Healthcare Breaches During COVID-19: The Effect of the Healthcare Entity Type on the Number of Impacted Individuals

By Martin Ignatovski, PhD

Abstract

The COVID-19 pandemic led to an increase in cybersecurity attacks on organizations operating in the healthcare industry. Health information professionals and health executives are unable to limit the impact of data breaches on records their organizations handle. While current research focuses on prevention strategies and the understanding of the causes of data breaches, it failed to address how to mitigate the impact of successful cybersecurity attacks. This quantitative research paper examined the effect the healthcare entity type has on the number of impacted individuals for healthcare data breaches that occurred during the pandemic. Health information professionals will be able to mitigate the number of breached records based on their organizational type. Some of this paper's findings include the call for implementation of organizational frameworks aimed to protect patient information, and the call for further research to understand how other factors might affect the impact of healthcare data breaches.

Keywords: cybersecurity, healthcare, data breaches, patient information, PHI

Introduction

The COVID-19 pandemic generated unique challenges and opportunities for organizations operating in the US healthcare industry. Health providers struggled providing non-pandemic care to their patients due to the overwhelmed healthcare system and large number of COVID-19 diagnosed patients who needed immediate attention.[1,2] To overcome restrictions that were the direct result of the pandemic and the associated lockdowns, organizations were forced to enable hybrid and remote work environments so they could continue with their daily operations. The use of current and new technologies such as electronic health record systems (EHRs), telehealth platforms (TH), and remote collaboration tools opened opportunities and additional vectors that could be exploited for cybersecurity attacks to harm organizations handling protected health information (PHI).[3,4] The implementation of appropriate controls meant to protect the security and privacy of PHI did not keep up with the new attack vectors created by the newly implemented technologies.[5] The US healthcare industry saw a 25 percent increase in successful cybersecurity attacks during the pandemic.[6]

The Office of Civil Rights (OCR) within the US Department of Health and Human Services (DHHS) oversees the implementation of the Health Insurance Portability and Accountability Act (HIPAA) regulation. The HIPAA regulation consists of three primary rules: HIPAA privacy rule, HIPAA security rule, and HIPAA breach notification rule. The HIPAA privacy rule defines the controls and procedures that need to be implemented to protect the privacy of PHI. The HIPAA security rule is focused on defining administrative, physical, and technical controls required for the protection of the security of PHI. Finally, the HIPAA breach notification rule sets the standards under which data breaches affecting PHI need to be reported. According to the HIPAA regulation, healthcare entities (HE) are required to report all data breaches that impact at least

500 individuals. The archive of all reported data breaches is publicly shared and available on the US DHHS website.

Executives and cybersecurity professionals within the healthcare industry lack full understanding of the HIPAA regulation requirements[7] and strategies on how to mitigate the effects of data breaches in their organizations.[8] Healthcare entities struggle to implement appropriate level of controls to meet the vague, but still needed, requirements of the HIPAA security rule.[9] An area of concern are the defined requirements for access of PHI.[10] Inappropriate access levels to PHI records could lead to impermissible disclosures and data breaches. Additionally, healthcare entities are not prepared to withstand cyberattacks due to the complexity of newly implemented technologies and their integration with old legacy systems and devices.[11] Some of those systems and devices are provided and managed by third-party vendors or business associates to the healthcare-covered entities.

Current research focuses on strategies and techniques to prevent data breaches from happening in healthcare organization.[12-15] Prevention strategies allow organizations to stop malicious actors by closing the "door" to their system and avoiding intrusion that could lead to impermissible disclosures of PHI. What happens once a breach occurs? There is a specific need to understand the factors that have a significant effect on the number of breached records.[16] Based on the data reported on the US DHHS website, it is safe to assume that it is no longer a question whether a breach will occur, but when will it occur. Health information managers and the healthcare entities they work for need to be prepared by implementing mitigation strategies to minimize the impact their entity type has on the number of breached records, once a data breach occurs.

Inappropriately protecting PHI could lead to violation of the three main HIPAA principles: confidentiality, integrity, and availability.[17] Successful cybersecurity attacks, especially ransomware, render PHI unavailable and unreadable,[18] thus causing inability of EHRs and other systems to access current and historical patient data.[19] The inability to access data leads to significant disruptions in patient care that could negatively affect patient outcomes and patient safety.[20] This research paper analyzes the relationship and the main effect the HE type has on the number of impacted individuals in healthcare data breaches. Exploring how the HE type affects the number of impacted individuals will allow health information management (HIM) professionals to understand how to implement controls that will mitigate the impact of healthcare data breaches within their specific organizational structure.

Research Question

Due to lack of current research on how to minimize the number of records that are impacted in data breaches targeting healthcare entities, and with an aim to expand the research body and contribute to future research, the research paper addressed the following research question: What is the effect, if any, the healthcare entity type has on the number of impacted individuals in healthcare data breaches reported by healthcare organizations within the US?

To address the research question in detail, the author set the following hypotheses:

- H0: There is no effect of the healthcare entity type on the number of impacted individuals during the 27 months of the COVID-19 pandemic.
- HA: There is significant effect of the healthcare entity type on the number of impacted individuals during the 27 months of the COVID-19 pandemic.

Method

The purpose of this research is to identify and analyze to what extent, if any, the healthcare entity type contributes to the number of individuals impacted in a healthcare data breach (**Figure 1**). This research utilized quantitative analysis by performing a one-way ANOVA analysis, with post-hoc test, using the number of impacted individuals as the dependent variable, and the HE type as the independent variable. One-way ANOVA is robust and informs whether three or more independent groups within the independent variable have significant differences when it comes to the effects on the dependent variable. This quantitative analysis was performed on secondary data of reported data breaches by HEs, as presented on the US DHHS website. For the purposes of this research, the author decided to use the entire population of the data set, which eliminates any sampling bias. The only intervention was the removal of duplicate data entries reported by the same entities (reporting date, entity name, number of impacted individuals). The entire data set includes 1,587 reported data breaches impacting at least 500 or more individuals per occurrence.

The two variables examined in this research include the HE type and the number of impacted individuals per data breach occurrence. The HE type is an independent variable that contains four categories: healthcare provider, health plan, healthcare clearinghouse, and business associate. Healthcare providers, health plans, and healthcare clearing houses are covered entities. Business associates are typically vendors used by covered entities and act as third-party vendors (**Figure 2**). The number of impacted individuals in a healthcare breach is the dependent variable, and it is measured on a continuous scale.

The author of the research did not collect the data directly from the HE types that reported the data breaches, but rather performed a quantitative statistical analysis on a secondary data set. The author implemented a five-step process to identify, obtain, and protect the integrity of the secondary data set reported on the US DHHS website. The first step included the identification of the website that stores the data set, thus determining that the US DHHS is a reliable website with its data used in many research articles.[13,21,22,23,24,25] As part of the second step, the author extracted the entire data set and saved it into a comma-separated values file. Next, the author examined the data and filtered it to include only the data breaches reported between April of 2020 and June of 2022. The selection of these dates corresponds with the pandemic lockdowns and the continued battle against the COVID-19 virus. In the fourth step of the process, the author encrypted the data set and created password protections so it could not be edited. Finally, the last step included loading and analysis of the data into statistical software, SPSS.

Results

Prior to conducting the one-way ANOVA with post-hoc analysis, the author ran comparison of data breaches and the number of impacted records prior and during the pandemic. The analysis included 27 months of data breaches reported during the pandemic, and 27 months of data breaches reported prior to the pandemic. The initial comparison shows that breaches that occurred during the COVID-19 pandemic accounted for 100,474,829 breached PHI records, which is 39,783,652 more breached PHI records than data breaches that occurred during the same time span prior to the pandemic.[26] (**Figure 3**)

As part of the data analysis, the author first examined the independent variable: healthcare entity type. Of the 1,587 records, 1,176 of the reported data breaches were by healthcare providers, followed by business associates with 208, and health plans with 200 data breach occurrences. The least amount of data breaches was reported by healthcare clearinghouses: three (**Table 1**). Additionally, the author ran descriptive statistics of the dependent variable, which had a mean value of 63,311.17 and standard deviation of 247,507.79 (**Table 2**).

The next step of the data analysis included running the one-way ANOVA function. According to the ANOVA results (**Table 3**), there was a significant main effect of the healthcare entity type on the number of impacted individuals for the data breaches reported during the COVID-19 pandemic, $F(3,1583) = 8.997$, $p < 0.001$. The results show that we can reject the null hypothesis that there is no significant main effect of the healthcare entity type on the number of impacted individuals, and accept the alternate hypothesis, showing there is significant main effect of the healthcare entity type on the number of impacted individuals. Since there was a significant main effect of the healthcare entity type on the number of impacted individuals, the results of the Tukey's function (**Table 4**) will be interpreted in the discussion portion of this article

Discussion

The results of the one-way ANOVA analysis show significant main effect of the independent variable (HE type) on the dependent variable (number of individuals impacted by data breaches). The analysis clearly shows that the number of breached records depends on the HE type that is handling the patient data. To further analyze the effect the author performed Tukey's post-hoc analysis on the data (**Table 4**). The post-hoc analysis revealed that breaches that occurred in business associates affect significantly larger number of individuals ($145,491.88 \pm 491,440.33$, $p = 0.002$) when compared to breaches that occurred in health plans ($57,026.85 \pm 275,853.51$, $p = 0.002$). Similarly, breaches that occurred in business associates affect significantly larger number of individuals ($145,491.88 \pm 491,440.33$, $p < 0.001$) when compared to breaches that occur in healthcare providers ($49,965.1 \pm 160,887.19$, $p < 0.001$). Additionally, Tukey's analysis also revealed that breaches in healthcare clearinghouses do not affect significantly more or less individuals than health plans and healthcare providers. Finally, Tukey's analysis reveals that breaches in health plans do not breach significantly more or less individuals than healthcare providers.

It is intuitive, and supported by the one-way ANOVA analysis, that business associates breach more records than health plans and healthcare providers. As we saw in **Figure 2**, business associates act as third-party vendors to covered entities, intuitively handling information on behalf of multiple organizations. Business associates provide various array of services to covered

entities, including but not limited to cloud hosting services,[27] help with the transmission of data, and handle sensitive information on behalf of the covered entities.[28] Additionally, businesses associates, unlike covered entities, could have primary operations in industries outside of healthcare. Operating outside of the healthcare industry, coupled with the fact that controls for protecting healthcare data are not clearly defined, create an opportunity for business associates to lack in the implementation of appropriate security and privacy frameworks and controls that protect PHI, thus leading to larger impact on the number of breached records. HIM and cybersecurity professionals need to focus on implementing sound data protection controls, implementing appropriate organizational culture, and educating employees how to protect PHI records. Operating in other industries and having lack of understanding of the HIPAA requirements does not excuse the lack of data protection controls given the amount of data business associates handle. HIM and cybersecurity professionals need to implement frameworks that go above and beyond the HIPAA requirements.

Since there is no true way to ensure alignment and compliance with the HIPAA regulation, HIM and cybersecurity professionals who work for business associates should implement the NIST Cybersecurity Framework (CSF) or the HITRUST Common Security Framework (CSF) to mitigate the effects of successful data breaches.[29] NIST CSF and HITRUST CSF incorporate multiple requirements that are aligned with HIPAA and cover controls across various domains, including but not limited to information protection, access control, physical security, vulnerability management, and data protection and privacy. On the other hand, covered entities (healthcare providers, health plans, and healthcare clearing houses) need to implement third-party (vendor) risk management programs that appropriately and continuously assess the vendors (business associates) they work with. A comprehensive program would allow HIM and cybersecurity professionals to appropriately assess the risk for each of their business associates and mitigate the effects of data breaches caused by those relationships.[30]

This research, just like other research articles and studies, has limitations. The first limitation of the study is relating to the understanding of the HIPAA legislation by the organizations operating in the healthcare industry; specifically, the author assumes the organizations' knowledge of the HIPAA Omnibus and Breach Reporting Role that requires them report all data breaches to the US DHHS including at least 500 records. The lack of understanding of the legislation could have caused some healthcare entities to not report their data breaches, thus rendering the data set potentially incomplete. The second limitation of this research is the US DHHS requirement to only report data breaches that impacted 500 or more individuals. Not reporting breaches that impact less than 500 individuals could skew the results and create uneven distribution of the reported breach instances. The third limitation is related to the accuracy of the data. While the US DHHS audits the documentation of all reported data breaches, not every healthcare entity is audited to ensure accurate representation of the breached number of records.

This research paper sets a foundation for cybersecurity and HIM professionals to understand what contributes to the number of impacted individuals, once data breaches occur. Based on the US DHHS dataset, additional research can be performed to consider the effects of other variables such as the type of data breach, the location of data breach, and the geographical location of the HE type.[16] The understanding of the relationship of these variables and the effects it has on the number of impacted individuals can inform researchers and HIM professionals on how to better

mitigate and reduce the impact breaches have on PHI. Further research, qualitative or quantitative, could offer mitigation strategies that focus on minimizing the impact data breaches have on individuals. Mitigation becomes prevention when the breach, after it occurs, affects zero individuals.

Conclusion

The author of this research paper focused on understanding what affects the number of impacted individuals in successful data breaches. Through quantitative analysis, using one-way ANOVA, the author was able to determine that the healthcare entity type has a main effect on how many records healthcare organizations breach once a breach occurs. More specifically, the author found that business associates breach more information when compared to health plans and healthcare clearing houses. This paper could serve as a foundational piece for future research and change the focus of HIM professionals, which is mostly on how to prevent data breaches, to a combination of prevention and mitigation. Appropriate implementation of cybersecurity frameworks within business associates that go above and beyond the HIPAA regulation requirements could minimize the impact of data breaches and ultimately lead to prevention. Finally, the author calls for additional research that will include additional factors and their effects on the number of impacted individuals.

Notes

1. Mareiniss, Darren P. “The Impending Storm: Covid-19, Pandemics and Our Overwhelmed Emergency Departments.” The American Journal of Emergency Medicine. W.B. Saunders, March 23, 2020. https://www.sciencedirect.com/science/article/pii/S0735675720301753?via%3Dihub.

2. Solomon, Zahava, Karni Ginzburg, Avi Ohry, and Mario Mikulincer. “Overwhelmed by the News: A Longitudinal Study of Prior Trauma, Posttraumatic Stress Disorder Trajectories, and News Watching during the COVID-19 Pandemic.” Social Science & Medicine. Pergamon, April 23, 2021. https://www.sciencedirect.com/science/article/abs/pii/S0277953621002884.

3. Tebeje, Tsion H., and Jorn Klein. “Applications of e-Health to Support Person-Centered Health Care at the Time of Covid-19 Pandemic.” Telemedicine and e-Health 27, no. 2 (2021): 150–58. https://doi.org/10.1089/tmj.2020.0201.

4. Muthuppalaniappan, Menaka, and Kerrie Stevenson. “Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health.” OUP Academic. Oxford University Press, September 27, 2020. https://doi.org/10.1093/intqhc/mzaa117.

5. Yeo, Liu Hua, and James Banfield. “Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis.” Perspectives in health information management. American Health Information Management Association, March 15, 2022. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/.

6. Diaz, Mabeth. “Data Integration and Analysis in Healthcare: A Pivot within the Industry.” D, May 16, 2022. http://d-scholarship.pitt.edu/42689/.

7. Krzyzanowski, Brittany, and Steven M Manson. “Twenty Years of the Health Insurance Portability and Accountability Act Safe Harbor Provision: Unsolved Challenges and Ways Forward.” JMIR Medical Informatics 10, no. 8 (2022). https://doi.org/10.2196/37756.

8. Castelli C, Gabriel B, Yates J, Booth P. “Strengthening digital society against cyber shocks: Key findings from The Global State of Information Security® Survey 2018.” Cybersecurity and Privacy. 2017:22

9. Dykstra, Josiah, Rohan Mathur, and Alicia Spoor. “Cybersecurity in Medical Private Practice: Results of a Survey in Audiology.” 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020. https://doi.org/10.1109/cic50333.2020.00029.

10. Solove, Daniel J. "HIPAA Mighty and Flawed: Regulation has Wide-Reaching Impact on the Healthcare Industry" Journal of AHIMA 84, no.4 (April 2013): 30-31.

11. Abraham, Chon, Dave Chatterjee, and Ronald R. Sims. “Muddling through Cybersecurity: Insights from the U.S. Healthcare Industry.” Business Horizons 62, no. 4 (2019): 539–48. https://doi.org/10.1016/j.bushor.2019.03.010.

12. Bhuyan, Soumitra Sudip, Umar Y Kabir, Jessica M. Escareno, Kenya Ector, Sandeep Palakodeti, David Wyant, Sajeesh Kumar, et al. “Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations.” Journal of Medical Systems 44, no. 5 (2020). https://doi.org/10.1007/s10916-019-1507-y.

13. McLeod, Alexander, and Diane Dolezel. “Cyber-Analytics: Modeling Factors Associated with Healthcare Data Breaches.” Decision Support Systems 108 (2018): 57–68. https://doi.org/10.1016/j.dss.2018.02.007.

14. McDermott, Donna S., Jessica L. Kamerer, and Andrew T. Birk. “Electronic Health Records: A Literature Review of Cyber Threats and Security Measures.” International Journal of Cyber Research and Education 1, no. 2 (2019): 42–49. https://doi.org/10.4018/ijcre.2019070104.

15. Khan, Freeha, Jung Hwan Kim, Lars Mathiassen, and Robin Moore. “Data Breach Management: An Integrated Risk Model.” Information & Management 58, no. 1 (2021): 103392. https://doi.org/10.1016/j.im.2020.103392.

16. Ignatovski, Martin. "Contributing Factors to the Number of Individuals Impacted by Data Breaches in Healthcare Organizations." PhD diss., Capitol Technology University, 2021.

17. Mehrtak, Mohammad, SeyedAhmad SeyedAlinaghi, Mehrzad MohsseniPour, Tayebeh Noori, Amirali Karimi, Ahmadreza Shamsabadi, Mohammad Heydari, et al. “Security Challenges and Solutions Using Healthcare Cloud Computing.” Journal of medicine and life. Carol Davila University Press, 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8485370/.

18. Hassan, Nihad A. “Ransomware Overview.” SpringerLink. Apress, January 1, 1970. https://link.springer.com/chapter/10.1007/978-1-4842-4255-1_1.

19. Kim, Lee JD. “Cybercrime, Ransomware, and the Role of the Informatics Nurse.” LWW, March 2020. https://journals.lww.com/nursing/Citation/2020/03000/Cybercrime,_ransomware,_and_the_role_of_the.17.aspx.

20. Slayton, Thomas B. “Ransomware: The Virus Attacking the Healthcare Industry.” Journal of Legal Medicine 38, no. 2 (2018): 287–311. https://doi.org/10.1080/01947648.2018.1473186.

21. Chernyshev, Maxim, Sherali Zeadally, and Zubair Baig. “Healthcare Data Breaches: Implications for Digital Forensic Readiness.” Journal of Medical Systems 43, no. 1 (2018). https://doi.org/10.1007/s10916-018-1123-2.

22. Dolezel, Diane, and Alexander McLeod. “Managing Security Risk.” The Health Care Manager 38, no. 4 (2019): 322–30. https://doi.org/10.1097/hcm.0000000000000282.

23. Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. “Healthcare Data Breaches: Insights and Implications.” Healthcare 8, no. 2 (2020): 133. https://doi.org/10.3390/healthcare8020133.

24. Gabriel, Meghan Hufstader, Alice Noblin, Ashley Rutherford, Amanda Walden, and Kendall Cortelyou-Ward. “Data Breach Locations, Types, and Associated Characteristics among US Hospitals.” The American journal of managed care. U.S. National Library of Medicine, February 2018. https://pubmed.ncbi.nlm.nih.gov/29461854/.

25. Angst, Corey M., Emily S. Block, John D’Arcy, and Ken Kelley. “When DO IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches.” MIS Quarterly 41, no. 3 (2017): 893–916. https://doi.org/10.25300/misq/2017/41.3.10.

26. U.S., DHHS. “U.S. Department of Health and Human Services Office for Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.” U.S. Department of Health & Human Services - Office for Civil Rights, 2021. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

27. Liu, W., and E. K. Park. “E-Healthcare Cloud Computing Application Solutions: Cloud-Enabling Characteristices, Challenges and Adaptations.” 2013 International Conference on Computing, Networking and Communications (ICNC), 2013. https://doi.org/10.1109/iccnc.2013.6504124.

28. Lee, In. “An Analysis of Data Breaches in the U.S. Healthcare Industry: Diversity, Trends, and Risk Profiling.” Information Security Journal: A Global Perspective 31, no. 3 (2021): 346–58. https://doi.org/10.1080/19393555.2021.2017522.

29. Udroiu, Adriana-Meda, Mihail Dumitrache, and Ionut Sandu. “Improving the Cybersecurity of Medical Systems by Applying the NIST Framework.” 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2022. https://doi.org/10.1109/ecai54874.2022.9847498.

30. Keskin, Omer F., Kevin Matthe Caramancion, Irem Tatar, Owais Raza, and Unal Tatar. “Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports.” Electronics 10, no. 10 (2021): 1168. https://doi.org/10.3390/electronics10101168.

Author Biography

Martin Ignatovski *is the chief information officer at SimplePractice and a doctoral dissertation committee member at Capitol Technology University.*