HACKING HEALTH: ANALYZING CYBERSECURITY RISKS IN THE MEDICAL DOMAIN

ABSTRACT

The rapid digital transformation of the healthcare sector has brought about significance advancements in patient care and record management. However, it has also exposed the industry to an increasing number of cyber threats. The digital storage of healthcare data has made it an appealing target for cybercriminals. Some of the emerging threats in the digital landscape encompass ransomware attacks, data breaches, vulnerabilities in Internet of Things (IoT) devices, as well as persistent phishing and social engineering schemes. These threats not only jeopardize patient privacy and data integrity but also present substantial financial; and legal risks to healthcare institutions.

In order to effectively handle these concerns, healthcare organizations need to make cybersecurity a top priority. It is absolutely necessary to coordinate efforts across different industries in order to exchange threat knowledge and develop effective defense measures. In this increasingly digital world, the protection of patient health information is not just a legal need, but also a moral commitment that must be met in order to safeguard the health of patients and uphold the credibility of healthcare service providers.

KEYWORDS:

Health, Data Privacy, Cybersecurity, Ransomware Attacks, Digital.

INTRODUCTION

The term "*personal data*" is defined under ***S.3(28)*** of the Personal Data Protection Bill, 2019 (referred to as "PDPB 2019" henceforth). Moreover, according to ***S. 3(36)*** of the Personal Data Protection Bill (PDPB) 2019, the data is additionally classified as "sensitive personal data," including financial data, health data, official identification, genetic data, transgender status, and other related categories. To this day, there has been no enactment of Indian legislation that properly safeguards "personal data," including information pertaining to an individual who may be identified directly or indirectly.[1]

The advent of the digital era brought about significant breakthroughs in all sectors, with healthcare being particularly impacted. The transition from traditional paper-based documentation to digital systems has had a transformative impact on the provision of healthcare services, enabling enhanced coordination, improved accessibility and heightened accuracy of medical data. Nevertheless, the advent of digital transformation has presented a distinct array of issues in the realm of cybersecurity vulnerabilities. The healthcare industry, which is entrusted with the protection of highly confidential and personal information such as patient medical records, is currently facing a significant challenge of combating cyberattacks.[2]

EXPLORATION OF ISSUES

1. THE HEALTHCARE DATA REVOLUTION:

The transition from paper-based to electronic health records (EHRs) has undoubtedly revolutionized healthcare. These digital systems have expedited access to patient information, enhanced treatment coordination and improved overall patient care. However, this technological advancement has also made healthcare data more susceptible to cyberattacks. In this digital age, patient medical records, treatment histories and personal information are stored electronically, providing cyber criminals with new opportunities for exploitation.

2. THE RISING TIDE OF CYBER THREATS:

A. RANSOMWARE ATTACKS:

[1]Bhumesh Verma, "Health Data Privacy - The Emerging Need," PL (CL) Apr, p. 82 (2020).
[2] Emily Harding and Harshana Ghoorhoo, *Background on Ransomware Attack* (Centre for Strategic and International Studies, 2022).

Ransomware attacks have emerged as a pervasive and grievous threat to healthcare data. These malevolent intrusions render the data of a healthcare institution in accessible until a ransom is paid. The dire consequences include delayed patient care and significant financial losses. In some instances, patient data has been permanently lost, posing a severe risk to both privacy and patient safety.[3]

B. DATA BREACHES:

Data intrusions continue to be a concern, frequently resulting from vulnerabilities such as weak passwords, insufficient network security and even basic human error. These intrusions expose sensitive patient data, making it an ideal target for identity theft and financial deception. In addition to the financial impact, data breaches can erode healthcare institutions credibility too.[4]

C. INTERNET OF THINGS (IOT) VULNERABILITIES:

The proliferation of IoT devices, such as medical devices and wearable technologies, in healthcare settings has introduced new cyberattack vectors. Even though these devices offer numerous advantages for patient care and monitoring, they frequently lack comprehensive security measures, leaving them vulnerable to exploitation by cybercriminals.

D. PHISHING AND SOCIAL ENGINEERING:

Phishing attacks continue to beset healthcare organizations, capitalizing on naïve employees with deceptive emails and social engineering techniques. These attacks can result in the unauthorized disclosure of sensitive patient information and are especially devious due to their reliance on human manipulation.

3. THE CONSEQUENCES OF CYBER ATTACKS:

A. PATIENT SAFETY COMPROMISED:

The compromise of patient safety is possibly the most alarming effect of cyberattacks in healthcare. In some instances, ransomware attacks can alter patient data, resulting in potentially fatal misdiagnoses or improper treatments.

[3] Dustin Volz and Robert McMillan, 'Hackers Hit Hospitals in Disruptive Ransomware Attack' *The Wall Street Journal* (2020).
[4] Guy Martin, Paul Martin et al., "Cybersecurity and Healthcare," *British Medical Journal* Vol. 358, (2017).

B. FINANCIAL LOSSES:

Cyberattacks frequently result in substantial financial losses for healthcare institutions. These losses include the cost of remediation, legal fees, and the erosion of public trust, which can lead to a decrease in the number of patients and revenue.[5]

C. LEGAL AND REGULATORY PENALTIES:

Failure to comply with data protection regulations, such as the Health Insurance Portability and Accountability Act (HIPAA)[6], can lead to severe legal and regulatory penalties including substantial fines and reputational harm.

FINDINGS AND ANALYSIS

A. THE RANSOMWARE ATTACKS:

Globally, the prevalence of ransomware has significantly impacted the healthcare industry, however, the situation in India poses unique and specific obstacles. According to the reports from Indian Computer Emergency Response Team (CERT-In), there is a noticeable increase in ransomware attacks directed on healthcare facilities in India, which is consistent with the worldwide pattern. Prominent instances, such as the recent ransomware attack on AIIMS Hospital in 2022[7] draw attention to the gravity of the matter, while worldwide occurrences like the 2017 Wanna Cry attack on the National Health Services (NHS) of the UK serve as the comparable benchmarks.[8] Cyberattacks are increasing day-by-day, as per the report published by the Cyber Peace Foundation and Autobot Infosec Private Ltd, last year alone in the health industry, India faced in total of 1.9 million cyberattacks.

B. THE PERIL OF DATA BREACHES:

Data intrusions in healthcare organizations have national and international repercussions.[9] The "Data Security Council of India (DSCI) Annual Cybersecurity Breach Survey' reveals that the costs of data breaches in India are on the rise, including regulatory penalties and reputational

[5] Owen Dyer, "Hacker's Demand Ransom to Release Encrypted US Medical Records," *British Medical Journal* Vol.353, (2016).
[6] *Health Insurance Portability and Accountability Act of 1996* (US).
[7] Anuja Jaiswal, "Delhi: Ransomware Cyber-attack on AIIMS Server," *TNN* (23 November 2022).
[8] Roger Collier, "NHS Ransomware Attack Spreads Worldwide," *National Centre for Biotechnology Information*, (2017).
[9] Malcolm Harkins and Anthony M Freed, 'The Ransomware Attack on Healthcare Sector," *Journal of Law* (Vol 6, No 2).

harm. These findings are consistent with global trends, as highlighted by the Ponemon Institute's annual Cost of Data Breach Report".

Further Silverman's[10] emphasizes the need for more stringent data protection measures in line with the international guidelines. Moreover, in the recent case of Lifecare Hospitals data breach, the court emphasized the need to strengthen the legal obligations of healthcare institutions to protect patient data, mirroring international legal trends in data breach cases.

C. IoT VULNERABILITIES AND REGULATORY SCRUTINY:

IoT vulnerabilities transcend national boundaries; they are a worldwide concern.[11] In the recent incident in 2022, a major hospital chain that runs over 1000 hospitals in U.S. was hit by cyberattack, resulting in impact of millions of American's data.

The global campaign to tackle cybercrime is growing, with substantial legislative advances. The EU parliament and European Council have approved the Network and Information Security Directive 2 (NIS 2.0), which replaces the original NIS directive. NIS 2.0 aligns the EU with the US and imposes rigorous incident reporting standards, requiring organizations to disclose cyber breaches and assaults within 24 hours of becoming aware of them, with significant fines for noncompliance.

In accordance with international efforts to establish IoT security standards, the Ministry of Electronics and Information Technology (MeitY) of India has issued guidelines for securing IoT devices in healthcare. Regulatory organizations, such as the Indian Council of Medical Research (ICMR), have emphasized the need for stringent Internet of Things (IoT) security standards, mirroring global efforts in this regard.

D. PHISHING AND SOCIAL ENGINEERING SCHEMES:

Phishing and social engineering are worldwide challenges that plague healthcare organizations in India throughout the world. According to the reports from Indian cybersecurity firms such as K7 Computing, healthcare organizations have suffered huge financial losses as a result of these attacks. Further, The Verizon Data Breach Investigations Report (DIBR) focuses on the global effect of social engineering techniques in healthcare

[10] David L Silverman, "Developments in Data Security Breach Liability," *The Business Lawyer* Vol.72(1),p.185, 185-194 (2017).

[11] Swaroop Poudel, "Internet of Things Underlying Technologies, Interoperability and Threats to Privacy and Security," *Berkeley Technology Law Journal* vol. 31(2), p. 997-1022 (2016).

data breaches. Further, Kevany's[12] research emphasizes the need of targeted cybersecurity awareness programs and further emphasized the legal ramifications of participating in phishing schemes, echoing worldwide legal features. These findings highlight the importance of increasing cybersecurity measures in healthcare, both locally and worldwide, in order to avoid significant financial losses.

E. THE IMPERATIVE FOR PROACTIVE SECURITY:

Reports such as the "Healthcare Data Privacy and Security" by the Data Security Council of India (DSCI) provide light on the intricate nature of adhering to healthcare data protection legislation in India. The aforementioned national findings are consistent with the worldwide issue of harmonizing cybersecurity practices with legislative obligations.

The General Data Protection Regulation (GDPR) of the EU is widely recognized as a notable illustration of rigorous data protection legislation from a global standpoint. Although not originating from India, it has exerted a significant impact on a worldwide discussion pertaining to data protection and privacy, including the ongoing development of India's data protection framework.[13]

RECOMMENDATIONS

1) REGULAR CYBERSECURITY TRAINING AND AWARENESS:

Ensure healthcare professionals get regular cybersecurity training and awareness. They should learn about phishing and how to handle suspicious emails and behaviors. Armed with knowledge, employees can defend against cyberattacks.

2) ROBUST ACCESS CONTROL AND AUTHENTICATION:

Control data access to authorize individuals with strict guidelines. To verify user identification and secure critical healthcare data, employ multi-factor authentication (MFA).

3) FREQUENT SOFTWARRE UPDATES AND PATCH MANAGAMENET:

[12] Sebastian Kevany and Deon Canyon, *Combating Health-Related Cyber Security Threats with Health Systems Approaches*, (Daniel K. Inouye Asia-Pacific Centre for Security Studies, 2021).
[13] Johan Turell and Vincent Boulanin, *Cyber-Incident Management*, (Stockholm International Peace Research Institute, 2020).

Keep operating systems, apps and medical equipment updated with security patches. Patch management should be reviewed and updated regularly to fix vulnerabilities and limit the attack surface.

4) **DATA ENCRYPTION AND BACKUP STRATEGY:**
Strong encryption protects patient data in transit and at rest. Set up strong data backup and recovery policy to periodically backup and restore essential healthcare data in the event of a cyberattack like ransomware.

5) **CYBERSECURITY INSURANCE MANDATE:**
Introduce legislation that mandated the healthcare organizations to have cybersecurity insurance coverage. In the event of a cyberattack, this would assist in mitigating financial losses.

CONCLUSION

Within the dynamic landscape of the intersection between healthcare and digital technology, the presence of cyber threats is a significant concern, potentially compromising the security and confidentiality of patient information and fundamentally impacting the healthcare sector. This comprehensive analysis has revealed a disconcerting revelation: the healthcare industry is currently embroiled in an ongoing struggle against enemies who exploit weaknesses, posing a threat not just to patient confidentiality but the fundamental trust at the core of medical practice.

As we conclude this critical essay, it is evident that the message resonates strongly. The importance of cybersecurity in the healthcare industry extends beyond regulatory compliance and technical expertise. It represents a deep ethical dedication to maintaining patient trust, ensuring uninterrupted care, and safeguarding the privacy and integrity of each person's medical experience. In the realm of education, we prioritize robust access controls, diligent protection measures, and prompt incident response to fortify the fundamental aspects of secure healthcare delivery in an era characterized by complex digital systems. Amidst a multitude of challenges, our steadfast commitment to the well-being of our patients is evident. We prioritize the security and confidentiality of their data, while also striving to maintain their unwavering trust in the healthcare industry.

REFERENCES

- B. Balamurugan, D. Sumathi et al., *Digitization of Healthcare Data Using Blockchain*, p. no. (Wiley, 2022).
- W Andrew H Gantt, *Healthcare Cybersecurity* (American Bar Association 2021).
- Daniele Giansanti, *Cybersecurity and the Digital Health* (MDPI AG 2022).
- Dinesh Chandra Dobhal, Kamlesh C. Purohit et al., *Cyber Trafficking, Threat Behaviour and Malicious Activity Monitoring for Healthcare Organizations*, (IGI Global, 2023).
- Amit Kumar Singh and Mohammad Elhoseny, *Intelligent Data Security Solutions for E-Health Applications* (Elsevier Science 2020).
- Personal Data Protection Bill, 2019.
- Anuja Jaiswal, 'Delhi: Ransomware Cyber-attack on AIIMS Server' *TNN* (23 November, 2022).