Evaluating Cybersecurity Risks in Modern Healthcare: Quantitative Assessment of Biomedical Device Compromises and Electronic Health Records Tampering

Kumar Amitabh[1], Anurag Mathur[2]

[1]National Institute of Electronics and Information Technology
Agartala, Tripura, India
kumar.amitabh@nielit.gov.in

[2]National Institute of Electronics and Information Technology
Agartala, India
dir-agartala@nielit.gov.in

***Abstract*:**
The adoption of digital technologies in the health sector has provided better operational effectiveness and care to patients while presenting critical cybersecurity vulnerabilities. The work presented here is the analysis of the cyber risks to the electro-medical devices used in the healthcare sector. An investigation has been done into the occurrences, cost implications, and implications on patient safety due to cyber-attacks on biomedical devices and Electronic Health Records (EHR). The significant data set of industry reports, case studies, and hospital breach records were analyzed and investigated using statistical methods. It provided a data-driven understanding of the relative risks imposed by compromising of biomedical devices and EHR tampering. The financial impact and burden imposed by the cyber-attack and EHR tampering have been elaborated. The findings of the work emphasize the differences and similarities between attack vectors, consequences, and mitigation strategies. It also provides evidence-based recommendations towards fortifying healthcare providers' cyber security measures.

***Keywords*:** Biomedical, Cybersecurity, Electronic Health Records, Financial Impact, Healthcare, Tampering.

(Article history: Selected from 3rd NICEDT 2025, Ropar, 14-15 Feb 2025)

I. INTRODUCTION

The healthcare sector is becoming increasingly dependent on interconnected digital Systems, biomedical devices, software, IT networks, and EHRs for improved patient care and streamlined operations [1]. The benefits of safe EHR are better healthcare efficiency which brings about substantial positive effects on the quality of treatment and safety for patients [2]. Among the biomedical devices that monitor and control patient status in real-time, and EHRs that hold sensitive patient data, there are vulnerabilities to cyber-attack [3].

The Indian healthcare system is considered one of the most important and fast-growing sectors with the availability of accessible and affordable treatment plans [4]. This is considered an important key for making healthcare more easily accessible to all of the people in India. When the Pandemic was declared, unruly exponential demand hit the healthcare system [5], so a rise in teleconsultation evolved [6]. This transformation has put an advanced step into the healthcare industry that has integrated patient data saved alongside cybersecurity measures for networked medical devices [7].

It has been found that phishing attacks are on the increase in the healthcare industry [8]. One of the major problems faced by healthcare organizations while dealing with these attacks is the accurate detection of phishing attacks [9]. With the help of basic security standards and strategies at both organizational and individual levels will help us rise against cyberattacks [10].
EHRs are hacked for various underlying reasons. Stolen information is used for economic benefit by either selling or used in identity theft, for blackmailing, for fraudulent billing, for industrial espionage, for hacktivism, for revenge or for curiosity and learning [11]. EHRs are attractive for hackers since they contain individual and financial information, while

being vulnerable to penetration attacks. Although sharing and accessing patient data has been simpler due to the increasing usage of electronic health databases [12], there is now a greater chance of security and privacy breaches.

This study aims to compare biomedical device compromises and EHR tampering by looking at it through the quantitative lens, hence giving valuable insights into how many times this happens, the financial costs incurred, and the impacts on patient safety.

In the context of this paper, it is our aim to present comparisons between and contrasts of compromised biomedical devices and EHR tampering in terms of the respective cybersecurity risks. It shall discuss how such attacks impact healthcare systems, open vulnerabilities, and assess present-day mitigation strategies. It does so by pointing out differences and similarities in various aspects of threat vectors, impact, and challenges towards mitigating these cybersecurity concerns.

The primary aim of this paper is to carry out a quantitative comparative analysis of cyberattacks targeting biomedical devices and EHRs in healthcare. We wish to answer the following research questions:
RO1: How frequently are biomedical devices and EHRs targeted in cyberattacks?
RO2: What are the cost implications of each attack type?
RO3: How are these attacks impacting patient safety and healthcare operations?

The study will address these questions to provide actionable recommendations for healthcare institutions to improve their cybersecurity strategies. This will help the study present actionable recommendations for health care institutions on how best to enhance their cybersecurity strategy.
The Chi-square test is a statistical method used to analyze categorical data. I helps to establish significant association between two categorical variables. It also establishes whether an observed frequency distribution is different from an expected distribution.

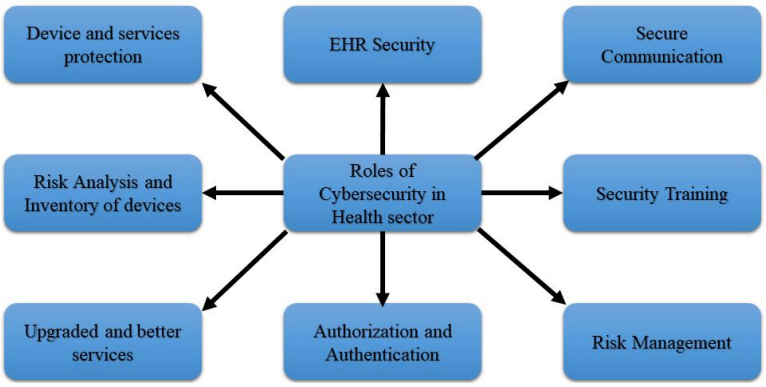

Fig.1. Roles of cybersecurity in health sector

Fig.1. illustrates the various roles of cybersecurity in health sector. Cybersecurity in health sector provides device protection, health services protection, EHR security, secure communication, analysis of risk to the devices, secure authorization and authentication to EHRs, management of risk, security training.

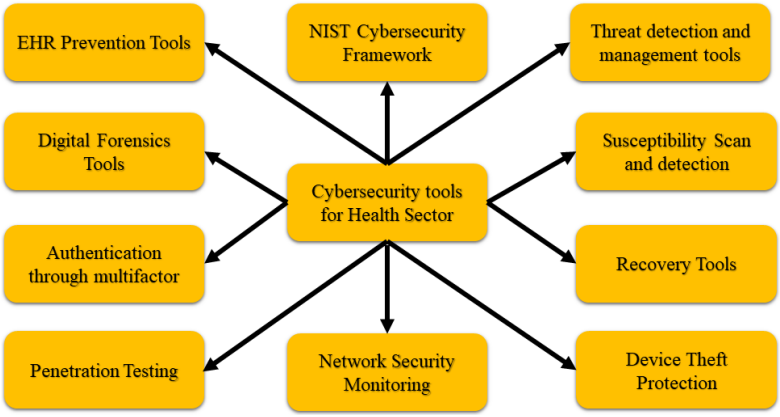

Fig.2. Cybersecurity tools for health sector

Fig.2. Illustrates the different tools of cybersecurity for health sector. NIST cybersecurity framework is largely used for healthcare providers to address cybersecurity risks. Other tools used are threat detection management, susceptibility scan, recovery, device theft protection, network security monitoring, penetration testing, access control, digital forensics, and EHR prevention.

II. METHODOLOGY

A three step method – data collection, data analysis and statistical method, was used for this research. A comprehensive study and analysis was carried to get the comparative evaluation of the cyber-attack threats to the biomedical devices and EHRs. A quantitative analysis report was computed for a decade from 2013 to 2022 and frequency of yearly attacks and tampering with EHRs was generated. The financial cost of the biomedical device attacks and the EHR tampering attacks were also computed and tabulated. Fig. 3 illustrates the methodology flow chart.

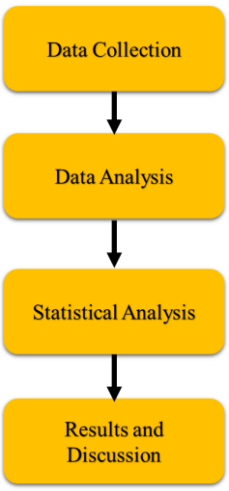

Fig.3. Methodology Flow chart

The data for the work were obtained from different levels of sources. Annual reports from cybersecurity companies, including IBM security [13], Verizon [14], and Symantec were obtained [15]. It gave an insight into the number of cases and financial losses due to the healthcare related cyberattacks. The hospitals breach information was obtained from the U.S. Department of Health and Human Services' Breach portal [16]. It provides the breach reports of biomedical devices and EHRs. To measure the effects of major cyberattacks on healthcare systems on patient safety and hospital operations, pertinent case studies were examined.

Data analysis revolved around three important metrics – frequency of attacks, financial costs, and patient safety impact. For computing the frequency of attacks, the reported number of incidents about biomedical devices and EHRs within the last ten years (2013 – 2023) was gathered for estimations of each attack's frequency. The financial costs include the average financial cost per incident, computed upon adding ransom payments, recovery costs, and regulatory fines. The effect of each type of attack on patient safety was measured using a qualitative-to-quantitative scoring system ranging from minimal (no direct harm) to severe (life-threatening).

Statistic tests were used to find if the observed frequency, cost, and safety-in-patient impacts from biomedical device compromises and EHR-related tampering were also statistically significant. For example, independent sample t-tests and chi-square tests were applied.

The statistical tests of chi-square and independent-samples t-tests were conducted to establish the significance of the discrepancies in EHR tampering versus biomedical device compromises. Following Chi-square test formula is used:

$$\chi 2 = \Sigma \frac{(O - E)^2}{E} \quad (1)$$

Where, O is observed frequency and E is expected frequency.
Such tests were essential for the purpose of ascertaining the statistical significance of the variations in the observed differences between costs, frequency, and impact on patient safety.

III. RESULTS

A. *Frequency of attacks*

The total number of incidents of cyberattacks on biomedical devices and EHR tampering attacks during 2013 to 2023 were accounted for and analyzed. The estimation of each attack's frequency was computed. It has been illustrated in Table – 1.

TABLE 1. FREQUENCY OF ATTACKS

Year	Biomedical device attacks	EHR Tampering attacks
2013	3	12
2014	4	18
2015	6	20
2016	8	24
2017	7	28
2018	10	32
2019	12	35
2020	15	40
2021	17	38
2022	18	41
2023	22	44
TOTAL	122	332

From the data in Table – 1, it is inferred that the frequency of cyberattacks on biomedical devices have increased significantly over the last decade, from 3 in 2013 to 22 in 2023. On the other hand, the frequency of EHR tampering incidents have also increased significantly, from 12 in 2013 to 44 in 2023. Figure 4 illustrates the increasing trend of frequency of cyberattacks.

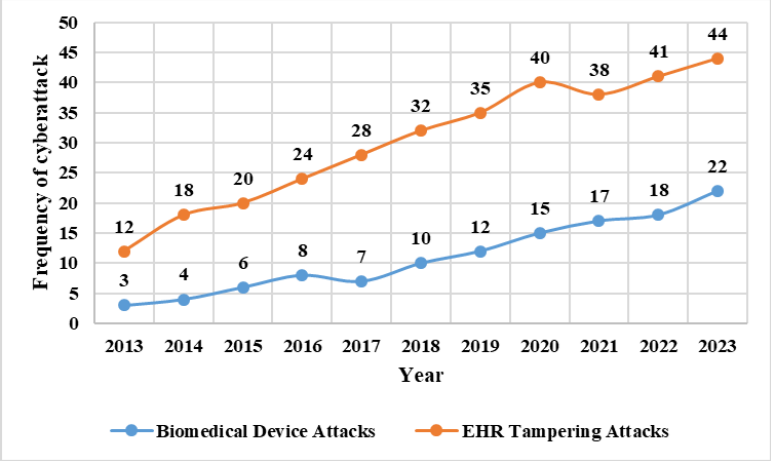

Fig.4. Increasing trend of cyberattack on healthcare sector

Reported incidents of cyberattacks on biomedical devices increased steadily from 2013 to 2023, with a total of 122 over the ten-year period. Compared with this, tampering cases involving EHR occurred more frequently, with 332 reported cases. The use of a chi-square test in statistical analysis indicated a difference in the frequency of attacks in both categories, as indicated by $p < 0.01$, thus making the case that EHRs are attacked more often than biomedical devices.

B. *Financial Costs*

Both kinds of attacks generally involve heavy financial losses but EHR tampering generally tends to have higher costs. The reasons are the complexity of recovering patient records, the increased volume of sensitive data held in EHR systems, and the penalties imposed by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for data breaches. The financial burden is nevertheless substantial because of device maintenance, system outages, and possible patient injury, even though the average cost of biomedical device attacks is somewhat lower. The cost impact is illustrated in Table – 2.

TABLE 2. COST IMPACT OF CYBERATTACK ON HEALTH SECTOR

Attack Type	Average Cost per Incident (USD)	Total Incidents	Total Cost (USD)
Biomedical Device Attacks	2.8 million	122	341.6 million
EHR Tampering Attacks	3.6 million	332	1195.2 million

According to an independent-samples t-test, the average financial cost of EHR tampering attacks was significantly higher than that of biomedical device attacks ($p = 0.03$), indicating that EHR tampering is more detrimental to the economy. The graphical comparison of financial cost between the two types of cyberattacks on health sector is represented in the figure 5.

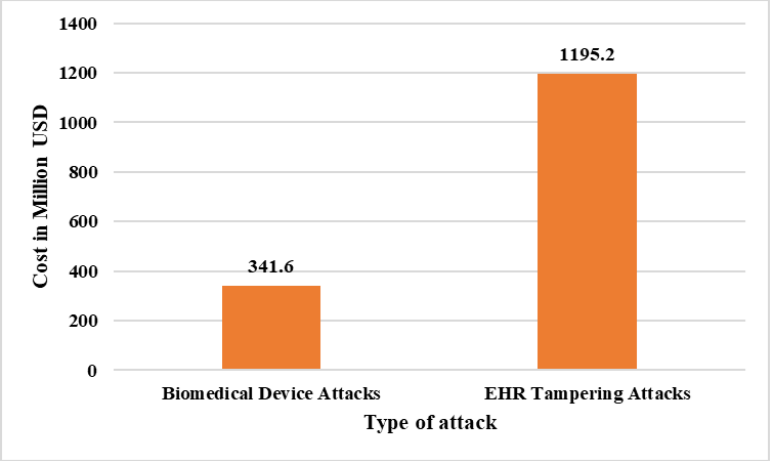

Fig. 5. Financial cost of two types of cyberattacks on the health sector

C. *Patient Safety Impact*

The impact on patient safety due to breaches in biomedical devices and EHRs was categorized into three levels – minimal, moderate, and severe. The percentage of incidents causing these impacts has been tabulated in Table – 3.

TABLE 3. PATIENT SAFETY IMPACT

Impact Level	Biomedical Device Compromises	EHR Tampering
Minimal	15%	32%
Moderate	45%	46%
Severe	40%	22%

The patient safety effects were stronger due to the breaches in the biomedical devices in comparison to the effects due to breaches with EHRs. The negative impacts of the attacks on biomedical devices were severe, since in those cases, 40 percent of the 40 percent of cases ended with equipment failure, wrong dosages of medicines, and even resulting in potentially fatal situations. The negative impacts of EHR tampering, in comparison to breaches in biomedical devices, were less severe, as only 22% of EHR tampering attacks had severe consequences, mostly due to wrong diagnoses brought on by tampered documents and delays in medical processes. Percentage of incidents causing different levels of impact on patient safety are illustrated in the figure 6.

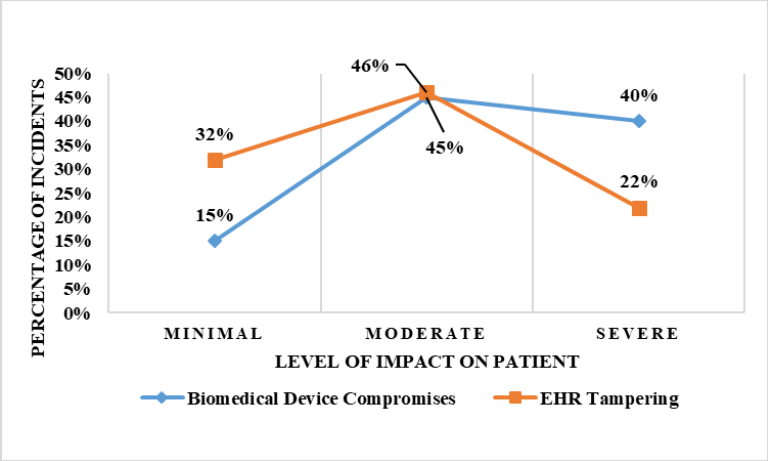

Fig. 6. Percentage of incidents causing different levels of impact on patient safety

Biomedical device compromises are more likely to directly jeopardize patient safety than EHR tampering. A chi-square test was done. It showed a statistically significant difference in patient safety impact between biomedical device compromises and EHR tampering ($p < 0.01$).

D. Recent Impact

The number of incidents during last three years (2022-2024) and number of individuals effected is illustrated in figure 7. Total number of incidents of cyberattack on health sector during 2022-2024 was 852 and total individuals effected were 274275138.

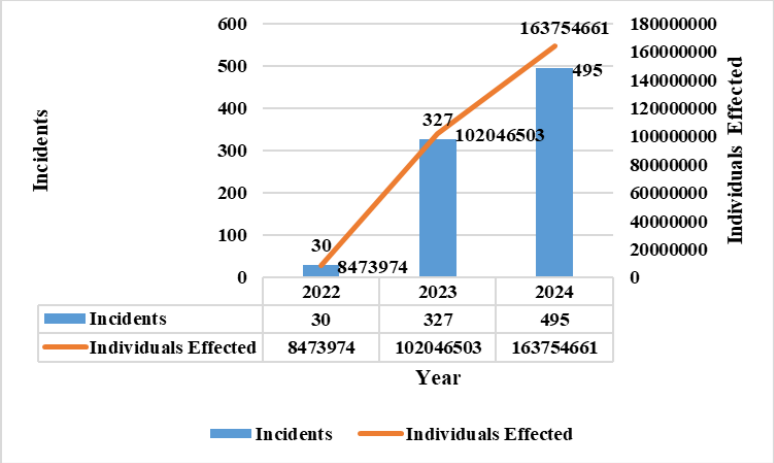

Fig. 7. Recent impact on patient safety

E. Cyberattacks on healthcare sector in India and its impact

Indian healthcare has seen a sharp rise in cybersecurity breach events during the period 2014 to 2024, with ransomware and EHR breaches emerging as the main dangers [17]. India's cybersecurity architecture has been gradually evolving, with significant advancements in data protection. The different types of threats and financial impact in crores INR is shown in Table – 4.

TABLE 4. TYPES OF THREATS AND FINANCIAL IMPACTS IN INDIA

Year	Type of Threat	Financial Impact (Crores INR)
2014	Phishing and Malware	20
2015	Ransomware, phishing, and insider threats	35
2016	Surge in EHR-related data breaches	50
2017	Phishing, ransomware, and insider data theft.	75
2018	Malware attacks on medical devices and phishing schemes.	90
2019	EHR breaches, ransomware, and insider threats	110
2020	Ransomware, phishing, and malware attacks on telemedicine platforms	150
2021	EHR breaches, ransomware, and attacks on IoT-connected biomedical devices	200
2022	Advanced persistent threats (APTs), phishing, and ransomware	180
2023	Cloud data breaches, ransomware, and social engineering targeting healthcare staff.	210
2024	EHR tampering, ransomware, and phishing campaigns	230

There has been a 20% rise in cyber security breach events on average per year over the course of ten years. During this period, there has been a transition from simple phishing assaults to more complex ransomware and advanced persistent threats. By 2024, financial losses had increased yearly to over Rs 1,350 crore.

F. Projected attack during 2024 to 2026

In the coming year, cyber attacks on biomedical devices are expected to grow at 20-30% annually owing to increased interconnectivity and security vulnerabilities. More than 65% of medical IoT in 2024, and gradually decreasing to about 50% by 2026, mainly due to added security measures. Ransom attacks increased by 40% in 2024. Incidents of device tampering will be increased by 70% by 2026, posing critical risks to patient safety and treatment efficacy. Medical service delays due to cyber attacks are increasing annually. By 2026, 78% of the hospitals may be at risk of significant disruptions.

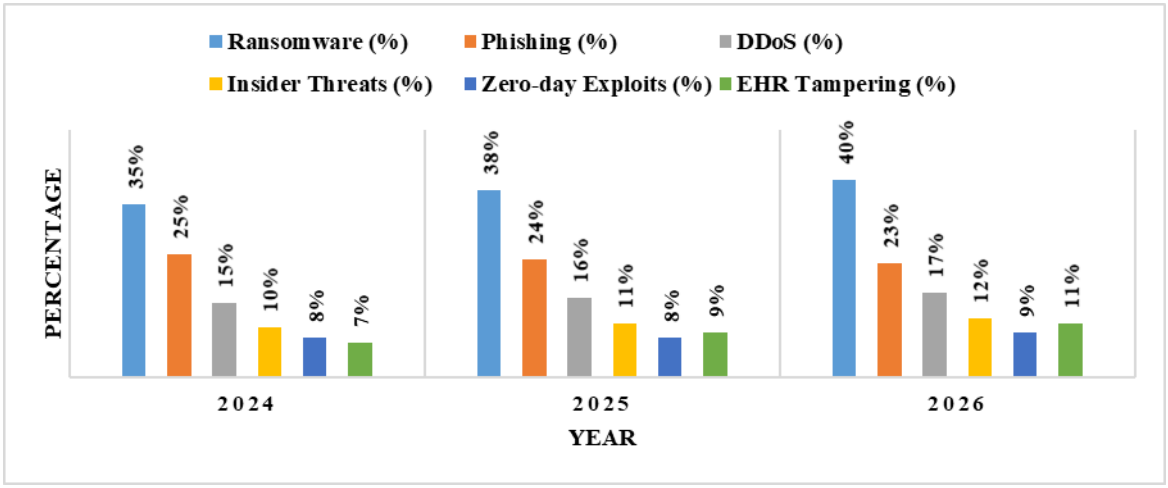

Fig. 8. Global projection of different types of attacks from 2024 to 2026

IV. Discussions

A. *Comparison of risks*

The results of the analysis show a number of significant distinctions between the risks caused due to the EHR tampering and biomedical device compromises.

1. Frequency of attack: EHR tampering happens more often than biomedical device compromises. This is probably because EHR systems tend to have a larger cyberattack surface, and patient data have significant financial value.
2. Financial Impact: EHR tampering leads to increased expenditure for data recovery, and sometimes regulatory fines. Nevertheless, both types of attacks have a significant cost impact on healthcare providers.
3. Patient safety: There is a larger direct danger to patient safety from biomedical device breaches, as many of these occurrences have serious health repercussions. Even though it is still risky, EHR tampering mostly has an indirect impact on patient care through delays and improper handling of medical records.

B. *Implications for healthcare security*

These findings indicate the necessity of unique cybersecurity approaches for EHR systems and biomedical devices. Biomedical devices should focus on maintaining device integrity, conducting regular firmware updates, and maintaining isolation from networks in a way that prevents potentially lethal compromises. For EHR systems, access controls, data backups, and robust encryption should be prioritized by healthcare providers to prevent patient records from being tampered.

V. Conclusion

The work presented and its outcome suggest that, biomedical device compromises have a greater immediate and serious effect on patient safety than EHR tampering, despite EHR tampering is more common and expensive. Healthcare providers need to take a holistic strategy to cybersecurity, taking into account the particular weakness of EHR systems and biomedical devices. Investment in cutting-edge security systems, staff training, and routine audits are essential for reducing the dangers associated with cyberattacks in contemporary healthcare.

VI. REFERENCES

[1] Awad, Atheer, Sarah J. Trenfield, Thomas D. Pollard, Jun Jie Ong, Moe Elbadawi, Laura E. McCoubrey, Alvaro Goyanes, Simon Gaisford, and Abdul W. Basit. "Connected healthcare: Improving patient care using digital health technologies." *Advanced Drug Delivery Reviews* 178 (2021): 113958.

[2] Okolo, Chioma Anthonia, Scholastica Ijeh, Jeremiah Olawumi Arowoogun, Adekunle Oyeyemi Adeniyi, and Olufunke Omotayo. "Reviewing the impact of health information technology on healthcare management efficiency." International Medical Science Research Journal 4, no. 4 (2024): 420-440.

[3] Burke, George, and Neetesh Saxena. "Cyber risks prediction and analysis in medical emergency equipment for situational awareness." Sensors 21, no. 16 (2021): 5325.

[4] Butsch, Carsten. "2.1 Access to Healthcare in the Fragmented Setting of India's Fast Growing Agglomerations–a Case Study of Pune." Resilience and Social Vulnerability (2008): 62.

[5] Lee, EunSu, Yi-Yu Chen, Melanie McDonald, and Erin O'Neill. "Dynamic response systems of healthcare mask production to COVID-19: A case study of Korea." Systems 8, no. 2 (2020): 18.

[6] Pappas, Harry, and Paul Frisch. Leveraging technology as a response to the COVID pandemic: Adapting diverse technologies, workflow, and processes to optimize integrated clinical management. CRC Press, 2022.

[7] Priyadarshini, Ishaani, Raghvendra Kumar, Le Minh Tuan, Le Hoang Son, Hoang Viet Long, Rohit Sharma, and Sakshi Rai. "A new enhanced cyber security framework for medical cyber physical systems." SICS Software-Intensive Cyber-Physical Systems (2021): 1-25.

[8] Priestman, Ward, Tony Anstis, Isabel G. Sebire, Shankar Sridharan, and Neil J. Sebire. "Phishing in healthcare organisations: Threats, mitigation and approaches." BMJ health & care informatics 26, no. 1 (2019).

[9] Wright, Adam, Skye Aaron, and David W. Bates. "The big phish: cyberattacks against US healthcare systems." Journal of General Internal Medicine 31 (2016): 1115-1118.

[10] Gehem, Maarten, Artur Usanov, Erik Frinking, and Michel Rademaker. Assessing cyber security: A meta analysis of threats, trends, and responses to cyber attacks. The Hague Centre for Strategic Studies, 2015.

[11] Gonzalez III, Joaquin Jay, and Roger L. Kemp, eds. Cybersecurity: Current Writings on Threats and Protection. McFarland, 2019.

[12] Jensen, Peter B., Lars J. Jensen, and Søren Brunak. "Mining electronic health records: towards better research applications and clinical care." Nature Reviews Genetics 13, no. 6 (2012): 395-405.

[13] IBM (2024) Cost of a Data Breach 2024. In: IBM. https://www.ibm.com/reports/data-breach

[14] Verizon (2024) 2024 Data Breach Investigations Report. In: Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[15] Higgins M (2003) Symantec Internet Security Threat Report

[16] U.S. Department of Health & Human Services (2024) U.S. Department of Health & Human Services - Office for Civil Rights. In: Hhs.gov. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[17] George, A. Shaji, T. Baskar, and P. Balaji Srikaanth. "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors." Partners Universal International Innovation Journal 2, no. 1 (2024): 51-75.