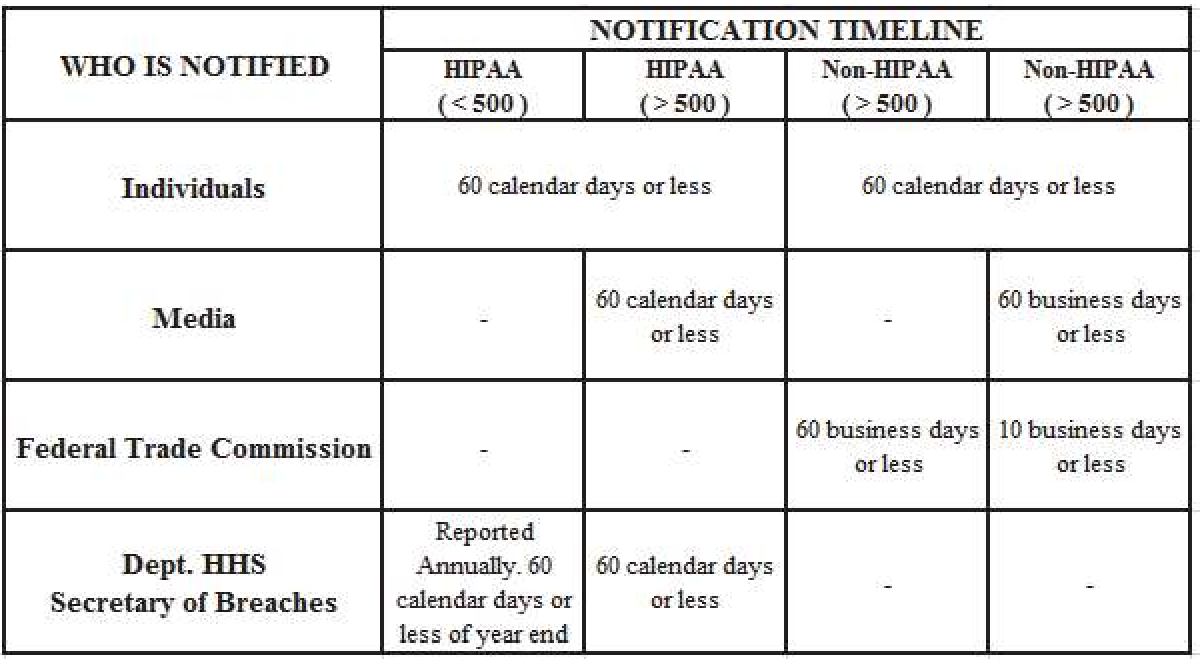
As the number of data breach instances increases, the need for data breach protection legislation becomes increasingly important. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 sets federal standards for securing electronic protected health information. The HIPAA Privacy Act requires that covered entities apply safeguards to protect the privacy of any form of protected health information (U.S. Department of Health and Human Services, 2009). It also requires policies and procedures for the proper handling and disposal of electronic protected health information and the media on which it is stored (U.S. Department of Health and Human Services, 2009). Additionally, the Federal Information Security Management Act (FISHMA) was implemented as part of the Electronic Government Act of 2002. It introduces a comprehensive model to protect government information, operations, and assets against natural or manmade threats like cybercrimes.

In 2009, President Obama signed the Health Information Technology for Economic and Clinical Health Act (HITECH Act). This legislation was created as part of the economic stimulus bill called the American Recovery and Reinvestment Act (ARRA) of 2009. Its purpose was to support the advancement of technology in the United States by encouraging the adoption of electronic health records (Stevens, 2010). With the enactment of the Affordable Care Act (ACA) of 2010, the healthcare industry has shifted from hard copy to electronic documentation for all components of Medicare patients' medical records (U.S. Department of Health and Human Services, 2010). Based on this act, healthcare providers (organizations, insurance companies, and medical providers) were charged with transitioning to electronic health records in an effort to decrease paper documentation, administrative demands, cost, and medical errors and to improve the quality of care delivery (U.S. Department of Health and Human Services, 2010) to improve care delivery, efficiencies and communication among healthcare providers. All of these pieces of legislature have data protection requirements that healthcare providers must adhere to prevent lofty fines. Unfortunately, compliance has varied across the industry due to differences that the healthcare organizations have with the government.

Reporting Data Breaches

When a breach occurs, organizations are required to notify affected individuals, the regulatory agency and in some cases the media. The notification timeline and the regulatory agency to be notified is based on whether or not the organization is covered by HIPAA laws and the number of people affected by the breach. HIPAA covered organizations are required to report breaches to the Health and Human Services Secretary of Breaches while organization not cover under HIPAA laws must report breaches to the Federal Trade Commission (FTC). Table 1 below summarizes breach notification requirements for healthcare organizations.

TABLE 1
HEALTH INFORMATION DATA BREACH NOTIFICATION REQUIREMENTS



WHO IS NOTIFIED	NOTIFICATION TIMELINE			
	HIPAA (< 500)	HIPAA (> 500)	Non-HIPAA (> 500)	Non-HIPAA (> 500)
Individuals	60 calendar days or less		60 calendar days or less	
Media	-	60 calendar days or less	-	60 business days or less
Federal Trade Commission	-	-	60 business days or less	10 business days or less
Dept. HHS Secretary of Breaches	Reported Annually. 60 calendar days or less of year end	60 calendar days or less	-	-

Congress has passed several pieces of legislature to protect citizens against information breaches, but they have failed to enact a single law that covers all types of information security and data breach notifications across all industries (Sullivan & Maniff, 2016).

THE ELECTRONIC HEALTH RECORD

More now than ever before, members of healthcare teams use portable personal data devices (e.g., laptops, tablets, cellular phones, data storage devices) and remote or virtual workstations to complete their assigned duties and tasks (Eddy, 2014). As electronic-centric work has become the new normal, the vulnerability of healthcare data-to-data breaches has increased due to hacker attacks from careless security practices, lost or stolen devices, unsecured mobile devices, malicious internal employee negligence, and third-party exchanges (Beeskow, 2015).

Data breaches, due to hacker attacks, have risen sharply in the healthcare sector. As a result, the fraudulent use of personal identifiable information has affected millions of patients. Why healthcare? This shift to electronic health records may have accomplished all the goals set forth in the ACA, but not without the added risk of hacker attacks. In a recent study conducted to explore the impact of the ACA on the security of patients' health information, 70% of respondents denoted that the ACA had increased or significantly increased the risk of hacker attacks due to inadequate data security measures (Eddy, 2014). This study further suggested that respondents conclude that electronic exchanges between healthcare providers and the government (75%), insecure databases (65%), and insecure patient registration websites (63%) all play a pivotal role in data breaches due to hacker attacks (Eddy, 2014, para. 4).

Risks Affiliated to Portable Devices

In addition to the increased hacking risk, employee negligence due to lost or stolen electronic devices has become one of the leading causes of data breaches in the healthcare industry (Eddy, 2014). One study suggests that 43% of all breaches are due to lost or stolen devices (Merisalo, 2015). Keane (2016) suggested that cybercrime is more prevalent due to lost or stolen devices, as thieves have noted an ease in hacking such devices versus healthcare databases. More often than not, such devices do not possess appropriate safeguards or encryptions that are necessary to prevent a hacker attack. It is interesting to note that data breaches of this nature often do not make it to news headlines because the number of impacted consumers is far lower than that of more dramatic hacker attacks, such as the Target data breach (Keane, 2016).

Internal Auditing

Healthcare organizations must also look introspectively at the careless security practices that exist, as many concerning factors exist that can lead to data breaches but that can also be prevented. Studies suggest a multitude of careless practices that organizations should explore, for which organizations should develop action plans to mitigate. These practices include a lack of encryption programs, equipment custody policies and procedures, employee training on effective privacy and security measures, installation of remote-wipe software on portable devices, policies for bring your own device, and effective data security programs as well as an urge for stronger passwords (Keane, 2016; Waterfill & Dilworth, 2014). Healthcare organizations should thoroughly reevaluate their information technology security programs and formulate plans to prevent costly data breaches.

Meanwhile, as healthcare companies add members to their team, data breaches due to non-malicious or malicious intent by frontline or third-party staff have become a cause for concern. Cybercrimes resulting in data breaches from internal staff continue to occur. Figure 1 denotes the key characteristics associated with non-malicious versus malicious intent, adapted from Willison and Warkentin (2013).

With increased demands being placed on multidisciplinary healthcare teams as care delivery demands change, data breaches due to the malicious intent of internal staff have become a legitimate concern but are often underreported due to organizational fears of reputational damage (Willison & Warkentin, 2013). Richardson (2009) conducted a study surveying 443 information technology professionals regarding organizational informational security. According to the survey findings, 25% of the respondents denote that 60% of data breaches associated with financial loss were due to non-malicious acts by internal staff, while 43% of the respondents denote that some data breaches were due to the malicious intent of internal staff (Richardson, 2009). Data breaches caused by either malicious or non-malicious acts can be devastating to affected healthcare organizations due to their financial impact. Also, individual level consequences can be dire; impersonation, identity theft, and compromised credit card records are some common examples.

FIGURE 1
INTERNAL STAFF CHARACTERISTICS FOR NON--MALICIOUS VERSUS MALICIOUS INTENT

Passive and non-volitional

- **Employee Act**
  - Accidental data entry error
- **Common Employee Characteristics**
  - Careless
  - Sloppy
  - Unmotivated
  - Poorly trained

Volitional and non-malicious

- **Employee Act**
  - Prolongs the completion of data backups
  - Avoids shredding sensitive data
  - Fails to encrypt data prior to transmission
  - Avoids changing passwords regularly
  - Avoids maintaining patient privacy by closing the door before sensitive discussions
  - Avoids the selection of strong passwords
  - Sharing passwords with co-workers
  - Knowingly violates company security policies
- **Common Employee Characteristics**
  - Intentional behaviors
  - Self-benefitting without malicious intent
  - Voluntary rule breaker

Intentional Malicious abuse

- **Employee Act**
  - Manipulation of data
  - Destruction
  - Theft of data (i.e., credit and social security cards, etc)
  - Fradulent behaviors
  - Blackmail
  - Embezzlement
  - Sells company property (trade secrets or technology)
  - Voluntary disclosure of sensitive or protected data
- **Common Employee Characteristics**
  - Motivated to inflict harm

Financial Impact

Data breaches are a constant threat for businesses worldwide, from small taco stands to a multibillion dollar company like Verizon. While businesses have safeguards in place to minimize the impact of data breaches, the risk of data breaches continues to result in undue financial implications (Garg, Curtis, & Halper, 2003). Studies suggest that some industries endure significant financial loss as a result of data breaches. The healthcare and finance industries typically suffer the greatest financial losses due to fines as well as higher rates of lost business and consumers after data breaches (Ponemon Institute, 2016).

In a recent study, the Ponemon Institute (2016) surveyed 383 organizations worldwide to study the cost of data breaches. At the conclusion of this study, the Ponemon Institute (2016) found that the average per capita cost for data breaches in the United States is $221 per breach and that the average organizational cost was $7 Million which was found to be the highest among other countries, including Germany, Brazil, India, and South Africa (p. 2). Furthermore, the researchers found that breaches of healthcare organizations due to loss or theft cost $355 globally, versus losses and theft in other industries, costing $158 (Ponemon Institute, 2016, p. 2). Exploring the major causes of data breaches, Ponemon (2016) found hacker attacks and inside breaches are responsible for 48% of breaches. This cost organizations roughly $170 per record to resolve (Ponemon Institute, 2016, p. 2). Data breaches based on system and human error are also costly to organizations. On average, organizations pay roughly $138 per record due to system glitches and $133 per record for unintentional human errors or negligence (Ponemon Institute, 2016, p. 3). Additional costs incurred for all breaches include the cost of notifying consumers of data breaches, which costs an average $0.59 per record per breach, and the response and detection after a data breach, which cost an average of $1.72 per record per breach (Ponemon Institute, 2016, p. 3). Based on the Ponemon Institute's (2016) findings, as the number of lost records increases, the cost of the data breach increases. Interestingly, of the 383 organizations studied, the average cost incurred for a noted data breach ranged from $2.1 million (10,000 records or less) to $6.7 million (50,000 records or more; Ponemon Institute, 2016).

Preventive Measures

Healthcare organizations should employ various data security systems and safeguards to protect themselves against data breaches. Protection efforts should not only be focused on complex IT networks but also on robust monitoring, intrusion detection systems, incident response frameworks and periodic third-party security audits.

Furthermore, in the May 2014 edition of *South Carolina Lawyer*, Dave Maxfield and Bill Latham examined both sides of the cybersecurity issue. Maxfield and Latham emphasized the responsibility that organizations have to be proactive and minimize the risk of serious data breaches. It is critical that businesses conduct annual reviews with a consulting company that specializes in data security and policy compliance. Likewise, organizations should invest in audits and reviews of web applications that could pose ever-evolving security threats. Furthermore, organizations must be educated about network security and the proper use of devices with access to company networks (Maxfield & Latham, 2014).

The *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* conducted by the Ponemon Institute (2015), even though cyber threats are present, many healthcare providers lack the funds and resources to sufficiently protect patient data. This unfortunately leaves them unprepared to protect against the evolving cyber threat environment. In another study, Kwon and Johnson (2013) drew similar conclusions in their research findings on healthcare data breaches. In this study, Kwon and Johnson (2013) compare similar healthcare organizations with similar compliance levels. The study revealed that while technical aspects and medical care were relatively the same in top-tier-compliance organizations and bottom-tier organizations, the difference was primarily in nontechnical or cultural compliance (Kwon & Johnson, 2013). For those top-tier compliance hospitals, third-party monitoring and audit reviews were of upmost importance.

Eliminating Data Exposures

As the number of data breaches increases, the need for data breach protection legislation becomes increasingly important. Federal information security laws have been in place for decades. While several pieces of legislation require timely consumer notifications when privacy breaches occur, Congress has failed to enact a single law that covers all types of information security and data breach notifications across all industries (Sullivan & Maniff, 2016). Because of the lack of comprehensive government legislation, 47 of the 50 states, along with the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, have adopted state-level laws that govern notification when a data breach occurs (Sullivan & Maniff, 2016).

The federal government has sponsored several projects to protect consumers' electronic health records. For example, Hippocratic Database and Active Enforcement was developed to collect and protect data using technical controls. Intel Health Guide is another technology that incorporates several privacy protections into technologies themselves. This provides security and control for both the patient and healthcare provider.

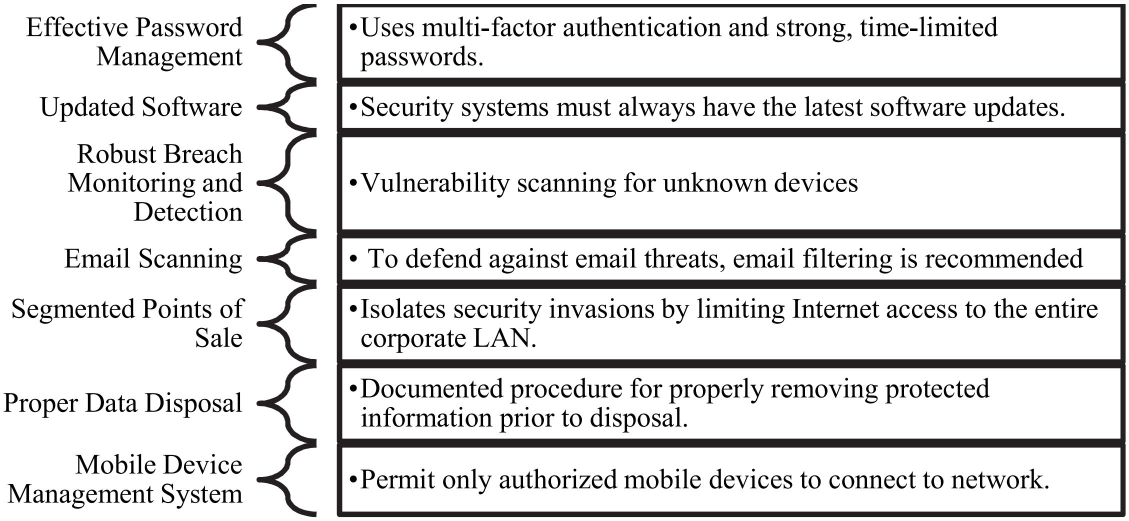
CONCLUSION

In conclusion, data breaches are a constant threat for healthcare organizations worldwide. While healthcare organizations have safeguards in place to minimize the impact of data breaches, the risk of data breaches remains, resulting in a major impact to the bottom line. Our exploration of the literature shows that healthcare organizations are not fully equipped to protect electronic health records of consumers from breaches and cybercrimes; therefore, both healthcare organizations, our federal government, and lawmakers must collectively develop strategies to detect, mitigate, and prevent data breaches. In addition, healthcare organizations must spend the necessary funds to provide adequate data security and extensive employee training. Finally, policies and procedures must robust in nature to prevent breaches and cybercrimes from occurring due to the lack of safe handling of portable devices.

Recommendations for Data Management Strategies

Several IT organizations, including the Verizon Business RISK Team (2016), published best practice guidelines on data breach prevention based on the breaches they examined. A summary of the most consistent best practice recommendations is shown in Figure 2.

FIGURE 2
DATA BREACH PREVENTION BEST PRACTICES



Effective Password Management	•Uses multi-factor authentication and strong, time-limited passwords.
Updated Software	•Security systems must always have the latest software updates.
Robust Breach Monitoring and Detection	•Vulnerability scanning for unknown devices
Email Scanning	• To defend against email threats, email filtering is recommended
Segmented Points of Sale	•Isolates security invasions by limiting Internet access to the entire corporate LAN.
Proper Data Disposal	•Documented procedure for properly removing protected information prior to disposal.
Mobile Device Management System	•Permit only authorized mobile devices to connect to network.

Data breaches in healthcare will continue to be problematic. This will leave the industry with a significant financial impact. To be world class, healthcare organizations must make securing private information a top priority. In order for healthcare entities to protect personal identifiable information from a breach, consider these recommendations.

At the end of the day, it all comes down to a strong management team, extensive employee training, and periodic internal audit in order to minimize breaches caused by employees. Based on our research, we identify key recommendations that will help reduce data breaches and minimize their financial impact.

First, build robust processes around proper disposal of health records.

The HIPAA Privacy Act requires these safeguards for protecting and disposing of health records, which should be put into place for covered entities. This protection should be adopted across the entire healthcare industry and not just entities that have dealings with the government. Hence, proper disposal of hard copy personal health information includes pulverizing records by burning and shredding methods. It is imperative that these documents are illegible and can never be reconstructed. Likewise, electronic media disposal can be accomplished with the proper hardware and/or software applications. The media, including computers, drives, and servers, should be completely cleared of electronic health information. Furthermore, degaussing can be used to expose the media to a strong magnetic field and destroy the data in these magnetic areas.

Second, reexamine health breach notification laws.

Several laws such as the FTC and the HIPPA Breach Notification Rule means executives can be held accountable for an organization's actions if it does not follow notification requirements. We feel that no matter how small or large the affected group is, notifications should be made immediately. Organizations should be required to remediate the breach within a 10- to 30-day timeframe of notification.

Third, and finally, develop educational practices that set standards.

Standards across the healthcare industry for data security would formalize the process for data sharing. An advocacy group or agency would have oversight of the implementation process across all entities. This group would ensure companies implement and maintain robust data security systems as well as collaborate with lawmakers to drive the agenda for federal legislation. Organizations should be required to implement and remain in compliance with these standards or face legal action or stiff fines. By educating healthcare organizations and standardizing on the process across the board, robust data security will become part of the culture. This will inherently decrease the number of data breaches.

REFERENCES

Aldhizer, G. R., & Bowles, J. R. (2011). Mitigating the growing threat to sensitive data: 21st century mobile devices. *The CPA Journal, 81*(5), 58–63.

Beeskow, J. (2015). Reducing security risk using data loss prevention technology. *Healthcare Financial Management, 69*(11), 108–112.

Chaput, M. A. (2014, July). Avoiding costly data breaches: Requires business associate management. *Benefits Magazine*, *51*(7), 20-25.

Chaudhary, R., & Ward, J. J. (2014). A practical approach to health care information security. *Managed Care Outlook, 27*(9), 1–9.

Eddy, N. (2014, March 19). Criminal attacks on health care organizations rise sharply. Retrieved from http://www.eweek.com/it-management/criminal-attacks-on-health-care-organizations-rise-sharply.html

Flower, K. (2016). An overview of data breaches. In R. Curtis (Ed.), *Data Breach Preparation and Response*, (pp.1-26), New York, NY: Elsevier.

Free, J. (2014, April). Better put on your running shoes: Mitigate the risks of cyber-attacks. *Health Management Technology, 35*(4), 12-13.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74–83.

Higgins, K. J. (2016, May 12). Healthcare suffers estimated $6.2 billion in data breaches. Retrieved from http://www.darkreading.com/threat-intelligence/healthcare-suffers-estimated-$62-billion-in-data-breaches/d/d-id/1325482

Huq, N. (2015). Follow the data: Analyzing breaches by industry. Trend micro analysis of privacy rights clearinghouse. 2005–2015 data breach records. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf

Joerling, J. (2010, January). Data breach notification laws: An argument for comprehensive federal law to protect consumer data. *Washington University Journal of Law & Policy, 32*(1), 467–488.

Keane, J. (2016, January). Why stolen laptops still cause data breaches and what’s being done to stop them. Retrieved from http://www.pcworld.com/article/3021316/security/why-stolen-laptops-still-cause-data-breaches-and-whats-being-done-to-stop-them.html

Khan, S. I., & Hoque, A. S. (2015). Towards development of health data warehouse: Bangladesh perspective. *International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*. doi:10.1109/iceeict.2015.7307514

Klie, L. (2015, May 1). Data security should be in everyone’s job description. *Customer Relationship Management, 19*, 32–36.

Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, *20*(1), 44–51. doi:10.1136/amiajnl-2012-000906

Maxfield, D., & Latham, B. (2014). Data breaches: Perspectives from both sides of the wall. *South Carolina Lawyer*, *25*(6), 28-35.

McMillan, M. (2015, April). The cost of IT security. *Healthcare Financial Management, 69*(4), 44-47.

Merisalo, L. J. (2015, July). Protecting patient identity: Top three tips to combat heightened medical identify threat. *Healthcare Registration, 24*(10), 10–12.

Neray, P. (2011, March). Protect patient data from an inside job: A layered approach, including safeguards against your own privileged users, may be your best bet for data security. *Healthcare Management Technology, 32*(3), 18.

Ponemon Institute. (2015). *Fifth annual benchmark study on privacy & security of healthcare data. Ponemon Institute research report*. Retrieved from https://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

Ponemon Institute. (2016). *2016 Ponemon cost of data breach*. Retrieved from https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov49542

PR Newswire US. (2015). The new healthcare crisis. More than 40% of Americans have suffered a healthcare data breach. Retrieved from http://www.prnewswire.com/news-releases/the-new-healthcare-crisis-more-than-40-of-americans-have-suffered-a-healthcare-data-breach-300131336.html

Richardson, R. (2009). *14th annual CSI computer crime and security survey*. New York, NY: Computer Security Institute.

Stevens, G. (2010). *Federal information security and data breach notification laws report. Congressional Research Service Report for Congress, January 28, 2010*. Retrieved from https://www.fas.org/sgp/crs/secrecy/RL34120.pdf

Sullivan, R. J., & Maniff, J. L. (2016). Data breach notification laws. *Economic Review - Federal Reserve Bank of Kansas City, 101*(1), 65-85. Retrieved from https://www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2016/1q16sullivanmaniff.pdf

U.S. Department of Health and Human Services. (2009, February 18). What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information*?* Retrieved from http://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html

U.S. Department of Health and Human Services. (2010, May 1). Patient protection and affordable care act health related portions of the health care and education reconciliation act of 2010. Retrieved from https://www.hhs.gov/sites/default/files/ppacacon.pdf

Verizon Business RISK Team. (2016). *Verizon’s 2016 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/#industry

Waterfill, M. R., & Dilworth, C.A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal*, *40*(2), 26–36.

Whitehouse.gov. (n.d.). Legislative language: Data breach notification. Retrieved from https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf

Willison, R., & Warkentin, M. (2013, March). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1–20.