Journal of Multidisciplinary Healthcare

Dovepress
Taylor & Francis Group

Open Access Full Text Article

ORIGINAL RESEARCH

Cybersecurity in Healthcare: Ensuring Patient Safety and Data Privacy

Diane Dolezel[1], Clemens Scott Kruse[2], Rohit Pradhan[3]

[1]Health Informatics and Information Management Department, Texas State University, Round Rock, TX, 78665, USA; [2]Dean College of Health Sciences, University of Texas at El Paso, El Paso, TX, 79968, USA; [3]School of Health Administration, Texas State University, San Marcos, TX, 78666, USA

Correspondence: Diane Dolezel, Health Informatics and Information Management Department, Texas State University, 100 Bobcat Way, Round Rock, TX, 78665, USA, Email dd30@txstate.edu

Objective: Healthcare data breaches have increased in both frequency and severity, yet limited empirical evidence exists on the factors associated with large-scale breach events. To address this gap, this study analyzed breaches reported to the US Department of Health and Human Services Office of Civil Rights between 2010 and 2025 to determine predictors of large breaches.

Methods: A total of 7327 breach reports from the Office for Civil Rights were analyzed. Logistic regression assessed predictors of high-severity incidents (≥ 100,000 individuals affected). Differences in breach size between incident types were assessed using Wilcoxon rank-sum tests. Negative binomial regression modelled factors associated with breach magnitude and temporal trends in Hacking/IT classifications over time, adjusting for covariates.

Results: Breach sizes were highly right-skewed; the median breach affected 3892 individuals (IQR: 1255–19,471), and roughly 10% of the incidents accounted for the majority of individuals affected. Hacking/IT events were associated with severe breaches (OR = 2.6) and increased from 4% in 2010 to 80% in 2025. Network server incidents resulted in significantly larger breaches than device theft events. Business associate involvement was independently associated with a larger breach magnitude (IRR = 2.0).

Conclusion: Hacking/IT mechanisms, network server involvement, and business associate participation were the strongest factors associated with breach severity and magnitude. These findings highlight persistent vulnerabilities in healthcare organizations and reinforce the need for targeted cybersecurity strategies.

Plain Language Summary: Over the past 15 years, healthcare organizations have experienced a steady rise in data breaches, many of which expose large amounts of patient information. Our analysis reviewed more than 7300 reported incidents to identify the factors linked with the most extensive breaches. Cyberattacks involving hacking were most frequently associated with large-scale events, particularly when attackers accessed network servers. Breaches that involved business associates, such as external vendors, also tended to affect more individuals. Hacking became increasingly common over time and now represents the majority of breaches. These results highlight critical weaknesses in healthcare systems and emphasize the need for stronger security practices and tighter oversight of third-party partners.

Keywords: healthcare data breaches, hacking/IT incidents, network server breaches, business associate involvement

Introduction

In recent years, the healthcare sector has experienced a marked increase in both the number and magnitude of data breaches, outpacing those in other major industries, yet the factors associated with breach severity remain insufficiently understood.[1–3] Advances in digital technologies, including electronic health records, telehealth platforms, cloud-based systems, and interconnected medical devices, have improved care delivery, but their rapid adoption has increased the cybersecurity attack surface.[3,4] Adversaries are using increasingly sophisticated methods to target protected health information (PHI) across fragmented infrastructures, making data security essential for safe and reliable care delivery.[5,6]

https://doi.org/10.2147/JMDH.S609209
Received: 14 March 2026
Accepted: 7 May 2026
Published: 14 May 2026

Health data are valuable to cybercriminals because they combine permanent identifiers, clinical histories, and billing information, making it a prime target for identity theft and insurance fraud.[7,8] Aging legacy systems and increasing IT complexity have also contributed to increased cybersecurity incidents.[9] National data has indicated a shift from breaches involving theft of devices or paper records toward large-scale hacking incidents affecting millions of individuals.[10] Ransomware can restrict access to electronic health records (EHR), delay diagnostics, disrupt medication delivery, and impair scheduling and communication workflows, creating significant patient safety risks.[5] The 2024 Change Healthcare ransomware attack illustrated the operational and clinical consequences of cyberattacks for millions of patients and healthcare organizations.[11]

Multidisciplinary Relevance

Large-scale Health Insurance Portability and Accountability Act (HIPAA)-reportable breaches require coordinated action across information technology, clinical leadership, care coordination, compliance, and administrative teams. Understanding patterns in breach mechanisms, severity, and vendor involvement supports cross-disciplinary prevention strategies, strengthens incident response planning, and improves organizational resilience.

Gap in Literature

Under HIPAA, healthcare organizations must report breaches of PHI affecting 500 or more individuals to the US Department of Health and Human Services Office for Civil Rights (OCR). These mandatory reports provide one of the primary national datasets for studying healthcare breaches. While many healthcare data breaches are small, a limited number of large-scale incidents account for the majority of affected individuals and may pose the greatest risks to patient privacy and healthcare operations.[12]

While the risk associated with healthcare cyber incidents is well documented, there is little empirical research on the predictors of severity in HIPAA-reportable breaches, or on whether specific breach attributes, such as incident type, breach location, or business associate involvement, are associated with high-severity breaches.[2,3,13–15] Although hacking/IT incidents have surpassed all other breach locations in both frequency and the number of affected individuals since 2016,[16] and business associates account for about 30% of HIPAA-reportable breaches in recent years,[10] these variables are seldom examined in multivariable regression models. Also, relatively few studies have examined whether these technical breach factors help explain why some incidents escalate into large-scale events affecting a large number of patients.[2,15] As health systems become more interconnected, understanding the characteristics associated with greater breach impact can inform more targeted cybersecurity strategies and support evidence-based regulatory decision-making.

Aim of the Study

The objective of this study was to identify predictors of high-severity healthcare data breaches within the population of HIPAA-reportable breaches, defined as incidents affecting ≥100,000 individuals. We examined whether key breach characteristics such as hacking/IT mechanisms, breach location, and business associate involvement were associated with breach magnitude. Secondary analyses assessed temporal trends in breach mechanisms across the United States.

Study Hypotheses

H1: Hacking/IT incidents are associated with higher odds of high-severity breaches.

H2: Network server breaches involve a greater number of affected individuals than device-theft incidents.

H3: Business associate involvement independently predicts breach magnitude.

H4: The proportion of breaches attributed to hacking/IT increased over time.

Materials and Methods

Study Design and Data Sources

This retrospective observational study analyzed all HIPAA-reportable healthcare data breaches affecting ≥500 individuals in the US Department of Health and Human Services OCR database. Publicly accessible, de-identified data were downloaded from both the active investigations list and the archived OCR cases on February 6, 2025.

Data Processing and Sample Selection

The OCR download yielded 7384 events reported from 2009 to 2016. To ensure comparable reporting, incidents from 2009 (n=18) and partial-year 2026 (n=28) were removed, resulting in an analytic window of all incidents from 2010 to 2025. The submission date was used as the temporal index because OCR provides no other date field, such as the occurrence date.

Records were screened for completeness and internal consistency. Duplicate events, identified as entries matching exactly on entity name, state, submission date, breach mechanism, breach location, and number of individuals affected, were removed. Missing data (<1%) were handled using listwise deletion, justified due to the low missingness rate and no systematic missingness. After removing seven incomplete records and four duplicates, the final analytic sample included 7327 breaches. All analyses were conducted in R version 4.5.2.

Predictors

The predictor variables were:

- Breach Type was converted to dummy variables (binary: 1 = breach classified into that category; 0 = otherwise). Categories included Hacking/IT, Improper Disposal, Loss, Theft, Unauthorized Access, Unknown, and Other.
- Breach Location was converted to dummy variables (binary: 1 = breach classified in that category; 0 = otherwise). Categories included Desktop Computer, Electronic Medical Record, Email, Laptop, Network Server, Other Portable Electronic Device, Paper/Films, and Other.
- Business Associate Present: Binary (1 = yes, 0 = no).
- Year: continuous variable rescaled as (Year – 2010 base year) to improve model coefficient interpretability and reduce multicollinearity.

Outcome Variables

Four outcomes are aligned with the study hypotheses.

H1: High-severity breach outcome (≥100,000 individuals affected). This threshold was selected because OCR breach sizes are extremely right-skewed, with large breaches accounting for most exposed individuals, and ≥100,000 person breaches occurring regularly in recent years.[16]

H2: Breach size (number of affected individuals) was examined between mutually exclusive network server and device-theft incidents.

H3: Breach magnitude (count of affected individuals) was the outcome. Business associate involvement was a predictor.

H4: Binary outcome of Hacking/IT breach type over time.

Statistical Analysis

All analyses were conducted in R (version 4.5.2). Because organizations could report multiple breaches, the dataset represents repeated events rather than longitudinal cohorts; therefore, regression models used cluster-robust standard errors clustered by reporting facility to account for repeated breaches reported by the same organization. Facility name strings were cleaned and lowercased.

For H1 and H4, logistic regression estimated associations with high-severity breach status and temporal trends in Hacking/IT classification, adjusting for year, breach type, breach location, and business associate involvement.

For H2, the highly skewed distribution of breach sizes was analyzed using a one-sided Wilcoxon rank-sum test comparing network server and device-theft breach magnitude. Rank-biserial correlation reported the effect size.

For H3, negative binomial regression modeled breach magnitude to account for overdispersion. Variance inflation factors indicated no problematic multicollinearity.

Ethical Considerations

This study utilized de-identified, publicly accessible OCR data and was therefore exempt from Institutional Review Board review because it meets federal exemption criteria for publicly available datasets under 45 CFR 46.104.

Results

Sample Characteristics

The analytic dataset included 7327 US healthcare data breaches reported between 2010 and 2025. Breach sizes were highly right-skewed. The mean breach size was 0.128 million individuals, but the standard deviation was 2.49 million, reflecting the influence of a small number of exceptionally large incidents (maximum = 192.7 million). In contrast, the median breach size was 3892 individuals, with an IQR of 1255.5 to 19,470.5, indicating that most breaches were substantially smaller than the upper-tail events. The extreme skewness in the number of individuals affected (skew=67.26) motivated the use of a negative binomial model for modeling count outcomes. High-severity breaches accounted for 741 events (10.1%).

Categorical Variable Descriptive Statistics

Table 1 summarizes breach characteristics by category. Breach locations were not mutually exclusive; organizations could have more than one breach location in a single breach. The most frequently reported locations included network servers (43.76%), Email systems (23.43%), paper or film records (13.44%), and laptops (6.87%), followed by several smaller categories. For breach types, Hacking/IT Incident dominated (58.19%), far ahead of Unauthorized access/disclosure (22.44%) and theft (14.24%). Business associates were present in 29.45% of the breach incidents.

Table 1 Breach Characteristics by Category (N = 7327)

Characteristic	n	Percent
Location		
Network servers	3208	43.76
Email systems	1718	23.43
Paper/film records	985	13.44
Laptops	504	6.87
Electronic medical records	441	6.02
Other	436	5.95
Desktop computers	367	5.01
Portable electronic devices	329	4.49

(*Continued*)

Table 1 (Continued).

Characteristic	n	Percent
Type		
Hacking/IT Incident	4266	58.19
Unauthorized access/disclosure	1645	22.44
Theft	1044	14.24
Loss	246	3.36
Improper disposal	125	1.71
Other	93	1.27
Unknown	16	0.22
Business Associate		
BA Present	2159	29.45

Notes: Locations are not mutually exclusive; percentages may not sum to 100%. Counts for 2025 may be incomplete due to routine reporting lag. Percentages represent the proportion of breaches involving each characteristic.

Annual Breach Frequencies

As shown in Table 2, annual breach frequency increased steadily over the study period. Reported breaches rose from 198 incidents in 2010 (2.70%) to a peak of 745 incidents in 2023 (10.17%). There were slight decreases in 2024 (742; 10.13%) and 2025 (707; 9.65%). The highest sustained levels occurred from 2020 to 2022, with 663 breaches in 2020 (9.05%), 715 in 2021 (9.76%), and 719 in 2022 (9.81%). The 2025 breaches may reflect a reporting lag.

Table 2 Percent of Total Breaches Occurring in Each Study Year (N = 7327)

Year	n	Percent
2010	198	2.70
2011	200	2.73
2012	217	2.96
2013	276	3.77
2014	311	4.24
2015	270	3.69
2016	328	4.48
2017	357	4.87
2018	368	5.02
2019	511	6.97
2020	663	9.05
2021	715	9.76

(*Continued*)

Table 2 (Continued).

Year	n	Percent
2022	719	9.81
2023	745	10.17
2024	742	10.13
2025	707	9.65
Totals	**7327**	**100**

Note: Percents reflect the proportion of all breaches occurring each year.

H1: Hacking/IT Incidents and High-Severity Breaches

Table 3 summarizes the distribution of high-severity breaches and regression results. Of the 741 high-severity breaches, 659 (88.9%) were associated with Hacking/IT incidents. High-severity breaches were significantly more frequent among Hacking/IT incidents than all other breach types (χ^2 (1, N = 7327) = 320.16, p <0.001). Logistic regression indicates that Hacking/IT breaches had 2.63 times higher odds of reaching high-severity status compared to non-Hacking/IT incidents (95% CI: 1.98–3.50). Network server involvement was also associated with greater odds of high severity (OR = 2.68, 95% CI: 1.97–3.65). In contrast, breaches involving paper or film records had lower odds of high severity (OR = 0.33, 95% CI: 0.17–0.64). A small but significant year-to-year increase in high-severity events was observed (OR = 1.03, 95% CI: 1.01–1.06).

H2: Network Server vs Device Theft Incidents

Network server breaches were significantly larger than device theft breaches. The median breach size for network servers was 10,815 (n = 2932, IQR = 58,255) compared to 2036 (IQR: 5016) for device theft incidents (n = 918). This difference was significant (Wilcoxon rank-sum test, W = 1,941,010, p < 0.001) with a moderate effect size (rank-biserial = 0.32, Hodges–Lehmann 95% CI: 0.29–0.35). We used the IQR because it is a robust measure of statistical dispersion, and it ignores extreme values.

Table 3 High-Severity Breach Frequencies and Logistic Regression Results for Hacking/IT Incidents

High Severity Breaches			
Characteristic	**Not high severity**	**High severity**	
Non-hacking	2981	82	
Hacking	3605	659	
Logistic Regression Predicting High-Severity Breaches			
Predictor	**OR**	**95% CI**	**p-value**
Hacking/IT	2.63	1.98–3.50	<0.001
Network server	2.68	1.97–3.65	<0.001
Email	0.77	0.56–1.07	0.126
Another portable device	0.74	0.33–1.64	0.456
Paper/films	0.33	0.17–0.64	0.001
Year (per year increase)	1.03	1.01–1.06	0.009

Note: Odds ratios were exponentiated coefficients from the logistic model.

Table 4 Sizes by Business Associate Involvement and Negative Binomial Regression Predicting Breach Magnitude

Breach Sizes with and without Business Associate Involvement			
Group	**n**	**Median**	**IQR**
BA Not Present	5170	3210	7854
BA Present	2157	6542	21,317
Negative Binomial Regression Results			
Term	**IRR**	**95% CI**	**p_value**
BA present	2.00	1.18–3.38	0.0096
Year	0.95	0.89–1.02	0.192
Hacking/IT incident	2.43	1.43–4.13	< 0.001
Network Server	7.14	4.7–10.84	< 0.001

H3: Business Associate (BA) Involvement and Breach Magnitude

Table 4 presents breach sizes with and without BA involvement. Breaches linked to BAs showed higher median counts and greater variability (median = 6542, IQR= 21,317) compared to breaches without BA involvement (median = 3210, IQR= 7854). Negative binomial regression indicated that BA involvement was associated with larger breach magnitude, after adjusting for breach type (Hacking/IT), network server location, and rescaled calendar year, with clustered standard errors by facility for repeated breaches.

Specifically, breaches involving a BA affected approximately twice as many individuals as those without BA participation (IRR = 2.00, 95% CI: 1.18–3.38, p =0.01). Hacking/IT (IRR = 2.43, 95% CI: 1.43–4.13, p <0.001) and network server location were also independent predictors (IRR = 7.14, 95% CI: 4.70–10.84, p <0.001). Breach magnitude displayed a modest, nonsignificant decrease over time (IRR = 0.95, p =0.19).

H4: Trends in Hacking/IT Incidents Over Time

Figure 1 illustrates the increase in Hacking/IT trends from 2010 to 2025, and Table 5 summarizes Temporal Trends in Hacking/IT by Year. Hacking/IT accounted for 4% of all breaches in 2010, increased steadily over the study period,

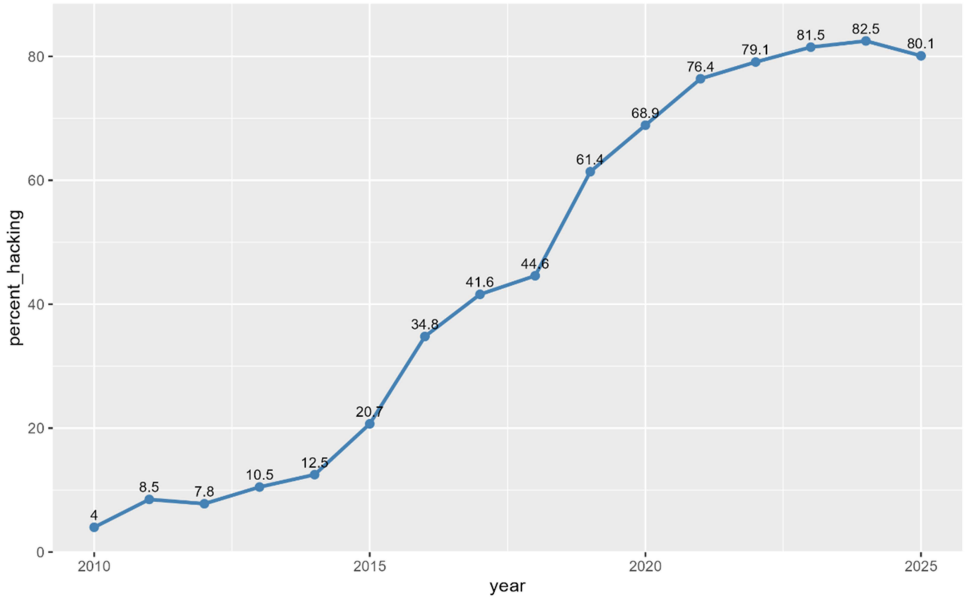

Figure 1 Percent of annual in Hacking/IT trends by year.

https://doi.org/10.2147/JMDH.S609209

Table 5 Temporal Trends in Hacking/IT by Year (N = 7327)

Year	Total Breaches	Number of Hacking/IT Breaches	Proportion of Hacking Breaches
2010	198	8	0.04
2011	200	17	0.09
2012	217	17	0.08
2013	276	29	0.11
2014	311	39	0.13
2015	270	56	0.21
2016	328	114	0.35
2017	357	149	0.42
2018	368	164	0.45
2019	511	314	0.61
2020	663	457	0.69
2021	715	546	0.76
2022	719	569	0.79
2023	745	607	0.81
2024	742	612	0.82
2025	707	568	0.80

Notes: Proportions reflect the proportion of Hacking/IT breaches occurring in each year. Table 5 presents annual counts of total breaches and Hacking/IT breaches. Proportions represent the share of breaches classified as Hacking/IT within each year.

peaking at 82% in 2024, before a slight decline to 80% in 2025. The number of Hacking/IT breaches increased from 8 incidents in 2010 to 568 incidents in 2025. Logistic regression confirmed a strong upward trend, with the year since 2010 being associated with a 38.0% increase in the odds of a Hacking/IT incident (OR= 1.38, 95% CI [1.35–1.40], p <0.001).

Discussion

We analyzed national HIPAA-reportable breaches over 15 years and identified specific factors associated with both breach severity and the number of individuals affected. Breach mechanism, location, and business associate involvement were associated with both breach size and breach frequency. Hacking/IT incidents were associated with higher odds of high-severity breaches and greater breach magnitude in all models. Network-server breaches were consistently associated with larger breach sizes and large-scale breaches. Breaches involving business associates were associated with approximately twice as many affected individuals. Over time, there was a pronounced shift across the study period toward breaches caused by Hacking/IT mechanisms.

Interpretation of Key Findings

Recent evidence underscores the growing dominance of ransomware and other Hacking/IT incidents in healthcare cybersecurity. National analyses indicate that ransomware now accounts for a substantial proportion of affected individuals in large-scale breaches, particularly in recent years.[17] Legacy systems, interconnected systems, and the expansion of digital infrastructure increase the cyberattack surfaces and introduce cyber risk, which contributes to breach persistence.[18] The increase in Hacking/IT incidents, which are now the dominant breach mechanism, highlights the need

for cross-disciplinary collaboration among IT, clinical, legal, and administrative teams to enhance cybersecurity measures and reduce risk across healthcare operations.

This observational study can indicate associations but cannot determine causal relationships. Network server incidents were associated with substantially larger numbers of affected individuals than incidents involving stolen devices, possibly reflecting the concentration of sensitive data in centralized systems. Business associate involvement was associated with approximately twice the number of affected individuals, even after accounting for breach type, location, and year.

These patterns may disrupt clinical workflows and delay access to patient records, although those variables were not available for assessment in this study. Additionally, cyberattacks can potentially compromise patient safety through treatment delays and the malfunction of medical devices like pacemakers, insulin delivery systems, and remote patient monitoring systems.[19]

Comparison with Previous Research

These results align with prior research identifying cyberattacks as a leading cause of large-scale healthcare breaches.[2,14,20] The pronounced effect of network server breaches reflects known vulnerabilities in centralized electronic systems.[14,16] Previous studies also highlighted the risks associated with business associates, whose security practices vary widely and may fall outside the direct governance of healthcare organizations.[9,15] Although earlier work examined these individual risk factors, few studies evaluated breach mechanisms, breach location, and business-associate involvement together at a national scale or assessed the individual contributions to breach magnitude.[2,13] This study fills that gap by simultaneously evaluating breach mechanisms, locations, and business associate involvement at a national level, providing precision as to the influence of technical and organizational characteristics on breach severity.

Implications for Practice

Healthcare organizations should prioritize strengthening network server security with strong access controls, continuous system monitoring, and intrusion-detection technologies. Because hacking incidents encompass multiple attack vectors, organizations should use multiple types of protection, with stronger authentication methods, ransomware safeguards, and vendor access controls. Given that business-associate involvement is associated with larger breaches, organizations should implement stricter vendor-risk management, including standardized cybersecurity requirements and ongoing oversight of third-party partners. The rapid increase in Hacking/IT incidents underscores the importance of proactive cybersecurity measures, such as regular workforce training, timely system updates, and well-practiced incident-response plans to address a growing and increasingly sophisticated threat landscape.

Limitations

This analysis has several limitations. First, its retrospective observational design precludes causal inference and limits the ability to determine whether specific breach characteristics directly lead to higher severity outcomes. Second, the analysis relies on OCR-reported breaches affecting 500 or more individuals, which may introduce reporting bias and under-representation of smaller incidents that could alter observed distributions. Third, breach classifications, such as hacking, network server involvement, or business associate participation, are dependent on reporting entities and may contain misclassification or incomplete information, and they may lack granularity. Specifically, the OCR "Hacking/IT" category combines many different types of cyberattacks, such as ransomware, phishing, and credential theft. Because these attacks are grouped, we cannot determine which specific attack types are driving the observed increases in breach size and severity. As a result, the findings describe overall cyber risk rather than specific attack methods.

Fourth, despite entity name cleaning, deterministic matching may miss near-matches due to minor name or spelling differences across OCR reporting. Fifth, the dataset lacks detailed contextual variables, including security controls in place, attack methods, organizational cybersecurity maturity, or internal vs external threat actor distinctions, constraining interpretation of underlying mechanisms. Sixth, temporal comparisons may be influenced by changes in reporting practices, cybersecurity awareness, and regulatory compliance over time rather than true shifts in threat prevalence. Finally, the breach discovery date would be more accurate, but it was not available in OCR.

Future Studies

Future work should incorporate detailed cybersecurity maturity indicators and examine how these factors affect breach size and frequency. Mapping third-party vendor networks and applying extreme-value modeling could further clarify systemic vulnerabilities and improve estimation of catastrophic breach risk. Research integrating time-to-detect metrics and validated security-readiness measures could also enhance understanding of how system-level preparedness influences breach outcomes. Future studies should examine how organizational cybersecurity practices, breach detection timing, and vendor relationships contribute to large-scale breach events.

Conclusion

Healthcare data breaches are increasingly driven by Hacking/IT incidents, particularly involving network servers and business associates. These breaches have grown both in frequency and in magnitude over the past decade, posing substantial risks to patient privacy and organizational liability. These findings suggest the need for stronger cybersecurity strategies, proactive monitoring, and stricter oversight of third-party data handlers. By addressing these vulnerabilities, healthcare organizations can mitigate the risk and impact of future breaches, protecting both patients and the integrity of the healthcare system. These findings, derived from observational OCR data, reflect associations and should be interpreted accordingly. Future studies could build on this work by using more detailed data and study designs that help clarify why large-scale healthcare data breaches occur. In particular, examining organizational cybersecurity practices, the timing of breach detection, and relationships with third-party vendors may help identify factors that can be addressed to reduce the size and frequency of breaches.

Acknowledgments

The authors have no acknowledgments.

Disclosure

The authors report no conflicts of interest in this work.

References

1. Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res*. 2019;54(5):971–980. doi:10.1111/1475-6773.13203
2. Dolezel DM, Beauvais BM, Stigler Granados PE, Fulton LV, Kruse CS. Effects of internal and external factors on hospital data breaches: quantitative study. *J Med Internet Res*. 2023;25(2023):e51471. doi:10.2196/51471
3. Brantly N. The US health system vulnerabilities. *BMC Health Serv Res*. 2026;26(32). doi:10.1186/s12913-025-13803-5
4. Farhud DD, Zokaei S. Ethical issues of artificial intelligence in medicine and healthcare. *Iran J Public Health*. 2021;50(11):i. doi:10.18502/ijph.v50i11.7600
5. McFarlane C. Healthcare breaches are more costly than financial breaches: here's why. *Forbes*. 2024.
6. Lyngass S. 'We're hemorrhaging money': US health clinics try to stay open after unprecedented cyberattack. Available from: https://www.cnn.com/2024/03/09/tech/medical-supply-chain-cybersecurity/index.html. Accessed February 10, 2024.
7. Alder S. Ascension ransomware attack hurts financial recovery. *HIPAA J*. 2024.
8. Journal C. Ransomware attack linked to permanent shut down of illinois hospital St. Margaret's health in spring valley. Available from: https://www.cpomagazine.com/cyber-security/ransomware-attack-linked-to-permanent-shut-down-of-illinois-hospital-st-margarets-health-in-spring-valley/. Accessed February 10, 2024.
9. HIPAA Journal. Healthcare data breach statistics. Available from: https://www.hipaajournal.com/healthcare-data-breach-statistics/. Accessed September 29, 2024.
10. Ponemon Institute. New ponemon report shows ransomware continues to impact patient safety, according to survey of hospital IT/security leaders. Available from: https://www.businesswire.com/news/home/20230118005592/en/New-Ponemon-Report-Shows-Ransomware-Continues-to-Impact-Patient-Safety-According-to-Survey-of-Hospital-ITSecurity-Leaders. Accessed June 26, 2023.
11. Kanter GP, Rekowski JR, Kannarkat J. Lessons from the change healthcare ransomware attack. *JAMA*. 2024;5(9). doi:10.1001/jamahealthforum.2024.2764
12. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: insights and implication. *Healthcare*. 2020;8(2):133. doi:10.3390/healthcare8020133
13. Raghupathi W, Viju R, Aditya S. Analyzing health data breaches: a visual analytics approach. Article. *Applied Math*. 2023;3(11):175–199. doi:10.3390/appliedmath3010011
14. Ronquillo J, Winterholler E, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open*. 2018;1(1):15–19. doi:10.1093/jamiaopen/ooy019
15. Dolezel D, Mcleod A. Cyber-analytics: identifying discriminants of data breaches. *Perspectives Health Inform Manag*. 2019;16(Summer):1–17.

16. McCoy TH, Perlis RH. Temporal trends and characteristics of reportable health data breaches. *JAMIA*. 2018;320(12):1282–1284. doi:10.1001/jama.2018.9222
17. Jiang JX, Ross JS, Bai G. Ransomware attacks and data breaches in US health care systems. *JAMA Network Open*. 2025;8(5):e2510180. doi:10.1001/jamanetworkopen.2025.10180
18. Qureshi R, Koo I. Comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. *Appl Sci*. 2026;16(3):1511. doi:10.3390/app16031511
19. Patra D, Rajagopalan N. Integration of emerging technologies in cybersecurity for healthcare: a systematic review. *Comput Secur*. 2026;161:104763. doi:10.1016/j.cose.2025.104763
20. HIPPA Journal. Healthcare data breach statistics. 2026.