




Spring 4-30-2019

# Safeguarding Against Data Breaches

Stephanie Johnson

*University of Tennessee Health Science Center*

Follow this and additional works at: <https://dc.uthsc.edu/hiimappliedresearch>

 Part of the [Health and Medical Administration Commons](#), and the [Health Information Technology Commons](#)

---

## Recommended Citation

Johnson, Stephanie, "Safeguarding Against Data Breaches" (2019). *Applied Research Projects*. 66. . <https://doi.org/10.21007/chp.hiim.0061>  
<https://dc.uthsc.edu/hiimappliedresearch/66>

This Research Project is brought to you for free and open access by the Department of Health Informatics and Information Management at UTHSC Digital Commons. It has been accepted for inclusion in Applied Research Projects by an authorized administrator of UTHSC Digital Commons. For more information, please contact [jwelch30@uthsc.edu](mailto:jwelch30@uthsc.edu).

# **Safeguarding Against Data Breaches**

---

**Stephanie Johnson, M.S., NCC**

**Dr. Sajeesh Kumar, Advisor**

**Department of Health Informatics & Information Management**

**University of Tennessee Health Science Center**

**April 30, 2019**

## Abstract

Reports of data breaches have seen an increase in the past decade and compared to other businesses; these breaches are estimated to be the most expensive in healthcare and affect millions of patients. One may ask what is a data breach, what causes it, and how can it be prevented? Particularly vulnerable to breaches is Protected Health Information (PHI) collected by the healthcare provider. This information is any part of the patient's medical record or payment history. Regularly, healthcare organizations utilize business associates and covered entities to deliver patient care. During this process, PHI is produced. This study addresses the obligations that business associates and covered entities have toward protecting patient information, the leading cause of breaches: hacking, medical identity theft, and unauthorized access to records, and what measures we will use to protect against such infringements.

Table of Contents

Chapter 1.....1  
    Introduction and Background.....1  
    Purpose and Significance of Study.....5  
    Research Questions.....5  
    Definition of Terms.....5

Chapter 2.....7  
    Review of Literature.....7  
    Findings and Causes of Breaches.....7  
    Role of Business Associates and Covered Entities Regarding Breaches.....10

Chapter 3.....12  
    Methodology.....12  
    Study Design and Objectives.....12  
    Method.....12

Chapter 4.....13  
    Results.....13

Chapter 5.....14  
    Discussion.....14

Chapter 6.....15  
    Conclusion.....15

References.....17

Appendices.....19  
    Appendix A.....21  
    Appendix B.....22  
    Appendix C.....23  
    Appendix D.....24

## **Chapter 1**

### **Introduction and Background**

Since the Privacy Rights Clearinghouse (PRC) began tracking data breaches in 2005, more than 563 million records have been breached. This number could even be higher in the healthcare sector given data breaches affecting less than 500 individuals are not reported. Section 13402 (e) (4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act decrees that the US Department of Health and Human Services (DHHS) post breaches involving (500 or more individuals) of unsecured PHI. When violations are discovered, they are usually attributed to human error, misuse of organizational resources, theft, hacking, malware, loss, and unauthorized disclosure (Wikina, 2014).

Healthcare organizations frequently use business associates and covered entities to provide patient care. According to the US Department of Health and Human Services (DHHS), individuals, organizations, and agencies that fall within the guidelines of a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must comply with the Privacy Rules' to shield the security and privacy of health information and must provide individuals with certain rights concerning their health information. If a covered entity (i.e., doctor, clinic, pharmacy, company health plan, or health care clearinghouse) engages a business associate to carry out its healthcare activities, the covered entity must have a written contract with the business associate. This contract establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Privacy Rules. Supplemental to these contractual obligations, business associates are unequivocally responsible for compliance with certain provisions of the HIPAA Rules (HHS.gov, n.d).

The Health and Human Services department defines a business associate as a person or entity that executes specific tasks or activities leading to the exposure of protected health information

for a covered entity. An affiliate of the covered entity's workforce is not a business associate, but a doctor, insurance company, or a health care clearinghouse is a business associate of another covered entity. Business associate occupations encompass claims processing, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Conversely, business associate services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

The Federal Register (Cavoukian, 2013) defines a breach as “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

Similarly, a breach of protected health information (PHI) is defined as the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by HIPAA. This breach poses a significant risk of financial, reputational, or other harm to the affected individual. There must be access to, use, or disclosure of unsecured PHI. This use, access, or disclosure violates the “Privacy Rule” and causes a significant financial risk that results in reputational harm to the patient, and no exceptions apply (Eisen & Gulick, 2012).

Data breaches (Giandomenico & Groot, 2018) in the healthcare industry can be internal (insiders) or external (outsiders). Healthcare is the only industry where insiders are the leading threat to an organization. Insiders have entree to sensitive information regularly know how that information is protected. So, if they want to steal or leak it, they can usually do so easier than outsiders. Furthermore, insiders unknowingly leak data by attaching the wrong file to an email, oversharing on social media, losing a laptop or USB drive; insiders can put an organization's data at risk with little effort. These healthcare workers or internal actors have a convenient means to

## SAFEGUARDING AGAINST DATA BREACHES

commit fraud (i.e., tax return fraud or opening lines of credit using PHI). Some healthcare workers (insiders) are prone to curiosity, and the accessing of patient data outside of their job responsibilities. A perfect example is when a family member, acquaintance or well-known personality is admitted into a hospital. A healthcare worker can be tempted to access the patient's health record, but have no apparent role in providing care or services to the patient. Any unwarranted access into that patient's history merely for curiosity sake would be (and is) considered a breach (Verizon, 2018).

Internal exploits are much more difficult to spot because the users are authenticated on the domain whereas, external attacks are achieved using an outward facing connection, which offers more profound security. SQL injection and DDoS are tools used to identify external attacks. However, they are limited in scope; these attacks do not compromise all data on a network. On the other hand, internal attacks can copy a large number of files without anyone knowing the source of the occurrences.

External threats, like cyber threats, are an evolving type of risk requiring organizations to increase their cybersecurity capability and ensure that the appropriate framework and especially cybersecurity skills are present. The third category with increasing importance is (covered entities), services providers, and subcontractors (business associates). Here, the line between internal and external is sometimes scarcely visible, and measures must be taken to mitigate related risks (Giandomenico & Groot, 2018).

A privacy breach occurs whenever personally identifiable information is collected, used, disclosed, retained or disposed of in a manner that violates privacy legislation; the privacy policies, procedures, and practices that have been implemented; or the privacy provisions of applicable agreements, such as confidentiality, data sharing, and research agreements.

## SAFEGUARDING AGAINST DATA BREACHES

Privacy breaches have severe repercussions for both the individuals to whom the information relates and to the health sector. From the individual's perspective, a privacy breach may result in stigmatization, discrimination, emotional and psychological harm, ineligibility for health insurance coverage, loss of employment and housing opportunities, and loss of trust in the health system. From the health sector's perspective, a privacy breach may result in damage to reputation, costs associated with containing, investigating and remediating the breach, notifying affected individuals, as well as expenses related to responding to inquiries, complaints and legal proceedings (Cavoukian, 2013).

Since the enforcement of the breach notification rule, breaches of all sizes involving various types of PHI have affected the healthcare industry. It seems that every day, the media features one story or another about a breach of PHI. By 2013, approximately 28 million individuals were impacted by a breach. The top three causes of a breach of PHI included theft, unauthorized access/disclosure, and loss with computer hacking [into networks] coming in close behind. The impact and consequences of a breach stretch far beyond the patients affected. It also impacts those involved in the inappropriate access while hurting the reputation and diminishing the trust factor of the overall organization—a cost that cannot be calculated in numbers. The financial expense, however, can be just as damaging. According to the 2012 Ponemon Benchmark Study on Patient Privacy and Data Security, the cost of a breach over two years is estimated at \$2.4 million [per infringement], ranging between \$10,000 to more than a \$1 million. The study also confirms the top three causes of breaches stating that the primary reasons for breaches were found to be theft and loss (Wikina, 2014).



## **Purpose and Significance of the Study**

This study addresses the rise in healthcare breaches ----when, where, how often they occur, and measures used to prevent them. Additionally, it discusses the role of healthcare business associates and covered entities and how they contribute to breaches. From the study, we hope to learn how to develop an effective data privacy and security program that promotes governance, awareness, education and training, monitoring, and evaluation all to reduce the number of healthcare breaches and lower healthcare cost.

## **Research Questions**

This study seeks to answer these questions:

- Where do healthcare breaches occur most?
- What responsibilities do business associates and covered entities have toward keeping healthcare data safe?
- How can we safeguard against data breaches?

## **Definitions of Key Terms**

**Protected Health Information (PHI)** - Protected health information (PHI) under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

**Privacy Rights Clearinghouse (PRC)** – A non-profit Corporation that advocates for consumers and raises their awareness about how technology affects personal privacy.

**Health Information Technology for Economic and Clinical Health (HITECH)** - The HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 is

## SAFEGUARDING AGAINST DATA BREACHES

legislation that was created to stimulate the adoption of electronic health records (EHR) and the supporting technology in the United States.

**Department of Health and Human Services (DHHS)** - This is the United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves.

**HIPAA Privacy Rules** - Assure individuals' that health information is properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and wellbeing.

**Covered Entity**- A covered entity is a healthcare provider, a health plan, and a healthcare clearinghouse (i.e., doctor, pharmacy, HMO, Medicaid, Medicare).

**Business Associate** - A business associate is a person or organization, other than a member of a covered entity's workforce, that performs specific functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of individually identifiable health information.

**The Federal Register** – This is a daily publication of the US federal government that issues proposed and final administrative regulations of federal agencies.

**Breach** - An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

**Internal Breaches** - These are breaches that occur inside the workplace, and they can be intentional or accidental.

**External Breaches** – These are breaches that occur outside the workplace, for example, cyber threats, unsecured laptops, the cloud, and mobile phones.

## Chapter 2

### Review of Literature

A broad search of pertinent literature was performed using PubMed, and CINAHL databases, Google Scholar search engine and the American Health Information Management Association's (AHIMA) Body of Knowledge. Additionally, this literature review has an excel spreadsheet including the author's name, journal year, keywords, study results, and methodology to compile the report (See Appendix A).

Each database was searched using keywords or combinations of keywords such as breaches in healthcare, PHI, cybersecurity in healthcare, HIPAA, confidentiality, patient data privacy, data protection, and health information technology. This literature review included articles published from 2013 to 2018, written in English, and full texted; whitepapers, blogs, and letters were also included.

The majority of the articles found in the literature contained information on causes and types of data breaches, ramifications of breaches and those affected, the responsibility of business associates and covered entities to the healthcare agency, and breach prevention methods.

### Findings

**Causes of Breaches-** Healthcare information is sensitive, vulnerable, and most attractive to criminals. Data breaches most often occur through theft, loss, unauthorized access or hacking. Many studies have been done as to the cause and ramifications of these breaches. The American Journal of Managed Care (2018) conducted a study whose purpose was to describe locations in hospitals where data was breached and identify the types of breaches that occur most often. From 2009-2016, employing The Office of Civil Rights breached data of healthcare providers affecting 500 or more individuals, research showed that approximately one-third of breaches occur in

## SAFEGUARDING AGAINST DATA BREACHES

hospitals and influence a significant number of individuals. Paper and films were the most frequent location breached, happening in 65 hospitals. While network servers were the least common location, their breaches affected most patients.

Similarly, between 2010-2017, The Journal of American Medical Association (2018) conducted a study to address temporal trends in the number of breaches and records affected in three categories of the federal database: business associate, health plan, and healthcare provider. Business associate refers to entities that do not provide or reimburse healthcare but are given access to HIPAA protected data to support physician or health plans. Conversely, a healthcare provider is a person or organization who furnishes bills or is paid for a health care service whereas, a health plan provides or pays the cost of medical care.

In this study, the most common entity breached was a healthcare provider with 1503 breaches (70%) comprising a total of 37.1 million records (21%). The 278 breaches (13%) of health plans accounted for the largest share of breached records, 110.4 million (63%). The most common information media breached was paper or film with 510 breaches (24%) comprising a total of 3.4 million records (2%). Information from the network server accounted for the largest share of breached records, 139.9 million (79%). The most commonly breached media locations shifted from laptop and paper or films in 2010 to a network server and email in 2017.

Wikina (2014), conducted research that revealed, yearly, data breaches involving personal health information leading to theft, loss, unauthorized access, improper disclosure, or hacking incidents are on the rise. Since 2009, reported breaches involving 674 covered entities and 153 business associates had affected 27 million people. These breaches come from various sources such as computer systems and networks, desktop computers, laptops, paper, e-mail, electronic health records, and removable/portable devices (CDs, USBs, x-ray films, backup tapes, etc.).

## SAFEGUARDING AGAINST DATA BREACHES

This study found that even with the increased use of health information technology by health care facilities and allied businesses, theft and loss (not hacking) constituted the major types of data breaches encountered. Removable/portable devices, desktop computers, and laptops were the top sources or locations of the breached information. In top six states—Virginia, Illinois, California, Florida, New York, and Tennessee—for nearly 75% of individual breaches, 33% came from covered entities, and about 30% involved business associates.

In 2018, AHIMA added to its ‘Wall of Shame.’ Over 160 new breaches and topped the list; Hacking, unauthorized access/disclosure, and theft/loss. Unauthorized access/disclosure proved to be the most common type of breach, with 73 incidents occurring between January and June 2018. These breach incidents involved email, electronic health records, and paper or film document. Nearly 558,000 people were affected by this type of breach, according to HealthcareInfoSecurity. With 54 breaches, hacking came in second—but affected more than 1.6 million individuals, which accounts for almost 60 percent of the total victims affected by Wall of Shame breaches. At 31 breaches, theft/loss was the third most common type of incident and affected 660,000 individuals.

In the Healthcare Leadership Review (2017), and according to data provided to HealthLeaders Media by the Identity Theft Resource Center, broken down by industry, hacking was the most common data breach source for the healthcare sector. Physical theft was the most significant breach category for healthcare in 2015 and 2014. Insider theft and employee error/negligence tied for the second-most familiar data breach sources in 2016 in the health industry. Also, insider theft was a bigger problem in healthcare than in other sectors. Insider theft is alleged to have been at play in the Jackson Health System incident. Former employee Evelina Sophia Reid was charged in a 14-count indictment with conspiracy to commit access device

## SAFEGUARDING AGAINST DATA BREACHES

fraud, possessing 15 or more unauthorized access devices, aggravated identity theft, and computer fraud. Prosecutors say that her co-conspirators used the stolen information to file fraudulent tax returns in the patients' names.

Verizon (2018) believes that internal actors are the biggest threat to a healthcare organization ----- 58% of incidents that occur involve insiders. Verizon adds that medical device hacking creates media hype, but the assets most often affected in breaches are databases and paper documents. Additionally, ransomware is the top malware variety by a wide margin; 70% of incidents involving malicious code were ransomware infections, and necessary security measures are still not being implemented. Lost and stolen laptops with unencrypted PHI continue to be the cause of breach notifications.

**Role of Business Associates and Covered Entities Regarding Breaches** - A study conducted by the Ponemon Institute, shows that 46% of the data breaches that occurred at chosen healthcare organizations were the result of third parties, including business associate's mistakes. Andrew Martin, a prominent attorney, says "even if the data breach is the result of a business associate's action, the liability for the breach affects the covered entity because it affects the relationship between the covered entity and the individual." Although the business associate agreement requires specific policies related to privacy and security of data, it is essential that the covered entity also includes a program to monitor the business associates' plan.

Christine Leyden senior vice president of client services and chief accreditation officer suggest that before you determine how often and in what manner you should monitor a business associate's privacy and security program, initiate a risk assessment to identify details to address in the agreement, including the physical safety of data. Also, Understand the flow of protected

## SAFEGUARDING AGAINST DATA BREACHES

health information from your organization to the business associate and from the business associate to others.

When employing a business associate, the covered entity should evaluate the amount and type of data the business associates will handle and be aware of their policies, privacy and security procedures. The covered entity should ask if the business associate offers training programs for their employees and what methods they have for storing, accessing, and destroying data. Also, the covered entity should inquire if the business associates do employee background checks, use subcontractors, require subcontractors to meet same privacy and security standards as the business associate, and will they allow onsite review of their privacy and security processes. Business associates should be limited to the information needed to perform the job for which they are contracted; organizations that receive limited data or data that will be used for a short, specific timeframe, subsequently, pose less risk. Efforts to monitor and audit a BA's privacy and security program should focus on agencies that receive a high volume of protected patient information on a consistent, ongoing basis (HIPAA Regulatory Alert, 2012).

### Chapter 3

#### Methodology

**Study Design and Objectives** -The objectives of this study are to describe the types of breaches that occur most often between covered entities and business associates at healthcare facilities, identify the locations of breached data, and reveal the number of individuals affected.

**Method-** Data for the study were obtained from the DHHS Information Privacy website. As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. Data obtained within the last 24 months, revealed that 423 covered entities, including business associates, and millions of individuals from all parts of the country were affected by various types of breaches ranging from hacking/IT incidents, theft, unauthorized access/disclosure, improper disposal, and loss. The location of breached information occurred on laptops, network servers, electronic medical record (EMR), paper/films, other portable electronic devices, email, desktop computer, and unknown/other sources (HHS.gov, n.d.).

The data for this study will be downloaded into a spreadsheet and then sorted into tables by type of breach, the location of breached information, and the state in which the breaches took place, using Microsoft Excel tools such as pivot tables. For this study, a distinction will be made between theft, which is a deliberate attempt by a determined person to steal health data or information, and loss, which could result from carelessness. In some cases, however, one can lead to the other, making the cause challenging to determine when reporting the loss. Finally, the number of individuals affected, and the number of covered entities and their business associates involved in a breach will be counted (Wikina, 2014).



## **Chapter 4**

### **Results**

As stated earlier in the study, business associates are entities that do not provide or reimburse healthcare but are given access to HIPAA protected data to support physicians or health plans. The health provider is a person or organization who furnishes, bills, or is paid for a healthcare service. Health plans provide or pay the cost of medical care (JAMA, 2018).

From 2017-2019, of the 423 covered entities in my sample, those breached most often were healthcare providers (311), health plans (65), and business associates (47). The breach type occurring most often was hacking/IT (205), followed by unauthorized access/ disclosure (143), theft (51), loss (14), and improper disposal (11). The locations breached most often were email (131), network servers (85), paper and film (68), the electronic health record (20), and the desktop computer (15). By state, the covered entities most affected were from Texas (32), followed by Illinois (26), California (26), New York (23), Missouri (21), and Michigan (20). Lastly, the percentage of covered entities that utilized business associates was 22%. The majority of the covered entities (78%) did not use business associates (See Appendix B).

In a letter, I reached out to Timothy Noonan, Regional Manager, in the Office for Civil Rights, for the U.S. Department of Health and Human Services, to share the results of my study. I wanted to know his thoughts about the rise in healthcare breaches over the last 24 months and what security measures he thinks are needed to protect patient health information? After several follow up attempts, Mr. Noonan has not been open to sharing this information with me (See Appendix C).

## **Chapter 5**

### **Discussion**

In the healthcare sector, data breaches affecting 500 or more individuals are required by law to be posted by the DHHS as public information. However, we don't know how many healthcare organizations know that they have been breached or report them. HIT researches are divided on where the leading causes of breaches emanate. Some say 85% of breaches occur off the network. Others say 75% of all security breaches are caused by fraud and failure to follow procedure. Then, there is the need to make a distinction between theft and loss. As stated earlier, theft is a deliberate attempt by a determined person to steal health data or information, and loss, could result from carelessness. One can lead to the other, making the cause challenging to determine when reporting the loss (Wikina, 2014).

## **Chapter 6**

### **Conclusion**

Training and education are needed for people who handle personal health information to educate them on their role in enhancing the privacy and security of the information they encounter in the course of their duties, and this training needs to be taken seriously. We focus on procuring the most advanced technological gadgets to protect and secure health information and the key lies in addressing the softer side of the equation. Proper disposal processes and procedures for removable electronic devices, paper records, desktop computers, laptops, and other computer equipment need to be put into place and adhered. The 2011 Benchmark Study on Patient Privacy and Data Security reported that 73 percent of respondents say they lack sufficient resources to prevent or detect unauthorized patient data access, theft, or loss. Staff responsible for data, need to be trained on necessary security procedures to recognize deceptive techniques used by fraudsters and identity thieves, such as social engineering and must report these techniques to the appropriate computer incident response team promptly. Therefore, organizations desiring to establish an effective data privacy and security programs should be aware that they hinge on the following pillars: (1) governance (leadership); (2) awareness, education, and training; (3) actions (implementing internal controls, including the use of data encryption, strong passwords, physical security, and electronic controls, as well as compliance testing); and (4) monitoring and evaluation (Wikina, 2014).

According to a Cybersecurity Survey conducted by HIMSS in 2015, 87% of healthcare professionals stated that information security had become a business priority; 81% lobbied for more creative and advanced tools, and 61% planned to increase spending to offset data threats. 73% of the healthcare organizations had implemented a data breach response plan, but they

## SAFEGUARDING AGAINST DATA BREACHES

didn't have a full understanding of what needed to be done if a breach occurred nor how to regain public trust once it happened. 41% of these individuals had no set time for reviewing or updating their response plan, and 37% had not discussed the plan since it was created. Small hospitals were ready and willing to implement security measures to protect patient data, but they were limited by their resources.

To guard against data breaches, what's emphasized is to conduct a HIPAA risk analysis, perform vulnerability assessments and penetration testing, and implement security information and event management. Further, healthcare organizations should know who can legitimately access their system from the outside. They must get rid of generic passwords, develop and implement a strategic data security plan, train employees in data security and privacy issues, and encrypt all patient data (See Appendix D).

References

- AHIMA, (2018). *Over 160 New Breaches Added to 'Wall of Shame' So Far in 2018*. Retrieved from [http://www.ahimajournal-digital.com/ahimajournal/september\\_2018?pg=19#pg19](http://www.ahimajournal-digital.com/ahimajournal/september_2018?pg=19#pg19)
- Caroukian, A. (2013). Tips to avoid and manage privacy breaches in the health sector. *OOHNA Journal*. Retrieved from <http://eds.a.ebscohost.com.ezproxy.uthsc.edu/eds/pdfviewer/pdfviewer?vid=9&sid=10527a56-c5e0-4ed8-b09f-a523985e11b2%40sessionmgr4006>
- Eisen, J. A., & Gulick, S. L. (2012). What is a breach under the hi-tech breach notification regulations? *ABA Health eSource*, 8 (9). Retrieved from [https://www.americanbar.org/content/newsletter/publications/aba\\_health\\_esource\\_home/aba\\_health\\_law\\_esource\\_0512\\_eisen.html](https://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_0512_eisen.html)
- Gabriel, M. H., Noblin, A., Rutherford, A., Walden, A., & Cortelyou-Ward, K., (2018). Data breach locations, types, and associated characteristics among us hospitals. *The American Journal of Managed Care*, 24(2), 78-84. Retrieved from <https://www.ajmc.com/journals/issue/2018/2018-vol24-n2/data-breach-locations-types-and-associated-characteristics-among-us-hospitals>
- Giandomenico, N., & Groot, J., (2018). Insider vs. outsider data security threats: What's the greatest risks? Retrieved from <https://digitalguardian.com/blog/insider-outsider-data-security-threats>

## SAFEGUARDING AGAINST DATA BREACHES

Health Management Technology. (n.d.). *Data breaches in healthcare: Tackling a big problem.*

Retrieved from <https://www.myconsultq.com/wp-content/uploads/sites/2001/2016/09/10-2015-Data-Breaches-in-Healthcare-Healthcare-Informatics.pdf>

HHS.gov. (n.d.). *Health information privacy.* Retrieved from <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html#>

HIPAA Regulatory Alert, (2012). Data breaches attributed to business associates increase, *covered entities review responsibility for monitoring business associates.* Retrieved from <https://www.reliasmedia.com/articles/76831-hipaa-regulatory-alert-data-breaches-attributed-to-business-associates-increase>

McCoy, T. H., & Perlis, R. H., (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. *The Journal of American Medical Association*, 320(12), 1282-1284.

Retrieved from

[https://www.researchgate.net/publication/327872629\\_Temporal\\_Trends\\_and\\_Characteristics\\_of\\_Reportable\\_Health\\_Data\\_Breaches\\_2010-2017](https://www.researchgate.net/publication/327872629_Temporal_Trends_and_Characteristics_of_Reportable_Health_Data_Breaches_2010-2017)

Pecci, A. W., (2017). Healthcare data breaches up 40% since 2015. Retrieved from

<https://www.healthleadersmedia.com>

Verizon. (2018). *Protected health information data breach report.* Retrieved from

[http://www.verizonenterprise.com/resources/protected\\_health\\_information\\_data\\_breach\\_report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf)

Wikina, S. B. (2014). What caused the breach? An examination of the use of information technology and health data breaches. *Perspectives in Health Information Management.*

Retrieved from <http://bok.ahima.org/doc?oid=300738#.We1KaluPKM8>

## SAFEGUARDING AGAINST DATA BREACHES

Appendices:

**Appendix A** – Literature Review Grid

**Appendix B** -- DHHS Breach Report with Pivot Charts and Graphs

**Appendix C** – Letter to Timothy Noonan, Regional Manager, Office for Civil Rights U.S.

Department of Health and Human Services

**Appendix D** --- Data Breaches in Healthcare: Tackling a Big Problem

# Running head: SAFEGUARDING AGAINST DATA BREACHES

Author(s)	Journal Year	Subject/Keywords	Study Results	Methodology
Ann Cavoukian	OOHNA JOURNAL, 2013	Tips to Avoid and Manage Privacy Breaches in the Health Sector		
Eric D. Perakslis, Ph.D.	The New England Journal of Medicine, 2014	Cybersecurity in Health Care		
Suanu Bliss Wikina, PhD	The American Health Information Management Association, 2014	What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches		Data for the website.
Meghan Hufstader Gabriel, PhD; Alice Noblin, PhD, RHIA, CCS; Ashley Rutherford, PhD, MPH; Amanda Walden, MSHSA, RHIA, CHDA; and Kendall Cortelyou-Ward, PhD	THE AMERICAN JOURNAL OF MANAGED CARE® VOL. 24, NO. 2, 2018	Data Breach Locations, Types, and Associated Characteristics Among US Hospitals	Of all types of healthcare providers, hospitals accounted for approximately one-third of all data breaches and hospital breaches affected the largest number of individuals. Paper and films were the most frequent location of breached data, occurring in 65 hospitals during the study period, whereas network servers were the least common location but their breaches affected the most patients overall. Adjusted multivariate results showed significant associations among data breach occurrences and some hospital characteristics, including type and size, but not others, including health IT sophistication or biometric use for security.	The OCR data breaches of individuals. We used data from Kroll/HIMSS security in By means of there has been and collected Medical De
Juhee Kwon, M Eric Johnson Beltran-Aroca CM1, Girela-Lopez E2, Collazo-Chao E2, Montero-Pérez-Barquero M3, Muñoz-Villanueva MC4.	BMC Med Ethics, 2016	Confidentiality breaches in clinical practice: what happens in hospitals?		
By Beth Hjort, RHIA, CHPS and Harry Rhodes MBA, RHIA, CHPS, CPHIMS, FAHIMA	Friday, January 22, 2010	Healthcare Breach Management: Business Associate Agreement Addendum		
C. Lee Ventola	Pharmacy and Therapeutics, 2014	Social Media and Health Care Professionals: Benefits, Risks, and Best Practices		When used potential to develop dangers the issued by H sound and We have a because co burdens; h doing so se groups.
Mann, Savulescu, and Sahakian Barry S. Herrin, CHPS, JD, FACHE, and Frankie T. Jones, Jr., JD	Philos Trans A Math Phys Eng Sci. 2016 2011 by The American Health Information Management Association	Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue Cybersecurity Insurance: Considering Coverage for Data Breaches		
Burke W. Mamlin, MD and William Tierney, MD	THE AMERICAN JOURNAL OF THE MEDICAL SCIENCES, 2016	The Promise of Information and Communication Technology in Healthcare: Extracting Value From the Chaos		Steps to be patient ide HIEs require vendors, ta
Bostjan Brumen, Marjan Heričko, Andrej Sevnčnikar, Jernej Završnik, Marko Hölbl	J Med Internet Res. 2013 Dec; 15(12): e283. Published online 2013 Dec 16. doi: 10.2196/jmir.2471	Outsourcing Medical Data Analyses: Can Technology Overcome Legal, Privacy, and Confidentiality Issues?	The decision trees built on encrypted data were virtually the same as those built on original data. Out of 30 datasets, 100% of the trees had identical accuracy. The size of a tree and the number of leaves was different only once (1/30, 3%, P=.19).	Medical da the course population full access legal regul data owne
DHHS	CMS, November 2004	Security 101 for Covered Entities		
Dale Jessop	Mhealth, 2016	Safe and sound: why a robust and workable data security policy is fundamental in healthcare programs		There is no connected becoming a drain on na healthcare this new sh Stolen lapt to be week challenge f show, inad as the liabi Protection breaches o Insurance f Informatio Economic breaches in reported. T may increa and exten
Kimela West, JD	Mo Med, 2014	Patient Medical Information At Risk From Stolen Computers		
Letters	JAMA, 2018	Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017		
Colorafi, Ph.D RN & Bailey, JD	JMIR Med Inform, 2016	It's Time for Innovation in the Health Insurance Portability and Accountability Act (HIPAA)		Whether it a segment far from th the Health represent a volumes of last twenty informatio innovation relate to the hands



## SAFEGUARDING AGAINST DATA BREACHES

Count of Name of Covered Entity	
Business Associate Present	Total
No	329
Yes	95
Grand Total	424

## SAFEGUARDING AGAINST DATA BREACHES

February 20, 2019

Timothy Noonan, Regional Manager  
Office for Civil Rights  
U.S. Department of Health and Human Services  
Sam Nunn Atlanta Federal Center, Suite 16T70  
Atlanta, GA 30303-8909

Dear Mr. Noonan,

I am a student in the Masters Health Information Informatics program at the University of Tennessee Health Science Center. This semester, under the supervision and direction of Dr. Sajeesh Kumar and Dr. Rebecca Reynolds, I am completing my thesis on Safeguarding Against Data Breaches.

My study addresses the leading cause of breaches, where the violations occur most often, the responsibility that business associates and covered entities have toward protecting patient health information, and what security measures are needed to protect patient records.

To gather and aggregate data for my research, I referenced the Department of Health and Human Services (DHHS) Information Privacy website and looked at records from 2017-2019. The data was sorted and analyzed using pivot tables and charts. Covering various states over 24 months, I discovered that in order of rank:

- The covered entities breached most often was healthcare providers, health plans, and business associates.
- The type of breach occurring most often was hacking/IT, unauthorized access/disclosure, theft, loss, and improper disposal.
- The locations breached most often were email, network servers, paper and film, the electronic health record, and desktop computer.
- By state, the covered entities most affected were from Texas, Illinois, California, New York, Missouri, and Michigan.

What are your thoughts about the above and what security measures do you think are needed to protect patient health information? Your opinion is valuable and will help to validate my study. Thanks for your time and I hope to hear from you soon.

Sincerely,

Stephanie Johnson, M.S., NCC  
[sjohn175@uthsc.edu](mailto:sjohn175@uthsc.edu)



**CONTACT:**  
151 Southhall Lane, Suite 150  
Maitland, FL 32751

**quammengroup.com**  
407.539.2015  
info@quammengroup.com

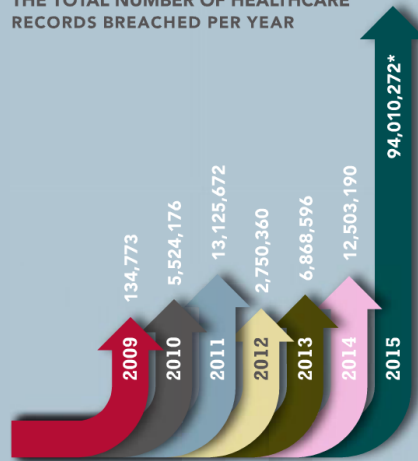
## DATA BREACHES IN HEALTHCARE: TACKLING A BIG PROBLEM

### THE FIVE BIGGEST HEALTH DATA BREACHES (SO FAR)



Source: U.S. Department of Health and Human Services, Office for Civil Rights. [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

### THE TOTAL NUMBER OF HEALTHCARE RECORDS BREACHED PER YEAR



\*2015 data through June 26, 2015  
Source: U.S. Department of Health and Human Services, Office for Civil Rights. [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

### DATA PROTECTION: AN EMERGING PRIORITY FOR HEALTHCARE ORGANIZATIONS

**87%** OF HEALTHCARE PROFESSIONALS INDICATED THAT INFORMATION SECURITY HAD BECOME A CRITICAL BUSINESS PRIORITY

**81%** BELIEVE MORE INNOVATIVE AND ADVANCED TOOLS ARE NEEDED

**63%** OF ORGANIZATIONS ARE PLANNING TO INCREASE SPENDING TO OFFSET DATA THREATS

Source: HIMSS 2015 Cybersecurity Survey, which included responses from 297 healthcare professionals with level of responsibility for data security.  
Source: Harris Poll survey of 920 IT decision makers conducted on behalf of Vormetric. <http://www.eweek.com/small-business/data-breaches-common-in-health-care-industry.html>

### DATA PROTECTION AND SECURITY: READY – OR NOT?

**73%** OF ORGANIZATIONS HAVE IMPLEMENTED A DATA BREACH RESPONSE PLAN **BUT**

- 67%** DON'T HAVE SOLID UNDERSTANDING OF WHAT NEEDS TO BE DONE TO MINIMIZE DAMAGES AND RETAIN CONSUMER TRUST IF A BREACH OCCURRED
- 41%** HAD NO SET TIME FOR REVIEWING AND UPDATING PLANS
- 37%** HAD NOT REVIEWED THEIR PLAN SINCE IT WAS CREATED

### SMALL HOSPITALS: READY, WILLING — BUT NOT ABLE?

**91%** OF SMALL HEALTHCARE PROVIDERS (LESS THAN 250 EMPLOYEES) HAVE SUFFERED A DATA BREACH

**23%** HAVE HAD A MEDICAL IDENTITY THEFT INCIDENT

**100%** OF THESE ORGANIZATIONS ARE TAKING STEPS TO PROTECT DATA

**BUT** **only 30%** HAVE RESOURCES NEEDED TO ENSURE PRIVACY/SECURITY REQUIREMENTS ARE MET

Source: Ponemon Institute, *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness*. The study included responses from executives from several business sectors including healthcare.  
Source: Ponemon Institute, *Data Security in Small Healthcare Organizations*.

### SAFEGUARDING AGAINST A DATA BREACH: DON'T MISS THESE 8 BASIC STEPS

- 1 Conduct a HIPAA security risk analysis
- 2 Perform vulnerability assessments and penetration testing
- 3 Implement SIEM [Security Information & Event Management]
- 4 Know who can legitimately access your systems from the outside
- 5 Get rid of generic passwords
- 6 Develop and implement a strategic data security plan
- 7 Train employees in data security and privacy issues
- 8 Encrypt all patient data