International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

The Mega Healthcare Data Breaches in the United States (2009 – 2023): A Comparative Document Analysis

Abiola Adedeji Adebanjo*

Harrisburg University of Science and Technology, 326 Mkt St, Harrisburg PA 17101, United States
Email: abiolar.adebanjo@gmail.com

Abstract

This paper presents a comprehensive analysis of the predominant healthcare data breaches in the United States from October 2009 to September 2023, utilizing a mixed-methods approach centered on seven publicly available breach reports. It aims to identify patterns, common factors, and measures to enhance cybersecurity within the sector. Through comparative document analysis, the study examines the nature, causes, and repercussions of these breaches, recognizing external attacks, internal errors, and software vulnerabilities as critical weaknesses. The consequences range from financial and reputational damage to erosion of patient trust. The findings stress the necessity for improved preventive strategies, bolstering of security practices, employee training, vendor oversight, and effective incident response mechanisms. The paper also offers insights into the legal and ethical implications of breaches. It suggests robust cybersecurity measures, including the adoption of emerging technologies like blockchain and AI/ML to deter threats. The recommendations guide healthcare organizations toward establishing robust protections for sensitive health data, ensuring regulatory compliance, and facilitating continuity of trust and care. The paper serves as a call to action for ongoing study into the multidimensional impact of data compromises in healthcare.

Keywords: healthcare data breaches; case study analysis; prevention measures; patient privacy; cybersecurity practices.

1. Introduction

The United States, predictably, is the most targeted country—by frequency, by severity, and by costs—for data breaches, defined as "a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so" [1].

Received: *11/17/2023*
Accepted: *1/17/2024*
Published: *1/27/2024*

---

* Corresponding author.

The U.S. is "the country most commonly targeted by data breaches", with 7,221,177 breaches per one million persons [2]. Also, the U.S. was by far the country with the "largest total number of breached users" in 2021, with 212.4 million accounts affected [3]. Once again, the U.S. is the country incurring, "for the 13th consecutive year", the "highest data breach costs", averaging $9.48 million [4].

Surprisingly, among industries in the United States, the healthcare sector is arguably the most affected in terms of frequency of data breaches and financial losses due to breached records. According to the Identity Theft Resource Center (ITRC)'s 2022 Data Breach Report [5], the healthcare industry had the highest number of data compromise cases i.e. personal data breaches, exposures, and data leaks [6] in the U.S. over the last three years: 2022 (344), 2021 (330), and 2020 (306). Likewise, healthcare, at $10.93 million – a 53.3% jump from 2020 - has surpassed every other sector of American industry in cost per data breach for 13 consecutive years [4].

However, there is a noticeable gap in the literature concerning the magnitude of exposed records because of healthcare data breaches. This aspect has received comparatively less attention in academic, industry, and government studies. This scholarly neglect is concerning because the number of exposed records in a data breach incident is a critical measure of its severity. The larger the number of records exposed, the greater the potential impact on the individuals whose data has been compromised [7].

A systematic analysis of the biggest data breaches that occurred in the U.S. healthcare sector between October 2009 and September 2023 is necessary to bridge this research gap. This investigation will provide insight into the scale, causes, and effects of these breaches. The steep increase in the incidence and magnitude of data breaches in recent years—particularly during and after the COVID-19 pandemic—emphasizes the need for this study. So far this year (the first nine months of 2023), the U.S. Department of Health and Human Services Office of Civil Rights (OCR) breach portal has recorded 511 healthcare data breaches [8]. Similarly, between January and September 2023, four of the 19 cases that constitute this study's shortlist of the greatest healthcare data breaches in the United States from 2009 to the present occurred.

Given that the highly regulated healthcare and public health (HPH) industry has been designated as one of the 16 critical infrastructure sectors [9], understanding the nature and impact of data breaches in this sector is critical. This is because the security of this sector has a direct impact on the country's well-being, affecting everyone who interacts with the healthcare system [10,11].

The significance of this study is twofold. First, it will enhance our awareness of the cybersecurity threats that the healthcare sector is currently being confronted with. Through a 14-year analysis of notable breach incidents, the study will identify common vulnerabilities, assess the effectiveness of current prevention measures, and deliberate on expert recommendations for preventing future occurrences.

Second, the study's findings can be applied by key players in the healthcare sector in a variety of ways. They will provide vital insights for healthcare providers, helping them to better understand the vulnerabilities in their systems and take necessary measures to enhance their security protocols. They will contribute to industry knowledge and professional practice by providing deeper insights into the cybersecurity challenges facing the

healthcare sector. Cybersecurity specialists can use these findings to develop more robust security measures. Policymakers can utilize this information to evaluate and strengthen existing regulatory frameworks such as HIPAA and HITECH.

To achieve the objectives of this study, the following research questions will guide our investigation:

1. What were the biggest healthcare data breaches in the United States from 2009 to 2023, and how many individuals were affected by each breach?

2. What were the primary causes of these breaches? Were they due to external attacks, internal errors, or other factors?

3. What were the impacts of these breaches on the affected individuals and healthcare providers? Did they result in financial losses, reputational damage, or other consequences?

4. What common vulnerabilities were exploited in these breaches? Were certain types of data or systems more prone to breaches than others?

These questions will guide the direction of this study and help to delineate its scope. They are directly tied to the purpose of the study and are designed to be specific, unambiguously stated, and open-ended.

Constraints: Assumptions

In conducting this study, the researcher operated under several assumptions:

1. **Data Availability**: The researcher assumes that sufficient and reliable data on healthcare data breaches from 2009 to 2023 is publicly available and accessible. This includes data from healthcare providers, news articles, and databases maintained by regulatory bodies.

2. **Data Accuracy**: The researcher assumes that the data collected from these sources is accurate and has been reported honestly by the entities involved.

3. **Technological Evolution**: The researcher acknowledges that technology and cybersecurity measures have evolved significantly from 2009 to 2023. Therefore, the conditions surrounding a breach in 2009 may be vastly different from those in 2023.

4. **Bias**: The researcher recognizes the potential for bias in interpreting the data and drawing conclusions. To mitigate this, the researcher commits to a rigorous and systematic approach to data analysis.

These assumptions are essential for framing the research process and interpreting the findings. They will be revisited throughout the study as necessary.

Constraints: Limitations

It is also important to acknowledge the scope of this study. Limitations are potential weaknesses or factors that might affect the outcome of the research. They are factors that the researcher cannot control. They represent the shortcomings of the study, often due to practical or methodological constraints.

The study, while comprehensive, has several limitations:

1. **Research Focus:** The research is focused specifically on the top 19 healthcare data breaches in the United States, selected based on predefined criteria. While these cases provide valuable insights, they may not capture all instances of healthcare data breaches. Nevertheless, this study does enough to contribute to the existing body of knowledge on healthcare data breaches and serve as a foundation for further research and practical interventions.

2. **Data Availability**: The study relies mainly on publicly available data, which may have limitations in terms of completeness and accuracy. Some breaches may go unreported or undisclosed for various reasons, especially legal or reputational concerns.

3. **Data Accuracy**: The accuracy of reported data is dependent on the sources from which they are obtained. If there are errors or discrepancies in these sources, it could affect the study's findings.

4. **Timeframe**: The study only considers data breaches that occurred between 2009 and 2023. Healthcare data breaches outside this period are not included.

5. **Causality Constraint**: The study uses a non-experimental research method, which avoids the manipulation of variables. This limits the ability to explore cause-and-effect relationships [34].

Constraints: Delimitations

Delimitations are boundaries set by the researcher to define the scope of a study. It is important to acknowledge these delimitations as they provide a clear focus to the study. Researchers and stakeholders should consider these limitations when interpreting the findings and applying them to specific contexts or future research endeavors.

Factors that delimit the study include:

1. **Geographical Scope**: The study is restricted to healthcare data breaches in the United States. Its findings may not apply to other countries with different healthcare systems and cybersecurity landscapes.

2. **Type of Breaches**: The study only considers breaches involving more than 500 records [35]. Smaller breaches, despite their potential impact, are not included in the study.

Ethical Considerations

As with any other data-intensive endeavor, the study of healthcare data breaches raises several ethical concerns that must be addressed. These considerations are crucial in maintaining trust in the research process and protecting the rights and interests of individuals whose data is being studied.

1. **Data Provenance**: Understanding the origin of the data is crucial. It's important to ensure that the data was collected and shared ethically.

2. **Purpose of Use**: The purpose for which the data will be used should be clearly defined and justified. Using data for purposes other than those for which it was collected can raise ethical issues.

3. **Data Protection**: Ensuring the security of the data is paramount. This includes safeguarding the data from unauthorized access, use, and sharing.

4. **Privacy**: Respecting the privacy of the individuals whose data is being studied is essential. This includes ensuring that personal information is not disclosed without consent.

5. **Data Preparation**: The process of preparing data for use, including cleaning and anonymization, should be done in a way that respects the rights of the individuals whose data is being used.

6. **Commercial Exploitation**: There are ethical concerns related to sharing patient data with entities that may exploit it for commercial interests.

7. **Data Governance**: Robust data governance structures and procedures need to be in place to ensure ethical access, use, and sharing of health research data.

The author disclaims that all data sources used in this study are publicly available and do not contain sensitive or classified information. The researcher was committed to upholding ethical standards in all aspects of the research process, with respect to confidentiality and compliance with the relevant copyright laws and regulations.

2. Literature Review

This section seeks to track the previous studies according to how they approach each of the research questions under investigation in this study.

What were the biggest healthcare data breaches in the United States from 2009 to 2023, and how many individuals were affected by each breach?

The biggest healthcare data breaches in the United States recorded between 2009 and 2023 have had a significant impact on the privacy and security of individuals' personal health information (PHI). These breaches have exposed sensitive data, including medical records, social security numbers, and financial information, leading to potential identity theft and financial fraud.

According to a report by IBM and the Ponemon Institute, the healthcare industry has experienced a rising frequency of data breaches since 2010, making it one of the most targeted sectors globally [12]. In fact, the healthcare sector is currently one of the top three sectors facing the highest number of breached incidents [13]. Hacking and IT incidents are the most prevalent forms of attack behind healthcare data breaches, followed by unauthorized internal disclosures [14]. Ransomware attacks on hospitals and healthcare organizations have also been a significant concern [15,16].

The number of individuals affected by healthcare data breaches is staggering. From 2005 to 2019, it is estimated that approximately 249.09 million people were affected by healthcare data breaches [17,18]. In 2019 alone, there was a 70% increase in the number of breached health care organizations compared to the six-year average monthly number of breaches [19]. Since 2009, over 176 million patients in the United States have been adversely impacted by data breaches affecting Health Insurance Portability and Accountability Act (HIPAA)-covered institutions [20].

These breaches have had far-reaching consequences. They not only compromise individuals' privacy and security but also have financial implications. The average costs of data breaches today are at an all-time high, globally and in the U.S., at $4.45 million and $9.48 million respectively [4]. Furthermore, breaches significantly affect individuals' trust in companies and their willingness to continue using their services [21].

The healthcare industry needs to prioritize cybersecurity to mitigate the risks associated with data breaches. This includes implementing robust security measures, such as advanced cryptographic techniques for data protection [22]. Additionally, there is a need for increased cybersecurity awareness and training among healthcare personnel to prevent breaches associated with low levels of cybersecurity awareness [23].

In conclusion, healthcare data breaches in the United States from 2009 to 2023 have had a significant impact on individuals' privacy, security, and financial well-being. The frequency of breaches has been on the rise, with hacking and IT incidents being the most prevalent forms of attack. The number of individuals affected by these breaches is alarming, highlighting the need for stronger cybersecurity measures in the healthcare industry.

What were the primary causes of these breaches? Were they due to external attacks, internal errors, or other factors?

The primary causes of healthcare data breaches in the United States from 2009 to 2023 can be attributed to a combination of external attacks, internal errors, and other factors.

External attacks, such as hacking and cyberattacks, have been a significant cause of healthcare data breaches. These attacks involve unauthorized individuals gaining access to healthcare systems and networks to steal sensitive data or disrupt operations. Hacking and IT incidents have been identified as the most prevalent forms of attack behind healthcare data breaches [15]. These attacks can be sophisticated and targeted, exploiting vulnerabilities in the healthcare industry's information systems.

Internal errors and mistakes by employees have also contributed to healthcare data breaches. These errors can

include accidental disclosure of sensitive information, mishandling of data, or failure to follow proper security protocols. Employees may unintentionally expose sensitive data through actions such as sending information to the wrong recipient or misplacing data sources [24]. Additionally, intentional breaches by employees, such as unauthorized access or misuse of data, have also been identified as causes of healthcare data breaches [24].

Other factors that have contributed to healthcare data breaches include technical errors and system vulnerabilities. Technical errors can include misconfigurations, software bugs, or inadequate security measures that leave healthcare systems susceptible to breaches. System vulnerabilities can be exploited by attackers to gain unauthorized access to sensitive data. For example, ransomware attacks on hospitals and healthcare organizations have become a significant concern, where attackers encrypt data and demand a ransom for its release [15].

It is important to note that the healthcare industry's increasing reliance on technology and the digitization of medical records have created new opportunities for data breaches. The interconnectedness of healthcare systems, the use of electronic health records, and the integration of Internet of Things (IoT) devices have expanded the attack surface and increased the potential for breaches [25].

In conclusion, the primary causes of healthcare data breaches in the United States from 2009 to 2023 can be attributed to a combination of external attacks, internal errors, and other factors. External attacks, such as hacking and cyberattacks, have been prevalent, along with internal errors and mistakes by employees. Technical errors and system vulnerabilities have also contributed to breaches. The increasing reliance on technology and the digitization of medical records have created new opportunities for breaches, emphasizing the need for robust cybersecurity measures and employee training to mitigate these risks.

What were the impacts of these breaches on the affected individuals and healthcare providers? Did they result in financial losses, reputational damage, or other consequences?

The impacts of healthcare data breaches on affected individuals and healthcare providers have been significant, resulting in financial losses, reputational damage, and other consequences.

For affected individuals, healthcare data breaches can lead to financial losses and identity theft. Compromised personal information, such as social security numbers and financial data, can be used for fraudulent activities, including opening unauthorized accounts or making unauthorized purchases. Victims may also face the financial burden of resolving these issues and restoring their identities. Additionally, the exposure of sensitive health information can have long-term consequences for individuals, including potential discrimination, denial of insurance coverage, or damage to their reputation [12].

Healthcare providers also face various consequences because of data breaches. Financially, breaches can lead to significant costs associated with investigating and remediating the breach, notifying affected individuals, providing credit monitoring services, and potential legal actions. The loss of patient trust and reputation damage can result in a decline in patient volume and revenue. Healthcare providers may also face regulatory penalties and increased scrutiny from regulatory bodies, leading to additional costs and operational challenges [26].

Furthermore, data breaches can hinder the delivery of healthcare services. The disruption caused by breaches, such as ransomware attacks, can impact the availability and accessibility of critical healthcare systems and patient records. This can lead to delays in patient care, compromised patient safety, and potential medical errors. The loss or inaccessibility of patient data can also hinder medical research and innovation, as it may limit the availability of data for analysis and development of new treatments [27].

The public perception of the healthcare field can also be negatively affected by data breaches. Breaches erode trust in healthcare providers and institutions, making individuals hesitant to share their personal information or seek medical care. This lack of trust can hinder the adoption of digital health technologies and impede efforts to improve healthcare outcomes through data-driven approaches [27].

In conclusion, healthcare data breaches have far-reaching impacts on affected individuals and healthcare providers. Individuals may experience financial losses, identity theft, and reputational damage. Healthcare providers face financial costs, reputational damage, and operational challenges. The delivery of healthcare services can be compromised, and the public perception of the healthcare field can be negatively affected. It is crucial for healthcare organizations to prioritize cybersecurity measures to mitigate the risks and consequences associated with data breaches.

What common vulnerabilities were exploited in these breaches? Were certain types of data or systems more prone to breaches than others?

The vulnerabilities exploited in healthcare data breaches encompass a range of technical and human factors. The increased connectivity of medical devices to existing computer networks has exposed them to new cybersecurity vulnerabilities [15]. Additionally, the reliance on centralized systems in healthcare has been identified as a vulnerability, as these systems are more prone to security vulnerabilities [28]. Furthermore, the use of wearable devices in e-health has introduced vulnerabilities related to data collection, resource constraints, and communication technologies, such as wireless communication [29].

Hacking and IT incidents have been identified as the most prevalent forms of attack behind healthcare data breaches, indicating vulnerabilities in the security of healthcare systems and networks [14]. Privilege abuse and the exploitation of sensitive and protected health data have also been common threats, highlighting vulnerabilities in access control and data protection measures [13]. The increase in the development of smart medical equipment and mobile devices has made the healthcare industry increasingly vulnerable to ransomware, a dangerous type of adaptable malware intended to prevent entry to the system of an entity or establishment [16].

Human factors, such as carelessness and lack of cybersecurity awareness among healthcare staff, have also contributed to vulnerabilities that can be exploited to cause internal or external breaches [30]. The inadvertent disclosure of personal health information through peer-to-peer file sharing programs has also been identified as a vulnerability, emphasizing the importance of user behavior and data handling practices [31].

Certain types of data and systems have been more prone to breaches than others. For example, the cross-institutional sharing of healthcare data has been challenging with current centralized systems, indicating

vulnerabilities in data sharing and interoperability [32]. The increase in the development of smart medical equipment and mobile devices has made the healthcare industry increasingly vulnerable to ransomware, highlighting vulnerabilities in the security of medical devices and IoT systems [16].

In conclusion, healthcare data breaches have exploited a range of vulnerabilities, including technical weaknesses in systems and networks, human factors such as carelessness and lack of awareness, and challenges in data sharing and interoperability. The vulnerabilities in medical devices, centralized systems, and data handling practices have made certain types of data and systems more prone to breaches. Addressing these vulnerabilities requires a comprehensive approach that encompasses technical, human, and organizational aspects of cybersecurity.

3. Methodology

This study employs a comparative document analysis (CDA) approach, a research method that involves the systematic investigation and analysis of existing documents or records [33]. This method is particularly suited to probing the occurrence of mega breaches over a 14-year period because the research questions being pursued in this study involve the historical study of retrospective phenomena and can be carried out using non-obtrusive, resource-efficient processes [34].

The study was conducted through a comprehensive review and analysis of publicly available information and statistics on (healthcare) data breaches collected from government records, industry reports, and academic publications.

The relevant sources selected for this research include:

1. **The Office for Civil Rights (OCR) Breach Portal**: This portal contains information on healthcare data breaches reported to the OCR. It provides insights into the types of breaches, the number of affected individuals, and the organizations involved in these incidents.

2. **The HIPAA Journal**: This website regularly updates its page with the latest healthcare data breach statistics and trends. It has compiled healthcare data breach statistics from October 2009, making it a valuable resource for obtaining information on healthcare-related breaches.

3. **The Protenus Breach Barometer**: This is an annual snapshot of reported or disclosed breaches impacting the healthcare industry, derived from incidents disclosed to the U.S. Department of Health and Human Services or reported in the media.

4. **The ITRC Data Breach Report**: The Identity Theft Resource Center (ITRC) provides annual data breach reports that include information on the number of data breaches and the number of records exposed by industry, including the healthcare sector.

5. **The Verizon Data Breach Investigations Report (DBIR)**: This annual report provides insights into the latest trends and changes in the threat landscape, including information on data breaches in the healthcare industry.

6. **The IBM/Ponemon Institute Cost of a Data Breach Report**: This annual study examines the financial impacts of data breaches, including those in the healthcare sector. It provides insights into the direct and indirect costs associated with data breaches.

7. **The Fortified Health Security Horizon Report**: This annual and mid-year report provides a comprehensive review of the current state of cybersecurity in healthcare, including information on data breaches.

Research Process

To conduct the CDA, the case data collected from the documentary sources were systematically examined and compared using both manual and computer-assisted methods. Qualitative information, such as the nature of the breaches, the contributing factors, the impact on affected organizations and their patients, as well as their response and recovery measures, were analyzed across the different cases. Additionally, quantitative data, such as the number of affected individuals and financial costs, were compared to identify trends or patterns.

Methodology Constraints

The research design choices made for this study and the opportunity costs that arise as a result inadvertently imbue this research with unavoidable tactical limitations. The author of this study acknowledges the implicit limitations associated with using a comparative document analysis (CDA) methodology.

These constraints include:

1. **Data Availability**: The availability and accessibility of relevant documents for the specified period (2009-2023) could be a challenge. Not all data breaches are publicly reported or documented in a way that allows for comparative analysis.

2. **Data Consistency**: The consistency of data across documents might be an issue. Different entities might report breaches differently, making it difficult to compare the data.

3. **Data Volume**: The sheer volume of data breaches during this period could be overwhelming. Between January 1, 2023, to October 31, 2023, more than 82.6 million healthcare records have been exposed or impermissibly disclosed.

4. **Time and Resource Intensive**: As a result of dealing with large volumes of data over an extended period, CDA can be time-consuming and resource intensive.

5. **Qualitative Nature**: CDA is a qualitative method, which means it focuses on understanding the content and context rather than quantifying data. This could limit the ability to make statistical inferences or identify trends.

6. **Subjectivity**: The process of appraising and synthesizing data can introduce subjectivity, which might affect the reliability and validity of the findings.

7. **Changing Standards and Regulations**: The standards and regulations related to healthcare data security have evolved over time. This could affect the comparability of data breaches across different years.

8. **Technological Evolution**: The technology used in healthcare data management and the methods used by hackers have evolved significantly over the years. This could add another layer of complexity to the analysis.

Despite these constraints, CDA can provide valuable insights into the nature, causes, and consequences of healthcare data breaches, and help identify patterns and trends that can inform future prevention strategies.

4. Results

The cases used for this study were obtained exclusively from the 42 entries featured in the "Largest Healthcare Data Breaches (2009 – Sept 2023)" shortlist made by Murray-Watson [8] for the HIPAA Journal website (last updated on October 23, 2023). The list was pruned to 19 after excluding the “business associates” because, according to Murray-Watson [8], the data breaches recorded against some of them may be inaccurate due to past incidents of multiple breach reporting.

The 19 mega breaches shortlisted for this study can be found in Table 1 below:

Table1

No.	Organization	Year	Type	Affected Individuals	Incident
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
3	Excellus Health Plan, Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
4	PharMerica	2023	Healthcare Provider	5,815,591	Ransomware attack
5	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
6	Colorado Department of Health Care Policy & Financing	2023	Health Plan	4,091,794	Hacking/IT Incident
7	Advocate Health and Hospitals Corporation, d/b/a Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft
8	Banner Health	2016	Healthcare Provider	3,620,000	Hacking/IT Incident

9	Florida Healthy Kids Corporation	2021	Health Plan	3,500,000	Hacking/IT Incident
10	Regal Medical Group	2023	Healthcare Provider	3,300,638	Ransomware attack
11	Advocate Aurora Health	2022	Healthcare Provider	3,000,000	Impermissible Disclosure (website tracking code)
12	Dominion Dental Services, Inc./Dominion National Insurance Company/Dominion Dental Services USA, Inc.	2019	Health Plan	2,964,778	Hacking/IT Incident
13	Harvard Pilgrim Health Care	2023	Health Plan	2,550,922	Hacking/IT Incident
14	Forefront Dermatology, S.C.	2021	Healthcare Provider	2,413,553	Hacking/IT Incident
15	21st Century Oncology	2016	Healthcare Provider	2,213,597	Hacking/IT Incident
16	Baptist Medical Center and Resolute Health Hospital	2022	Healthcare Provider	1,608,549	Hacking/IT Incident
17	Inmediata Health Group, Corp.	2019	Healthcare Clearing House	1,565,338	Unauthorized Access/Disclosure
18	Eskenazi Health	2021	Healthcare Provider	1,515,918	Hacking/IT Incident
19	Community Health Network	2022	Healthcare Provider	1,500,000	Impermissible Disclosure (website tracking code)

It is important to note that the data only includes non-business associate HIPAA-covered reporting entities, and certain business associate data breaches are not reflected in the table.

Key takeaways from the data in the given table:

- Out of the 14 years under scrutiny (2009 excluded for having only three months of data), only seven years featured in the study – 2015, 2023, 2021, 2022, 2016, 2019, and 2013.
- Healthcare providers suffer the most mega breach occurrences at 11 hits, followed by health plans at 7 hits, and healthcare clearinghouse at just 1 hit.
- The biggest healthcare data breaches have been caused by hacking/IT incidents, which accounted for 13 out of the 19 breaches and have affected 128,779,111 out of a total 147,990,208 affected patient records, a staggering 87% of occurrences.
- At a distant second are incidents due to Disclosures with just 3 breach occurrences affecting 6,065,338 individuals.
- Ransomware attacks have caused 2 breaches so far in 2023, affecting 9,116,229 individuals.
- Theft caused a single breach in 2013, affecting 4,029,530 individuals.

- The breaches caused by unauthorized access/disclosure have affected the least number of individuals, with a total of 1,565,338 individuals affected.
- The year 2015 saw the highest number of breaches, with 4 incidents affecting 104.3 million individuals, all of which were caused by hacking/IT incidents. This singular year recorded 139% more data breaches in the U.S. healthcare sector than the other six years combined.
- Despite the year 2023 having the same number of breach incidents as 2015, even with three months to go, its 15,758,945 affected records, though second place in the rankings, is 85% less than the 2023 incidences.
- The top 3 mega breaches had four things in common: they all occurred in the year 2015, they were caused by Hacking/IT incidents, and they all affected Health Plans associated with the Blue Cross Blue Shield health insurance network.
- The top 6 mega breaches were shared between the years 2015 and 2023 (albeit not equally, 2015 had two-thirds of the positions leaving the remaining one-third for 2023)

Here are some possible points of discussion based on the findings above:

- The findings show that healthcare data breaches are a serious and persistent threat to the privacy and security of patients' personal health information. The number and impact of data breaches have increased over the years, especially due to hacking/IT incidents, which are the leading cause of breaches. Hacking/IT incidents include cyberattacks such as ransomware, phishing, malware, and denial-of-service attacks, which can compromise the confidentiality, integrity, and availability of healthcare data.

- The findings also reveal that different types of healthcare entities have different levels of exposure and vulnerability to data breaches. Healthcare providers, such as hospitals, clinics, and physicians, suffer the most mega breach occurrences, followed by health plans, such as insurers and managed care organizations. Healthcare clearinghouses, which process health information from other entities, have the least number of breaches. This may reflect the differences in the size, complexity, and security practices of these entities, as well as the value and attractiveness of their data to hackers.

- The findings highlight the need for more effective and proactive measures to prevent and mitigate healthcare data breaches, such as implementing data encryption, conducting regular risk assessments, updating software and systems, training staff on cybersecurity awareness, and complying with the HIPAA Security Rule and other relevant regulations. Additionally, healthcare entities should have contingency plans and incident response protocols in place to minimize the impact and disruption of data breaches, such as notifying affected individuals, reporting breaches to authorities, and restoring normal operations as soon as possible.

- The findings also suggest some areas for further research and analysis, such as exploring the root causes and motivations of hackers, the costs and consequences of data breaches for healthcare entities and patients, the best practices and benchmarks for data breach prevention and response, and the emerging trends and challenges in healthcare cybersecurity.

These findings also raise an interesting new question:

Why was 2015 such a bad year for healthcare data breaches?

According to academic literature, 2015 was a particularly challenging year for healthcare data breaches due to several interconnected factors. The frequency of healthcare data breaches, the magnitude of exposed records, and the financial losses due to breached records were increasing rapidly [14]. Furthermore, the healthcare industry had the highest number of reported data breaches globally in 2015 and was estimated to be the costliest compared to other sectors [36]. In the first half of 2015, 255 healthcare data breach cases were reported, with 130 of these instances being attributed to hacking/IT incidents, accounting for 50.98% of the total breaches [37].

The widespread adoption of mobile consumer devices, such as smartphones, made it difficult to protect health data from risks posed by general-purpose devices [15]. Additionally, the continued use of legacy systems in healthcare organizations, such as Windows XP, which had not been supported since 2014, allowed hackers and malware to easily avoid detection, as evidenced by the WannaCry attack [15].

According to the PricewaterhouseCoopers analysis, the average cost of a single information security and data protection breach doubled during 2015 [38]. In addition, the healthcare industry was a prime target for cybercriminals due to the plethora of sensitive information it holds, such as social security numbers, birth dates, and insurance and billing data, which are notoriously difficult to monitor or safeguard after a breach [39].

One highly regarded industry report, the Verizon 2016 Data Breach Investigation Report reported the claim by ThreatConnect, a cybersecurity firm, that Deep Panda, the Chinese cyber-espionage threat group with suspected ties to its home government [40], was responsible for at least the top 2 mega breaches – Anthem Inc. and Premera Blue Cross – a combined casualty figure of 90 million individual records.

Another well-known industry report, the 2016 Cost of Data Breach Study identified “seven global megatrends” that account for the steep financial implications of adverse cybersecurity incidents [41].

These scholarly and industry sources support the premise that a combination of factors led to a perfect storm for healthcare data breaches in 2015. The challenges posed by the rapid technological advancements, the vulnerabilities of legacy systems, malicious intent by hostile foreign entities, and the increasing financial incentives for cybercriminals created an environment where healthcare data breaches became more frequent and damaging. As a result, the public perception of the healthcare field was negatively impacted, and future research was threatened by more stringent regulatory restrictions.

Summary of key findings:

The cross-sectional analysis of the case studies yielded several insights related to data breaches in healthcare organizations. These findings provide valuable insights into the nature of breaches, their impact, and the contributing factors.

1. **Common Breach Methods**: The case studies revealed that data breaches in healthcare organizations often occurred through methods such as unauthorized access to databases, phishing attacks targeting employees, or compromised third-party vendors.

2. **Impact on Individuals**: The breaches had significant implications for affected individuals, including increased risk of identity theft, medical identity theft, and potential harm to privacy and healthcare decisions.

3. **Contributing Factors**: The breaches were attributable to various contributing factors, including inadequate security controls, lack of employee awareness and training, vulnerabilities in third-party vendor systems, and shortcomings in incident response capabilities.

Evaluation of the effectiveness of current prevention measures

Based on the findings from the case studies, an evaluation was conducted to assess the effectiveness of current prevention measures in mitigating data breaches. This evaluation involved analyzing the preventive measures implemented by the organizations and their level of success in safeguarding sensitive data. It also considered any gaps or shortcomings in the preventive strategies that contributed to the breaches. The evaluation encompassed various aspects, such as:

1. **Security Controls**: The effectiveness of security controls, such as access controls, encryption, and intrusion detection systems, in preventing unauthorized access to sensitive data.

2. **Employee Training and Awareness**: The impact of cybersecurity training and awareness programs on reducing human errors, such as falling victim to phishing attacks or mishandling sensitive information.

3. **Vendor Management**: The adequacy of vendor management practices, including security assessments, contractual agreements, and ongoing monitoring of third-party vendors' security measures.

4. **Incident Response**: The efficiency and effectiveness of incident response plans in detecting and mitigating breaches, as well as the timeliness of breach notification and customer support provided to affected individuals.

5. Discussion

The findings from the case studies have several implications for healthcare organizations and patients:

1. **Strengthened Security Measures**: Healthcare organizations need to enhance their security measures, including robust access controls, encryption, and intrusion detection systems, to protect sensitive patient data from unauthorized access.

2. **Employee Training and Awareness**: Comprehensive cybersecurity training programs should be implemented to educate employees about the risks of phishing attacks and data mishandling, and to promote a culture of security awareness throughout the organization.

3. **Vendor Management**: Organizations must prioritize vendor management practices, conducting thorough security assessments, clearly outlining security requirements in contractual agreements, and regularly monitoring the security practices of third-party vendors.

4. **Incident Response Readiness**: Healthcare organizations should establish effective incident response plans, including prompt breach detection, containment, and notification procedures, to minimize the impact of data breaches and provide timely support to affected individuals.

Future research directions

Based on the findings, several areas for future research in data breaches in healthcare organizations can be identified:

1. **Long-term Impact**: Further research can explore the long-term consequences of data breaches on affected individuals, such as the persistence of identity theft risks and psychological distress.

2. **Cybersecurity Frameworks**: Comparative studies can be conducted to evaluate the effectiveness of different cybersecurity frameworks and best practices in preventing and mitigating data breaches in healthcare settings.

3. **Emerging Threats**: Research is needed to identify and understand emerging threats in the healthcare sector, including the impact of technologies such as Internet of Things (IoT) devices and artificial intelligence on data security.

4. **Legal and Ethical Considerations**: Investigation into the legal and ethical implications of data breaches in healthcare, including the role of legislation, patient consent, and privacy rights, can provide insights for policymakers and practitioners.

By addressing these research directions, future studies can contribute to the development of more effective preventive measures, incident response strategies, and policy frameworks to protect patient data and enhance the overall security posture of healthcare organizations.

Legal and ethical considerations of healthcare data breaches:

Healthcare data breaches have significant legal and ethical implications that require careful consideration. The following are key considerations in this regard:

1. **Legal Compliance**: Healthcare organizations must ensure compliance with applicable laws and regulations governing the protection of patient data. This includes adhering to data protection laws, privacy regulations (such as HIPAA in the United States), and breach notification requirements.

2. **Patient Consent and Transparency**: Organizations should prioritize obtaining informed consent from patients regarding the collection, use, and disclosure of their personal and medical information. Transparent communication with patients about data breaches, their impact, and available remedies is essential to maintain

trust and accountability.

3. **Duty of Care**: Healthcare organizations have a duty to implement reasonable security measures to protect patient data. Failure to fulfill this duty may result in legal liabilities, financial penalties, and reputational damage.

4. **Ethical Obligations**: Healthcare providers have an ethical obligation to protect patient privacy and confidentiality. Breaches that compromise patient data can undermine trust, erode professional relationships, and have detrimental effects on patient care and outcomes.

Recommendations for healthcare organizations to prevent data breaches:

To strengthen data breach prevention efforts, healthcare organizations should consider the following recommendations:

1. **Robust Security Measures**: Implement comprehensive security measures, including strong access controls, encryption, regular vulnerability assessments, and network monitoring, to safeguard patient data from unauthorized access.

2. **Employee Education and Training**: Provide regular cybersecurity awareness training to all employees, emphasizing the importance of identifying and reporting phishing attempts, practicing good password hygiene, and following secure data handling practices.

3. **Multi-factor Authentication**: Implement multi-factor authentication (MFA) for accessing sensitive systems and accounts. MFA adds an extra layer of security by requiring additional verification beyond passwords, reducing the risk of unauthorized access.

4. **Third-Party Vendor Management**: Assess the security practices of third-party vendors before engaging in partnerships, establish clear security requirements in contracts, and regularly monitor their compliance with security protocols.

5. **Incident Response Planning**: Develop and regularly test incident response plans to ensure a swift and effective response in the event of a breach. This includes procedures for breach detection, containment, notification, and providing support to affected individuals.

6. **Data Minimization and Retention Policies**: Adopt data minimization practices to collect and retain only the necessary patient information. Implementing retention policies aligned with legal and regulatory requirements helps reduce the volume of data at risk and mitigate potential harm from breaches.

7. **Regular Audits and Assessments**: Conduct periodic audits and security assessments to identify vulnerabilities, address gaps in security controls, and proactively address potential risks.

8. **Continuous Monitoring and Threat Intelligence**: Employ continuous monitoring systems and leverage threat intelligence to detect and respond to emerging threats promptly.

By implementing these recommendations, healthcare organizations can enhance their data breach prevention efforts, reduce the risk of breaches, and protect patient data, thereby safeguarding patient privacy, maintaining legal compliance, and preserving trust in the healthcare system.

6. Conclusion

This study was predicated on the latest "Healthcare Data Breach Statistics" (last updated on October 5, 2023) compiled by the HIPAA Journal. Murray-Watson [8]. Special attention was paid to the healthcare data breach trends and a comprehensive analysis was conducted on the biggest data breaches in U.S. healthcare organizations from October 2009 to August 2023. Multiple case studies were examined to understand the nature of breaches, their impact on individuals, and the contributing factors. Through the comparison and evaluation of the data, commonalities and differences were identified across the selected cases, and evaluated for the effectiveness of current prevention measures. The key findings highlighted common breach methods, the significant impact on affected individuals, and the contributing factors that led to breaches. These findings underscore the importance of strengthening security measures, enhancing employee training and awareness, improving vendor management practices, and establishing robust incident response capabilities in healthcare organizations. The paper then discussed the legal and ethical considerations associated with healthcare data breaches, emphasizing the need for compliance with relevant laws, patient consent, transparency, and the ethical duty of care towards patient privacy. Additionally, recommendations were provided for healthcare organizations to prevent data breaches, including implementing robust security measures, enhancing employee education and training, and establishing effective incident response plans.

Previous studies

While investigating the mega healthcare data breaches in the U.S. from 2009 to 2023, 41 document sources were consulted and listed as references for this research. The analysis of the 41 references reveals a diverse range of topics within the field of healthcare cybersecurity. The references collectively highlight the importance of robust cybersecurity measures in healthcare, the financial implications of data breaches, and the potential of emerging technologies in enhancing data security. The findings underscore the need for continuous research and development in this field to safeguard sensitive healthcare data.

Taken together, five main themes emerged which could add additional insights and nuances to this study. They are Government Reports and Directives, Cost and Statistics of Data Breaches, Healthcare and Cybersecurity, Technological Solutions and Frameworks, and Case Studies and Research Articles.

Government Reports and Directives: These documents capture the role of government in providing guidelines and directives related to cybersecurity. They include references that discuss government policies and directives related to cybersecurity, such as the U.S. Department of Health and Human Services' guidelines on data breach response plans, indicating the government's proactive approach to managing potential data breaches [1], the White House's policy directive on critical infrastructure security and resilience, underscoring the government's commitment to protecting critical infrastructure, including healthcare systems, from cyber threats [9], and the

"Breach Notification rule" published by the Office of Civil Rights (OCR) [35].

Cost and Statistics of Data Breaches: These documents offer valuable insights into the substantial financial implications of data breaches and the widespread prevalence of such incidents across the United States. These include reports from Proxyrack [2], Surfshark [3], IBM Security [4], Identity Theft Resource Center [5], and Ponemon Institute [41]. Others in this category include [6], [8], and [19].

Healthcare and Cybersecurity: These documents highlight the unique challenges faced by the U.S. healthcare sector in maintaining cybersecurity. They cover a range of topics including the disclosure of data breaches via social media, ransomware attacks on the healthcare industry, and the cybersecurity culture within healthcare critical infrastructures. Resources in this category include [7,10,12,15,16,20,21,23,30,39].

Technological Solutions and Frameworks: These documents explore the role of technology in tackling healthcare cybersecurity challenges. They include proposals and discussions on the use of blockchain technology, machine learning-based frameworks, and ontological frameworks for healthcare web applications security. Resources in this category include [11,13,17,18,22,25,27,28,29,32,37].

Case Studies and Research Articles: These documents provide in-depth insights and implications of healthcare data breaches, discuss legal aspects of processing patient data in health insurance, and evaluate privacy and security vulnerabilities of patients' data in healthcare. They provide real-world examples and detailed analyses of specific issues in healthcare cybersecurity. Resources in this category include [14,24,31,33,34,36,38,40].

Final thoughts and recommendations

Data breaches in healthcare organizations pose significant risks to patient privacy, trust, and the overall integrity of the healthcare system. As technology continues to advance and threats evolve, it is crucial for healthcare organizations to prioritize data breach prevention efforts.

It is recommended that healthcare organizations invest in comprehensive security measures, employee education, and training programs to foster a culture of cybersecurity awareness. Collaboration with third-party vendors should involve thorough security assessments and ongoing monitoring to ensure data protection throughout the supply chain. Incident response plans should be regularly tested and updated to address emerging threats effectively.

Furthermore, healthcare organizations should stay abreast of legal and regulatory requirements, ensuring compliance with data protection laws and breach notification obligations. Open communication with patients about data breaches is vital for maintaining trust and providing necessary support.

Future research should focus on exploring the long-term impact of data breaches, evaluating the effectiveness of cybersecurity frameworks, and addressing emerging threats in the healthcare sector. Additionally, ethical considerations in data breach response and recovery should be further examined to ensure the highest standards of patient care and confidentiality.

By implementing the recommendations and conducting further research, healthcare organizations can strengthen their data breach prevention strategies, protect patient data, and fortify the trust patients place in them. Ultimately, these efforts contribute to a more secure and resilient healthcare ecosystem that safeguards patient privacy and promotes the delivery of quality care.

References

[1] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Administration for Children and Families, "State and Tribal Child Welfare Information Systems, Information Security Data Breach Response Plans," Jul. 01, 2015. https://www.acf.hhs.gov/sites/default/files/documents/cb/im1504.pdf

[2] Proxyrack, "Cost of a Data Breach," *Proxyrack*, Dec. 02, 2022. https://www.proxyrack.com/blog/cost-of-a-data-breach/ (accessed Nov. 04, 2023).

[3] Surfshark, "Data breach statistics by country in 2021," *Surfshark*, Dec. 20, 2021. https://surfshark.com/blog/data-breach-statistics-by-country-in-2021

[4] Ponemon Institute and IBM Security, "Cost of a Data Breach Report," IBM Security, 2023. Accessed: Nov. 04, 2023. [Online]. Available: https://www.ibm.com/downloads/cas/E3G5JMBP

[5] Identity Theft Resource Center, "2022 Data Breach Report," Jan. 2023. Accessed: Jan. 06, 2024. [Online]. Available: https://www.idtheftcenter.org

[6] A. Petrosyan, "Healthcare and Cybercrime in the U.S. - Statistics & Facts." Statista, Dec. 18, 2023. [Online]. Available: https://www.statista.com/topics/8795/healthcare-and-cyber-security-in-the-us/#topicOverview

[7] P. Rosati, P. Deeney, M. Cummins, L. Van Der Werff, and T. Lynn, "Should You Disclose a Data Breach via Social Media? Evidence from US Listed Companies," *Proceedings of the ... Annual Hawaii International Conference on System Sciences*, Jan. 2018, doi: 10.24251/hicss.2018.600.

[8] R. Murray-Watson, "Healthcare Data Breach Statistics." HIPAA Journal, Jan. 06, 2024. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[9] The White House - Office of the Press Secretary, "Presidential Policy Directive - Critical Infrastructure Security and and Resilience," Feb. 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[10] M. Bricknell and S. Horne, "Personal view: security sector health systems and global health," *BMJ Military Health*, vol. 169, no. e1, pp. e64–e67, Sep. 2020, doi: 10.1136/bmjmilitary-2020-001607.

[11] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain Technology in medicine and Healthcare: Challenges and future Perspectives," *Cryptography*, vol. 3, no. 1, p. 3, Jan. 2019, doi: 10.3390/cryptography3010003.

[12] S. Argaw *et al.*, "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, Jul. 2020, doi: 10.1186/s12911-020-01161-7.

[13] A. H. Seh, J. F. Al-Amri, A. F. Subahi, A. Agrawal, R. Kumar, and R. A. Khan, "Machine learning based framework for maintaining privacy of healthcare data," *Intelligent Automation and Soft Computing*, vol. 29, no. 3, pp. 697–712, Jan. 2021, doi: 10.32604/iasc.2021.018048.

[14] A. H. Seh *et al.*, "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[15] L. Coventry and D. B. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.

[16] W. Triplett, "Ransomware attacks on the healthcare industry," *Journal of Business, Technology and Leadership*, vol. 4, no. 1, pp. 1–13, Apr. 2022, doi: 10.54845/btljournal.v4i1.31.

[17] A. Almulihi, F. Alassery, A. I. Khan, S. Shukla, B. K. Gupta, and R. Kumar, "Analyzing the Implications of Healthcare Data Breaches through Computational Technique," *Intelligent Automation and Soft Computing*, vol. 32, no. 3, pp. 1763–1779, Jan. 2022, doi: 10.32604/iasc.2022.023460.

[18] M. Alenezi, "An ontological framework for healthcare web applications security," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, Jan. 2021, doi: 10.14569/ijacsa.2021.0120658.

[19] U. Y. Kabir, E. Ezekekwu, S. S. Bhuyan, A. Mahmood, and A. Dobalian, "Trends and best practices in health care cybersecurity insurance policy," *Journal of Healthcare Risk Management*, vol. 40, no. 2, pp. 10–14, May 2020, doi: 10.1002/jhrm.21414.

[20] S. R. Kessler, S. Pindek, G. Kleinman, S. A. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," *Health Informatics Journal*, vol. 26, no. 1, pp. 461–473, Mar. 2019, doi: 10.1177/1460458219832048.

[21] J. Carré, S. R. Curtis, and D. N. Jones, "Ascribing responsibility for online security and data breaches," *Managerial Auditing Journal*, vol. 33, no. 4, pp. 436–446, Mar. 2018, doi: 10.1108/maj-11-2017-1693.

[22] N. Lewis, Y. Connelly, G. Henkin, M. Leibovich, and A. Akavia, "Factors influencing the adoption of advanced cryptographic techniques for data protection of patient medical records," *Healthcare Informatics Research*, vol. 28, no. 2, pp. 132–142, Apr. 2022, doi: 10.4258/hir.2022.28.2.132.

[23] F. Gioulekas *et al.*, "A cybersecurity culture survey targeting healthcare critical infrastructures," *Healthcare*, vol. 10, no. 2, p. 327, Feb. 2022, doi: 10.3390/healthcare10020327.

[24] S. Rasoulian, Y. Grégoire, R. Legoux, and S. Sénécal, "Service crisis recovery and firm performance: insights

from information breach announcements," *Journal of the Academy of Marketing Science*, vol. 45, no. 6, pp. 789–806, May 2017, doi: 10.1007/s11747-017-0543-8.

[25] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized Privacy-Preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.

[26] F. Gioulekas *et al.*, "A cybersecurity culture survey targeting healthcare critical infrastructures," *Healthcare*, vol. 10, no. 2, p. 327, Feb. 2022, doi: 10.3390/healthcare10020327.

[27] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient Medical Record management," *Npj Digital Medicine*, vol. 3, no. 1, Jan. 2020, doi: 10.1038/s41746-019-0211-0.

[28] A. Ali *et al.*, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, no. 16, p. 2034, Aug. 2021, doi: 10.3390/electronics10162034.

[29] F. Nakayama, P. Lenz, S. Banou, M. Nogueira, A. Santos, and K. R. Chowdhury, "A continuous user authentication system based on galvanic coupling communication for S-Health," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–11, Nov. 2019, doi: 10.1155/2019/9361017.

[30] P. K. Yeng, M. A. Fauzi, and B. Yang, "A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals," *Information*, vol. 13, no. 7, p. 335, Jul. 2022, doi: 10.3390/info13070335.

[31] K. E. Emam *et al.*, "The inadvertent disclosure of personal health information through peer-to-peer file sharing programs," *Journal of the American Medical Informatics Association*, vol. 17, no. 2, pp. 148–158, Mar. 2010, doi: 10.1136/jamia.2009.000232.

[32] J. Fu, N. Wang, and Y. Cai, "Privacy-Preserving in healthcare blockchain systems based on lightweight message sharing," *Sensors*, vol. 20, no. 7, p. 1898, Mar. 2020, doi: 10.3390/s20071898.

[33] X. Ren, Y. Lv, K. Wang, and J. Han, "Comparative document analysis for large Text Corpora," *arXiv (Cornell University)*, Oct. 2015, doi: 10.48550/arxiv.1510.07197.

[34] M. Hassan, "Documentary research - types, methods and examples," *Research Method*, Aug. 15, 2023. https://researchmethod.net/documentary-research/

[35] O. for C. Rights, "Breach Notification rule," *HHS.gov*, Jun. 28, 2021. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

[36] F. B. Satria, U. Iqbal, and M. Rabrenović, "Legal aspects of processing patient data in health insurance according to Taiwan law," in *Удружење за право осигурања ; Удружење осигуравача Србије eBooks*, 2022, pp. 331–342. doi: 10.18485/aida.2022.23.ch24.

[37] H. Alhakami, A. Baz, W. Alhakami, A. Pandey, A. Agrawal, and R. A. Khan, "A usability management framework for securing healthcare information system," *Computer Systems Science and Engineering*, vol. 42, no. 3, pp. 1015–1030, Jan. 2022, doi: 10.32604/csse.2022.021564.

[38] D. Olifer, N. Goranin, A. Kačeniauskas, and A. Čenys, "CONTROLS-BASED APPROACH FOR EVALUATION OF INFORMATION SECURITY STANDARDS IMPLEMENTATION COSTS," *Technological and Economic Development of Economy*, vol. 23, no. 1, pp. 196–219, Jan. 2017, doi: 10.3846/20294913.2017.1280558.

[39] F. Tazi, J. Dykstra, P. Rajivan, and S. Das, "SOK: Evaluating privacy and security vulnerabilities of patients' data in healthcare," in *Lecture Notes in Computer Science*, 2022, pp. 153–181. doi: 10.1007/978-3-031-10183-0_8.

[40] TeamPassword, "Who is Deep Panda and how can you protect yourself?," *TeamPassword*, Aug. 31, 2021. https://teampassword.com/blog/who-is-deep-panda-and-how-can-you-protect-yourself (accessed Nov. 10, 2023).

[41] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," IBM Security, Jun. 2016.