INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

Volume 4 | Issue 1 Art. 13

2025

An Analysis of Legal Measures to Protect Sensitive Health Care Data from Cyberattacks

Sreelakshmi PR and Jyotirmoy Banerjee

An Analysis of Legal Measures to Protect Sensitive Health Care Data from Cyberattacks

Sreelakshmi PR and Jyotirmoy Banerjee

LLM Student, Amity Law School, Amity University, Bengaluru
Assistant Professor, Amity Law School, Amity University, Bengaluru

Manuscript Received 04 Jan. 2025 **Manuscript Accepted** 06 Jan. 2025 **Manuscript Published** 08 Jan. 2025

ABSTRACT

The rapid adoption of advanced technologies such as the Internet of Medical Things (IoMT), smart devices, information systems, and cloud services has transformed the healthcare industry, significantly enhancing accessibility and service delivery. These innovations have improved patient care, streamlined operations, and provided convenience for both providers and patients. However, this progress has also led to increased vulnerability, with the healthcare sector becoming a prime target for cyberattacks. Data breaches have emerged as a major challenge, compromising the confidentiality, integrity, and availability of sensitive healthcare data, with far-reaching consequences for organizations, clients, stakeholders, and the broader business ecosystem. This study offers a comprehensive analysis of healthcare data breaches, categorizing various types of breaches and assessing their prevalence, impact, and causes. It investigates the increasing frequency of these breaches, the rising magnitude of compromised records, and the escalating financial losses. The research reveals that hacking and IT-related incidents are the most common causes of breaches, while unauthorized internal disclosures, though less frequent, still pose significant risks. Healthcare data, which is highly valuable, is an attractive target for cybercriminals due to the sensitive nature of personally identifiable information (PII), medical histories, insurance details, and financial data. These breaches can disrupt operations, erode trust, and jeopardize patient safety. Using two time series analysis techniques simple moving average and simple exponential smoothing, the study further analyses historical data to identify trends *and project future occurrences of breaches. The findings indicate a troubling upward trend in both the frequency and financial impact of healthcare data breaches, highlighting the urgent need for robust data security measures, improved monitoring, and effective risk management frameworks.*

KEYWORDS

Cyber Attacks, Health Care Data Breach, Protect Data Confidentiality.

INTRODUCTION

The healthcare industry has undergone a significant digital transformation over the last few decades, driven by advances in information and communication technology. Traditional paper-based systems have been replaced with Electronic Health Records (EHRs) and other digital platforms to improve healthcare delivery, enhance patient care, and streamline operations. Electronic systems provide healthcare providers and patients with easy and constant access to critical health information, leading to better disease management, more accurate diagnoses, and improved efficiency. Additionally, the proliferation of smartphones, cloud-based services, and interconnected smart devices has reshaped the way healthcare services are accessed and delivered, further accelerating the digitalization of healthcare processes.[1]

While this digital revolution offers numerous benefits, it also introduces significant risks. Healthcare data, which includes sensitive patient information such as personally identifiable information (PII), medical histories, insurance details, and financial records, has become a prime target for cyberattacks. Unlike other types of data, healthcare data commands a higher value in the black market due to its comprehensive nature and utility for identity theft, insurance fraud, and other malicious purposes. Cybercriminals exploit vulnerabilities in healthcare systems to steal, manipulate, or hold sensitive data for ransom, creating serious challenges for healthcare organizations in safeguarding patient privacy and maintaining trust.

Healthcare systems rely on interconnected technologies, including Electronic Medical Records (EMR) systems, Order Communication Systems (OCS), Picture Archiving and

[1] Adil Hussain Seh et al., *Healthcare Data Breaches: Insights and Implications*, 8 Healthcare (Basel) 133 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/ (last visited Dec 19, 2024).

Communication Systems (PACS), and wearable medical devices. These systems facilitate data storage, sharing, and real-time analysis to enhance clinical decision-making and patient outcomes. However, their reliance on networks and the internet makes them highly susceptible to breaches. In addition to external cyber attacks, insider threats, whether malicious or unintentional, pose another risk to healthcare data confidentiality. A single data breach can result in significant financial losses, reputational damage, legal consequences, and compromised patient care.

To address these growing challenges, governments and regulatory bodies worldwide have implemented various legal measures aimed at protecting sensitive healthcare data from cyber attacks. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and similar frameworks in other regions establish guidelines for data protection, privacy, and security in the healthcare sector[2]. These regulations mandate healthcare organizations to implement security safeguards, report breaches, and ensure compliance with legal requirements to protect sensitive information.

Despite the existence of these legal frameworks, cyberattacks on healthcare systems continue to rise in frequency and sophistication. This highlights gaps in the implementation, enforcement, and effectiveness of current legal measures. The rapid evolution of technology and the increasing complexity of cyber threats necessitate a continuous reassessment of existing laws and the development of proactive strategies to mitigate risks.

DIGITAL HEALTH CARE DATA AND ITS CONFIDENTIALITY

In this modern society, national borders are increasingly irrelevant in the context of cyberspace. Businesses across multiple industries have benefitted from new opportunities and revenue streams by shifting their business models to incorporate digital technologies. Digitalization has allowed organizations to expand operations, streamline processes, and achieve unprecedented levels of growth and efficiency. In the healthcare sector, digitalization has revolutionized the way medical services are delivered, facilitating better interaction with healthcare professionals, enabling quicker decision-making regarding

[2] Sara Belfrage, Gert Helgesson & Niels Lynøe, *Trust and Digital Privacy in Healthcare: A Cross-Sectional Descriptive Study of Trust and Attitudes towards Uses of Electronic Health Data among the General Public in Sweden*, 23 BMC Med Ethics 19 (2022).

treatment, and improving patient outcomes. It has also enhanced the ability to share medical data seamlessly across systems, creating an interconnected ecosystem of healthcare providers, patients, and medical technologies[3].

Healthcare innovation through digital platforms, mobile applications, and integrated web systems is primarily focused on optimizing the work of medical professionals, improving patient care, reducing human errors, and lowering operational costs. Technologies such as telemedicine, wearable health devices, and cloud-based health information systems have made patient data accessible in real-time, helping medical professionals make more informed decisions[4]. Furthermore, data integration in this sector enables the smooth exchange of electronic information, minimizing the expenses and technical challenges of building interfaces between disparate systems. This interconnected ecosystem ensures continuity of care, better coordination among providers, and improved patient satisfaction.

The integration of the "Internet of Medical Things (IoMT)" has been a significant driver of digital transformation in healthcare. IoMT encompasses connected medical devices, such as wearable monitors, smart diagnostic tools, and implantable devices, which collect, transmit, and analyze patient data. While these devices have improved clinical efficiency and personalized care, they also introduce new risks to privacy and data security[5]. The sheer volume of data generated by IoMT, combined with its transmission across networks and cloud servers, has increased the vulnerability of healthcare systems to cyberattacks.

One of the primary challenges of healthcare digitalization is ensuring the security and confidentiality of sensitive patient data. Cybercriminals recognize the value of healthcare data, which includes personally identifiable information (PII), medical records, and financial details. These records are highly sought after on the black market, making healthcare organizations prime targets for cyberattacks. Unauthorized access, data breaches, and ransomware attacks pose significant risks to patient privacy and

[3] Shyh-Wei Chen et al., *Confidentiality Protection of Digital Health Records in Cloud Computing*, 40 J Med Syst 124 (2016).

[4] Ahmed Arafa, Haytham A. Sheerah & Shada Alsalamah, *Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review*, 14 Information 640 (2023), https://www.mdpi.com/2078-2489/14/12/640 (last visited Dec 19, 2024).

[5] Mohammad Zarour et al., *Ensuring Data Integrity of Healthcare Information in the Era of Digital Health*, 8 Healthcare Tech Letters 66 (2021).

trust, while also threatening the financial stability and operational integrity of healthcare organizations.[6]

- ***Digital Technologies in the Healthcare Sector***

Many medical advances have come and gone over millennia, but none have had as transformative an impact as digital technologies. Innovations in networking and computing have expanded the spectrum of medical therapies and revolutionized the way healthcare professionals operate. Digital tools, including cloud platforms, smart devices, and integrated health systems, now enable the seamless storage, sharing, and management of medical data. These innovations enhance decision-making, optimize workflows, and improve the delivery of patient care.

The primary security objectives for the healthcare sector are to ensure the protection of patient information, maintain privacy and confidentiality, and preserve the availability and integrity of healthcare systems. The shift to Electronic Health Records (EHRs), telemedicine, and Internet of Medical Things (IoMT) devices has enabled continuous access to patient data, improved diagnostic capabilities, and better patient outcomes[7]. However, these advancements have also brought new risks, particularly in the areas of cybersecurity and data privacy.

IoMT devices, such as wearable monitors, implantable medical devices, and connected diagnostic tools, collect vast amounts of sensitive health data. This data, when transmitted across networks or stored in cloud servers, becomes vulnerable to cyberattacks. Healthcare data is particularly valuable to cybercriminals due to its comprehensive nature, which can be exploited for identity theft, insurance fraud, and ransomware attacks. The increasing reliance on digital systems has made healthcare organizations attractive targets for hackers seeking to compromise sensitive information.

Healthcare providers also face the challenge of maintaining compliance with stringent legal and regulatory requirements. Laws such as HIPAA and GDPR mandate the implementation of safeguards to protect patient information

[6] Metty Paul et al., *Digitization of Healthcare Sector: A Study on Privacy and Security Concerns*, 9 ICT Express 571 (2023), https://www.sciencedirect.com/science/article/pii/S2405959523000243 (last visited Dec 19, 2024).

[7] Nicholas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. Ill. L. Rev. 681 (2007).

from unauthorized access and breaches[8]. Despite these measures, many healthcare organizations lack the necessary cyber security infrastructure, expertise, or investment to defend against sophisticated cyber threats. This gap leaves healthcare systems exposed to data breaches, operational disruptions, and financial losses[9].

- ***Protect Sensitive Health Care Data***

Data security remains a significant concern across industries, particularly in healthcare, as many organizations fail to recognize that it extends beyond regulatory compliance. While compliance focuses on meeting minimum standards, data security ensures the comprehensive protection of sensitive information. According to the U.S. Department of Health and Human Services, privacy involves the appropriate use and disclosure of individuals' health information, whereas security focuses on safeguarding that information, specifically in its electronic form, through national standards.

In simpler terms, privacy pertains to the access and use of a patient's health information, while security ensures its confidentiality, integrity, and availability. These concepts, although distinct, are interconnected and play a critical role in improving patient care and building trust. Privacy ensures that only authorized individuals access sensitive data, while security measures such as encryption, firewalls, and secure data transfer protocols to protect this information from breaches, loss, or unauthorized use[10]. Failure to address either privacy or security can result in data leaks, identity theft, and legal penalties, causing damage to both the patient and the organization. More importantly, it can erode trust, which is essential for delivering effective patient care. Healthcare providers must understand that robust data security strategies go beyond compliance frameworks like HIPAA; they involve a proactive approach to risk management and continuous improvement.

By prioritizing both privacy and security, organizations not only meet regulatory requirements but also ensure a safer environment for handling sensitive health information. This, in

[8] HIPAA vs. GDPR compliance: what's the difference?, https://www.onetrust.com/blog/hipaa-vs-gdpr-compliance/ (last visited Dec 19, 2024).

[9] Ateya Megahed Ibrahim et al., *Balancing Confidentiality and Care Coordination: Challenges in Patient Privacy*, 23 BMC Nurs 564 (2024).

[10] Angelo Costa et al., *A Legal Framework for an Elderly Healthcare Platform: A Privacy and Data Protection Overview*, 33 Computer Law & Security Review 647 (2017).

turn, improves patient outcomes, enhances organizational reputation, and fosters trust within the healthcare ecosystem[11].

KEY LEGAL FRAMEWORKS FOR PROTECTING HEALTHCARE DATA

India's data protection framework has evolved significantly over the years, with various legislative measures aiming to address the challenges of protecting personal data in an increasingly digital world. Historically, India's primary legal provisions related to data protection included the Information Technology Act, 2000 (IT Act), and the Sensitive Personal Data or Information (SPDI) Rules, 2011. These provisions laid the groundwork for data protection in the country but were limited in scope, particularly as data usage and digital transactions grew more complex[12].

To strengthen the protection of personal data, India introduced several draft bills, including the Personal Data Protection Bill, 2019 (PDPB 2019) and the Data Protection Bill, 2021 (DPB 2021). These drafts were designed to address the shortcomings of the IT Act and SPDI Rules, but it was only with the enactment of the Digital Personal Data Protection Act, 2023 (DPDP 2023) that a comprehensive and updated legal framework was established.

The act brought a shift into the concept of data protection and it replaces Section 43A of the IT Act and the SPDI Rules, which had governed the handling of sensitive personal data. These older provisions were considered inadequate in addressing the scale and complexity of digital data processing in today's environment. Further the Act 2023 introduces robust provisions concerning the processing of personal data, including the requirement for clear consent from data subjects, the establishment of data protection authorities, and the imposition of strict penalties for data breaches[13].

Under the DPDP Act 2023, data fiduciaries, or entities that collect and process personal data, are required to adhere to strict data processing norms, ensuring that data is collected for lawful

[11] 5 Ways To Protect Sensitive Healthcare Data, https://www.healthitoutcomes.com/doc/ways-to-protect-sensitive-healthcare-data-0001 (last visited Dec 19, 2024).

[12] M. Banerji, *India Enacts New Rules Governing the Storage of Personal Data*, 6 Journal of Intellectual Property Law & Practice 863 (2011), https://academic.oup.com/jiplp/article-lookup/doi/10.1093/jiplp/jpr159 (last visited Dec 19, 2024).

[13] Himanshu, *Cybersecurity Law: Challenges and Legal Frameworks for Protecting Digital Assets and Privacy Rights*, 2 IJL 18 (2024).

purposes, processed transparently, and stored securely. It further gives individuals an right over their data and such rights include the right to access, correct, and erase their own personal information whenever it is necessary. Furthermore, the act introduces mechanisms for data portability, giving individuals greater control over how their data is used across different platforms and services.

One of the critical aspects of the DPDP Act 2023 is its emphasis on data localization and cross-border data transfers. The Act mandates that certain categories of data must be stored within India, while also setting conditions for the transfer of personal data to other countries. This was introduced with a view of safeguarding national interests and ensuring that data remains protected within the country's legal jurisdiction.

While the DPDP Act 2023 provides a broad and general framework for data protection, India also recognizes the need for sector-specific regulations, especially in sensitive areas like healthcare. This is why the Digital Information Security in Healthcare Act (DISHA) and the Health Data Management Policy, 2022 (HDMP) have been proposed as additional frameworks for data protection in the healthcare sector[14]. These sector-specific regulations are designed to address the unique challenges of managing sensitive health-related data, which requires heightened safeguards due to its potential to cause harm if misused.

The DISHA framework aims to protect digital health data by creating a secure ecosystem for the collection, storage, and sharing of health information. It includes provisions for ensuring the privacy and security of health data, while also promoting the use of health data for research and innovation, under strict regulatory oversight. Similarly, the HDMP sets guidelines for the management of health data, including data ownership, consent, and security measures, while also encouraging the use of digital technologies to improve healthcare delivery.

Despite the passage of the DPDP Act 2023, these health-specific frameworks have not been rendered redundant. Instead, they complement the general provisions of the DPDP Act by addressing the specialized requirements of healthcare data protection. The introduction of these dual layers of data protection legislation are general and sector-specific which reflects India's

[14] Digital Information Security in Healthcare Act | eStartIndia, https://www.estartindia.com/, https://www.estartindia.com/knowledge-hub/blog/digital-information-security-in-healthcare-act (last visited Dec 19, 2024).

evolving approach to safeguarding personal data while recognizing the need for tailored solutions in certain sectors[15].

EMERGING CYBER THREATS IN HEALTHCARE

The healthcare industry is a primary target for cybercriminals due to its vast collection of sensitive data, critical infrastructure, and increasing reliance on networked devices, collectively making it a highly valuable and vulnerable target. Several factors contribute to this focus on healthcare by cyber threat actors, including:

- *Sensitive Data*: Healthcare organizations hold a wealth of sensitive information, such as patients' health records and payment card details. This data is invaluable to cybercriminals, who target healthcare organizations to steal, sell, or exploit it. Given the volume of personal information centralized in one place, healthcare systems are particularly appealing targets for data theft.
- *Critical Infrastructure*: Healthcare organizations are essential for public well-being, often being involved in life-saving activities. This dependency makes them more susceptible to ransomware attacks, as cybercriminals know that healthcare organizations are highly likely to pay ransoms to restore critical operations. When healthcare systems are disrupted, patient care is impacted, which can force organizations to comply with ransom demands.
- *Internet of Medical Things (IoMT*): The rise of connected medical devices in healthcare facilities introduces another layer of vulnerability. Many of these devices, which are integral for patient care, often have inadequate security protections. Cybercriminals exploit vulnerabilities in these devices to gain access to the organization’s networks and sensitive data.
- *Data Breaches*: Cybercriminals often target healthcare systems to steal large volumes of sensitive data, such as medical records and personal health information. Data breaches can lead to identity theft, financial fraud, and reputational damage for healthcare providers.
- *Ransomware:* This type of attack is especially dangerous for healthcare organizations, which depend on their data and systems for patient care. Ransomware can lock an organization's systems, halting medical services and demanding a ransom for their release. Healthcare

[15] Commentary: Protecting healthcare privacy: Analysis of data protection developments in India, Indian Journal of Medical Ethics, https://ijme.in/articles/protecting-healthcare-privacy-analysis-of-data-protection-developments-in-india/ (last visited Dec 19, 2024).

organizations are often willing to pay to restore critical functions quickly.

- *Malware*: Malware, including infostealers, can infect healthcare systems to steal login credentials or other sensitive data. Attackers may use this malware to gain unauthorized access to secure systems, allowing them to steal or corrupt sensitive information.
- *Distributed Denial of Service (DDoS*): DDoS attacks overwhelm healthcare networks with traffic, rendering them inoperable. Attackers may demand a ransom to stop the attack, causing operational disruptions and delays in patient care.
- *Phishing:* Phishing attacks deceive individuals into providing sensitive information, such as login credentials or credit card numbers. These attacks are often a precursor to more damaging threats like data breaches or ransomware attacks, as they allow cybercriminals to infiltrate systems and access critical data[16].

CASE STUDIES

- ***Singhealth Data Breach (2018)***

The most significant and high-profile healthcare data breach in Singapore occurred in 2018 when the personal data of 1.5 million patients, including Prime Minister Lee Hsien Loong, was stolen. The breach occurred in the IT systems of SingHealth, one of Singapore's largest healthcare clusters. Attackers gained unauthorized access to the database, primarily targeting outpatient medication records.

The hackers infiltrated the IT network through a vulnerability in the system. The stolen data included patients' names, NRIC numbers (National Registration Identity Card numbers), addresses, and dates of birth. However, the attackers did not access critical medical information or financial details.

The breach prompted immediate action from the Singapore government and the healthcare sector. The Cyber Security Agency of Singapore (CSA) and the Personal Data Protection Commission (PDPC) launched investigations into the breach. In response to the incident, SingHealth implemented several security enhancements, including network monitoring and stronger access controls, and adopted a multi-layered

[16] Cyber-attacks on critical health infrastructure, https://www.who.int/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure (last visited Dec 19, 2024).

cybersecurity approach. Additionally, the government reviewed cybersecurity practices across all public healthcare institutions.

The breach underscored the importance of cybersecurity and personal data protection in the healthcare sector. Singapore's Personal Data Protection Act (PDPA), enacted in 2012, came under scrutiny for ensuring that healthcare organizations meet the necessary security standards. The breach led to discussions about further tightening data protection laws and increasing penalties for data breaches[17]

- ***The Indian Medical Association (Ima) Vs. The Central Government (2018)***

This case primarily deals with the issue of protecting healthcare data and patient privacy in India. The IMA, a leading medical body in India, filed a petition seeking stronger safeguards for the protection of sensitive health data stored in digital formats. This petition came in the wake of increasing concerns about unauthorized access and misuse of personal health information, which was becoming a target for data breaches and cyberattacks.

The IMA argued that there was an urgent need for a robust framework to ensure that patient health records and other sensitive data were securely managed, stored, and shared in the digital age. The petition urged the government to formulate a comprehensive law to govern the security of health data, focusing on privacy, consent, and the rights of individuals to control their health information.

In response, the government acknowledged the need for stronger regulations and agreed that health data needed to be better protected. This case played a pivotal role in raising awareness about the importance of healthcare data protection in India and contributed to discussions that led to the formulation of more stringent data protection laws, such as the Digital Information Security in Healthcare Act (DISHA) and the Health Data Management Policy (HDMP)[18].

[17] Public Report of the COI into the cyber-attack on Singapore Health Patient Database, https://www.mddi.gov.sg/media-centre/press-releases/public-report-of-the-coi/ (last visited Dec 19, 2024).

[18] Diva Rai, *Insight on Digital Information Security in Healthcare Act, 2018*, iPleaders (Nov. 15, 2020), https://blog.ipleaders.in/insight-on-digital-information-security-in-healthcare-act-2018/ (last visited Dec 19, 2024).

- ***Care Shield Life Data Breach (2020)***

In 2020, the Ministry of Health (MOH) in Singapore reported a breach of the CareShield Life scheme, which provides long-term care insurance. The breach involved unauthorized access to the data of 50,000 individuals, which included personal and medical details.

A contractor working on the CareShield Life project was responsible for accessing the data without proper authorization. While the breach was contained, it raised concerns about the access control and oversight mechanisms in place for sensitive healthcare data. Following the breach, the MOH and the related agencies conducted internal reviews and audits to address the vulnerabilities and strengthen access controls. The incident led to the introduction of new safeguards and regulations aimed at preventing unauthorized access to personal healthcare information[19].

CONCLUSION

The protection of sensitive healthcare data from cyber threats is becoming increasingly critical as the healthcare sector continues to rely on digital systems. Healthcare organizations are facing an uptick in cyber-attacks, including ransomware, data breaches, phishing, and malware, which target valuable patient information. These attacks not only compromise patient privacy but also undermine the trust that patients place in healthcare providers. Legal frameworks designed to safeguard healthcare data, such as the Information Technology Act, 2000 (IT Act) and the Sensitive Personal Data or Information (SPDI) Rules, 2011, have laid a foundational structure for data protection. The introduction of the Personal Data Protection Bill, 2019, and the Digital Personal Data Protection Act, 2023 (DPDP Act) has further strengthened these protections by mandating stricter data security measures and penalties for non-compliance.

However, the effective implementation of these legal provisions faces significant challenges. One of the primary difficulties is the rapidly evolving nature of cyber threats, which often outpace the legislative response. The growth of technologies such as the Internet of Medical Things (IoMT) has introduced new vulnerabilities, as many medical devices lack adequate security, providing potential entry points for cybercriminals. Legal frameworks must evolve to address these emerging risks.

[19] Liudmyla Pryimenko, *7 Real-Life Data Breaches Caused by Insider Threats*, Syteca (2023), https://www.syteca.com/en/blog/real-life-examples-insider-threat-caused-breaches (last visited Dec 19, 2024).

Furthermore, smaller healthcare organizations often struggle with limited resources to comply with rigorous cybersecurity standards, making them more vulnerable to attacks.

In addition, while the legal frameworks outline clear data protection requirements and penalties, enforcement remains a challenge. With a wide range of public and private entities involved in healthcare, ensuring consistent compliance and robust cybersecurity across all stakeholders is a complex task. This requires enhanced oversight, coordination between regulatory bodies, healthcare providers, and technology vendors to effectively mitigate cyber threats and safeguard sensitive healthcare data.