SSN Journal of Management and Technology Research Communications Vol 1 No (1) May-June-July 2024
Online ISSN: 3049-0014

Healthcare Cybersecurity: A Mini Review on Recent Incidents and Preventive Strategies

Maseera Khan,[1] Ranveer Kumar[2] and Jasim Khan[2*]

[1]Jefferson County, Birmingham, Alabama, United States, 35205

[2]The University of Alabama at Birmingham, Birmingham, Alabama, United States of America, 35233

ABSTRACT

Healthcare organizations are fast becoming a prime target of cyberattacks, that threat the sanctity and accessibility to patient data, medical histories, personal details as well financial information. The impact of cyberattacks in healthcare are wide-ranging from ransomware attacks, phishing attack and data breaches. These attacks lead to severe disruption not only to organizations but to patients and stakeholders such as data losses, financial costs, operational disruption, reputational damage. Furthermore, healthcare organizations face the extra challenge of complying with strict regulatory requirements. Healthcare organizations are particularly prone to cyberattacks due to the sensitive nature of data, often outdated IT systems which can attract cybercriminals seeking financial gain or exploit personal information. To prevent cyberattacks, organizations require a multifaceted approach, updating and patching outdated systems to eliminate vulnerabilities. Using data encryption, intrusion detection systems to help protect sensitive data, Regular audit and penetration testing, zero trust architecture (ZTA), employee training and awareness, advanced threat and detection, ensures that the organization can quickly address and mitigate the impact of a cyber incident. Adopting proactive measures and organizing regular audits can help identifying and addressing possible weakness in system and thus healthcare organizations can protect their data and ensure the integrity and trust of their patients.

KEY WORDS: HEALTHCARE, CYBERATTACKS, VULNERABILITIES, RANSOMWARE, DATA BREACHES.

INTRODUCTION

The prevalence and adaption of digital infrastructure in the last few decades gave rise to numerous advanced innovations to the current technology-friendly society. Several cutting-edge inventions with the application of digitalization provided strong and supportive environment for information technology in daily life of human beings.[1] These advancements resulted in the greater improvements in education, communication, workforce productivity, community welfare, industrialization, environmental protection, banking, biomedical research and healthcare.[2]

With all the benefits from these technological advancements, there are few inseparable vulnerabilities which follows digitalization due to generation and exchange of tremendous amount of data from the regular functionality[3]. Organizations have their growth and productivity data available to be accessed to public, but some data are not meant to be freely available and required to be protected from getting into hands of bad actors. [4,5] Technological transformation of healthcare, enhanced efficiency and patient care which accompanied by several vulnerabilities that cybercriminals can exploit [5,6].

Healthcare is one of the prime targets of these cybercriminals as it is a critical part of societal infrastructure involving tremendous amount of sensitive healthcare and financial data involving patients and payment system [6,7]. As per the recent report, cyberattacks against American healthcare system rose 177% in 2023 These incidents negatively affect patient care, healthcare emergency services and financial services involved. These cybercriminals usually ask for huge amount of money in exchange of returning stolen data or service halted by their cyber-attack. [8,9].

Article Information: *Corresponding Author: jkhan@uabmc.edu
Received 29/05/2024 Accepted after revision 19/07/2024
Publication Date: 31st July 2024 Page Number- 12- 19

Available at: https://mntrc.in/
DOI: http://dx.doi.org/10.21786/mntrc/1.1.3

The data breach can impact beyond the patient's privacy and can affect patients' safety by altering the shared networks and devices connected to it. Any cybersecurity flaw in the connected device can cause serious harm to the patients taking services from that device [6,7,8]. The cyber breaches cause elevated financial burden for the industry, which already involves low monetary profits and high expenditures compared to other industries. At present, risk and cost of data breach or loss is much higher for healthcare organization compared to organizations in other sectors.[10,11]

It is estimated that data breaches will cost $10.5 trillion annually by 2025 compared to $3 trillion in 2015.[12] This review will delve into the recent healthcare related cyberattacks, challenges faced by the healthcare sector, and discuss the necessary and robust preventive security measures against the future cyber incidents.

Healthcare

An ever-vulnerable target of cybercriminals? Till last decade, people believed that there are negligible chances of any attack on healthcare system and patient data which led to the loose protective measures to save the system and related data. There was no concept of cybersecurity till 2014, when Boston Children's Hospital was attacked by anonymous entity with distributed denial-of-service (DDoS) attacks. [13, 14] In later years, 2015 and 2016, there were few more similar notable healthcare organizations targeted cyber-attacks done by threat actors.

This led to their unrestricted access to protected health information (PHI) in exchange with the ransom demands.[15, 16] Nowadays, healthcare targeted attacks occur more frequently than before and must be tackled with efficient preparedness in cyber threat landscape Table 1.[17] There are several factors involved in the complex architecture and vulnerabilities in healthcare cybersecurity. Some of them are:

Hardware vulnerabilities in medical devices can become as major shortcoming of cybersecurity system and attackers can exploit these vulnerabilities. To counter these vulnerabilities, advanced and dependable Cyber Physical System (CPS) is required to prevent the shared hardware of the organization,[22]. Studies have suggested regular update of device access passwords, updated firewalls and limiting access to unsecured networks. [21,23]

Impact of healthcare cyberattacks

Healthcare cyberattacks have wide-ranging consequences, which has severe impact on patient care, data security, financial stability, and overall healthcare facilities. These incidents put more risks to the people involved with the targeted organization causing crucial harm. Here is a detailed analysis of these impacts.

Patient Safety Risks

Patient safety is threatened by cyberattacks on healthcare system. Loosing access to medical health records, medical device and all other critical operators which can lead to serious effects on patient health and lives. This causes delayed medical care to the patients in need of emergency care and continuous medical assistance through the respective hospital system for survival. In recent cyberattack to the accension hospital system, clinicians had to revert to paper-based patient care raising the events of delayed medical services to the needy. [32,37]

Data Breaches

Data breaches in healthcare organizations are widely observed because they contain enormous amount of personal sensitive information of patients, including their health record, medical histories, financial information. The PHI are most likely to be breached and used for identity theft, privacy violations, and many more [(38)]. This type of cyberattacks creates following issues:

Financial burden

Cyberattacks in healthcare organizations causes huge impact in financial cost. Financial breach can cause disclosure of financial information resulting in ransomware attacks, Phishing scams, which further impacts financial cost including remediation costs, legal and regulatory penalties, investigation costs, Ransomware payments. Financial data breach in healthcare organization can be severe effecting organizations, patients, employees, stakeholders.[38,39]

Operational Disruption

Cyberattacks can cause significant operational disruptions resulting in device malfunctions, patient appointment cancellation and delays, system outages, delays in diagnosis and treatment. Failure to maintain robust data integrity and security or patient data breaches can lead to fines and legal consequences [(40)]. Scripps health Cyberattack caused shutdown of electronics system for weeks, resulting in compromised patient care. This caused long term detrimental effect on overall healthcare of the organization affecting larger population receiving the medical services. [(31, 32)]

Reputational Damage

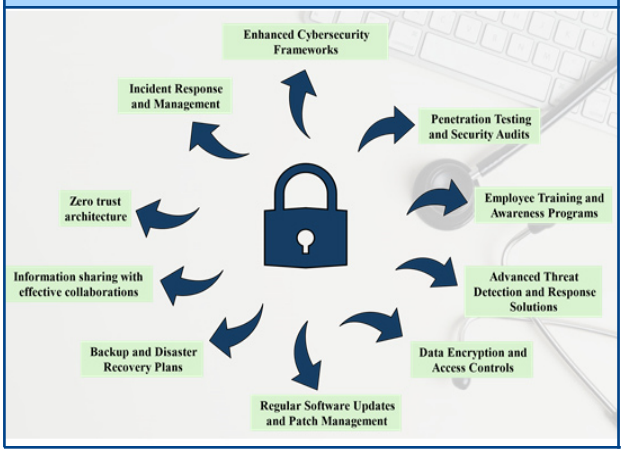
Impacts of healthcare cyberattacks can be severe in terms of reputational damage because of the broken trust of the patient, leading to loss of patient trust in healthcare providers. Confidentiality concerns, facing rejection to collaborate with third party organization, media coverage, fear of misusing of data [(31, 41, 42)]. Attacks and breaches which faces media backlashes resulting in negative comments, damaging the organization's reputation [(42)]. For example, Anthem Inc. Healthcare attack in 2015, caused major set-back to the organization's reputation and patient confidence. [(43)]

Table:1 Healthcare cyberattack incidents occurred in recent years.

S.No.	Attack Name	Location	Impact
1	Black Basta Ransomware Attack 2024	United States	A major US healthcare network with over 100 hospitals and 50 senior living facilities was hit by a ransomware attack. This disrupted electronic health records, phone systems, and ordering processes for tests, procedures, and medications, leading to ambulance diversions and operational disruptions[24].
2	Change Healthcare Cyberattack 2024	United States	This attack disrupted the payment processing systems critical for handling Medicare, Medicaid, and commercial health plan claims. It led to delays in payments and operational difficulties across many healthcare providers.[(25)].
3	Norton Healthcare Data Breach 2023	United States	Norton Healthcare has suffered a data breach impacting an It is estimated that around 2.5 million people were impacted by data breach from Norton Healthcare based in Kentucky, United States. They reported that, Cybercriminals got unauthorized access to personal information of patients and many employees[(26)].
4	UK's National Health Service (NHS) 2023	United Kingdom	The NHS faced multiple cyberattacks in 2023, one of which caused significant disruptions in healthcare services, including delays in surgeries and appointments. A specific attack led to the compromise of the data of thousands of patients[(27)].
5	Australian Health Provider Medibank 2022	Australia	Personal data of 9.7 million current and former customers was stolen, including sensitive health records. The attackers leaked the data online after a ransom demand was not met[(28)].
6	AIIMS Ransomware Attack 2022	India	Hackers targeted systems of one the biggest and famous hospital, All India Institute of Medical Sciences (AIIMS) and allegedly demanded ransome of around Rs 200 crore in cryptocurrency[(29)].
7	Morley Companies 2022	United States	Ransomware attack on Morley Companies, a third-party provider of medical services. This caused, exposure of over 521,000 individual records to cybercriminals [(30)].
8	Scripps Health 2021	United States	A ransomware attack caused significant disruptions to the hospital's IT systems, impacting patient care and forcing the diversion of critical care patients. Personal data of around 147,000 patients were compromised [(31, 32)]
9	Ireland's Health Service Executive (HSE) 2021	Ireland	The HSE was hit by a ransomware attack that caused widespread disruption across its network. The attack led to the shutdown of IT systems, affecting patient care and administration across the country. Personal data and medical records of patients were also compromised [(33)].

10	Finnish Vastaamo Psychotherapy Center 2020	Finland	Sensitive patient records were stolen and used for extortion. Attackers demanded ransom from both the clinic and individual patients, threatening to publish their private therapy session notes online.[34]
11	French Hospital System AP-HP 2020	France	AP-HP, which is part of the Assistance Publique–Hôpitaux de Paris, faced a cyberattack that targeted its administrative systems. The attack disrupted operations and threatened patient data [(35)].
12	University Hospital Düsseldorf 2020	Germany	A ransomware attack led to IT systems being shut down, and a patient seeking emergency treatment was redirected to another hospital, resulting in delayed care. The incident raised significant concerns about the impact of cyberattacks on patient safety[(36)]

Figure 1: Graphical representation of preventive cybersecurity in healthcare.



Potential solutions to prevent future cyberattacks

There are various types of impact which is caused by cyberattacks on healthcare organization and it is important to implement robust cybersecurity measures to prevent any possible future incidents. Here are some possible solutions (Figure 1):

Enhanced Cybersecurity Frameworks

Enhanced cybersecurity frameworks play an essential role for protecting healthcare organizations. These frameworks should incorporate risk management, network security measures, incident response, threat detection and robust endpoint protection.[15,44]. Frameworks like NIST Cybersecurity Framework provides a guideline for managing and reducing cybersecurity risks. By implementing these frameworks, healthcare organization can upgrade their cybersecurity prevention methods, give better protection to organization, and ensure compliance with regulations [(45, 46)].

Penetration Testing and Security Audits

Cyberattacks in healthcare can be avoided by regularly checking for security audits and penetration testing ensuring regulatory standards, identifying and mitigating risks and improving overall efficiency [(47)]. Proactively involving simulated cyberattacks against organizations system can be helpful to identify any weakness that could be exploited by malicious actors and to strengthen system defenses. Continuous improvement by regular audits, employee training can protect sensitive patient data and maintain trust with patients and stakeholders [(17)].

Employee Training and Awareness Programs

Employee training and awareness programs plays a crucial role to protect and maintain data security [(48)]. Human errors can be mitigated by training healthcare workers on recognizing phishing attempts, secure data practices to properly handle, store and transmit patient data, password management, incident response and report, compliance with regulations, by implementing training programs can help improving security posture and can significantly reduce the risk of potential cyber-attacks. [(38, 46, 48)]

Advanced Threat Detection and Response Solutions

Advance threat detection and response solutions are vitally important for healthcare organizations to help recognize and address to potential threats and vulnerabilities [(49)]. These solutions can be implemented by using tools like Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA) and many more which can help monitor alerts in real time to detect any suspicious activities and threats.

Integrating threat intelligence platforms can help to stay updated on emerging threats (50, 51). By combining Artificial Intelligence (AI) and Machine Learning (ML) with these tools can help achieve a robust security posture. [(52, 53)]

Data Encryption and Access Controls

Protecting sensitive data from cyber-attacks is crucial in healthcare; by implementing encryption not only it will protect from unauthorized access but remains keeps the data confidential and secure both at rest and in transit. [6, 45] Furthermore, using security measures such as access control can help ensuring data protection, reducing risks of data breaches and helps meet regulatory requirements [7, 22]. They ensure only authorized users have access to sensitive information. Strategies like Multi Factor Authorization (MFA), least privilege principle, audit and monitoring can be used for reducing the risks of internal threats, prevents unauthorized access. [54]

Regular Software Updates and Patch Management

Regular software updates and patch management plays significant role ensuring the systems are up to date maintaining the security, enhancing security by addressing vulnerabilities, maintaining compliance, and saving costs associated with security incidents [55]. Risk of human error and to streamline the deployment process automated patch management tools can be used. Implementing robust patch management policies, prioritizing critical patches, training IT staff on patch management practices can help in reducing risk of cyberthreats [38, 47].

Backup and Disaster Recovery Plans

Backup and disaster recovery plans can help organization to protection of sensitive data from data loss or system failure. It protects critical information of patients from being compromised, ensuring healthcare service can continue with minimal interruption of any event [38]. Strategizing data backup and data recovery plans with regularly testing and software updating can help in reflecting changes in the IT environment and emerging threats [56]. Also, using automated backup process and utilizing cloud services can help in providing consistency, cost-efficiency and remote access, making them a cornerstone of a strong cybersecurity strategy in healthcare. [57]

Information sharing with effective collaborations

Healthcare organizations are required to maintain strong collaborations with cybersecurity experts, and government agencies for efficient protection from potential cyberthreats from the cybercriminals [7]. All the information from the recent threats and appropriate best practices should be shared between the collaborative agencies [58]. This will enable the healthcare organization stay prepared and ahead of cybercriminals strengthening the overall cyber defense. Information-sharing and analysis centers (ISACs) and industry consortiums provide the robust and effective collaborative platform for strong cyber defense for healthcare organizations [59].

Zero trust architecture

Zero Trust Architecture (ZTA) is a security model that works on principle “Zero trust”, meaning that no user or device can be trusted. Zero trust assumes that threat could be exists in outside or outside of the network [60]. By implementing this approach, the user or devices are granted least privileges or minimum access necessary for user to perform tasks which limits potential entry points for attackers reducing risks of cyberattacks [61]. Ensuring end point security, continuous monitoring can help healthcare organization to improved data protection and operational efficiency. ZTA offers robust strategies for better or enhanced security protection. [60, 61].

Incident Response and Management

Incident Response and management are vital for handling, detecting and responding cybers attacks in healthcare. Incident management can minimize impact by reducing potential damage and operational disruption [62]. By using monitoring tools like SIEM can be helping to stay informed about emerging threats and by implementing mitigation strategies threat damage can be minimized ensuring removal of threats from system [63]. Conducting regular assessments, audits, penetration testing can help organization to prevent future incidents. [44, 63]

Recommendations

Early and unified adaption of cybersecurity in healthcare organizations is of utmost importance / These organizations are guardians of sensitive PHI data, innovative clinical research and financial information. This data is considered confidential. Implementing robust cybersecurity measures can safeguard this sensitive data from data breaches which can ultimately protects from legal outcomes and financial loss. Strict regulatory standards should be implemented, and every employee should be trained to oblige to follow them through necessary certifications and regular audits.

Security compliances should be obliged to be updated as per the recent cyberthreat environment which requires considerable investments at regular intervals in cybersecurity compliance. Robust and well-informed cybersecurity environment following the advanced security measures in the healthcare organization by increasing regular employee awareness by workshops on phishing attacks, malicious contents, their implications and promoting the well-informed responsible approach for supporting healthcare organizations can prevent the future operational disruptions in healthcare delivery and possible financial loss.

CONCLUSION

Cybersecurity in healthcare is critical and must have component in the organizational framework to maintain patient trust, prevent data breaches, operational disruptions, and financial loss. This required utilizing latest technologies and promoting awareness in the respective organization. Failure comply with these necessities by

healthcare organization can lead to serious damage to critical and essential resources leading to unprecedented harm to its stakeholders. This can be made possible by regular security audits, addressing regulatory compliance. Another crucial measure for effective healthcare cybersecurity is promoting regular and well-informed awareness on possible cyberthreats through workshops, seminars and trainings for beneficiaries and employees which can harness the robust cybersecurity infrastructure.

Author contribution

MK and JK conceptualized have written the manuscript, MK, RK and JK edited the final version of manuscript.

Conflict of interest declaration statement

Authors declare no conflicts of interest in this manuscript

Ethical declaration statement

No animal or human data is used in this manuscript.

REFERENCES

1. Statista. Adoption rate of emerging technologies in organizations worldwide in 2023 2024 [updated 03/19/2024. Available from: https://www.statista.com/statistics/661164/worldwide-cio-survey-operational-priorities/.
2. Alotaibi YK, Federico F. The impact of health information technology on patient safety. Saudi Med J. 2017;38(12):1173-80.
3. Mesko B, Drobni Z, Benyei E, Gergely B, Gyorffy Z. Digital health is a cultural transformation of traditional healthcare. Mhealth. 2017;3:38.
4. Cobb C, Sudar S, Reiter N, Anderson R, Roesner F, Kohno T. Computer security for data collection technologies. Dev Eng. 2018;3:1-11.
5. Vinuesa R, Azizpour H, Leite I, Balaam M, Dignum V, Domisch S, et al. The role of artificial intelligence in achieving the Sustainable Development Goals. Nat Commun. 2020;11(1):233.
6. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. J Med Internet Res. 2021;23(4):e21747.
7. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018;20(5):e10059.
8. Staff S. Healthcare and finance were prominent cyberattack targets in 2023: Security; 2024 [updated 05/29/2024. Available from: https://www.securitymagazine.com/articles/100709-healthcare-and-finance-were-prominent-cyberattack-targets-in-2023
9. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 2022;34(10):8176-206.
10. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736.
11. Perakslis ED. Cybersecurity in health care. N Engl J Med. 2014;371(5):395-7.
12. Morgan S. Cybercrime To Cost The World $10.5 Trillion Annually By 2025: Cybercrime Magazine; 2020 [Available from: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
13. Adil M, Khan MK. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. Sustain Cities Soc. 2021;75:103311.
14. Raths D. Six Lessons From Boston Children's 'Hacktivist' Attack: Healthcae Innovation; 2018 [Available from: https://www.hcinnovationgroup.com/cybersecurity/article/13030808/six-lessons-from-boston-childrens-hacktivist-attack.
15. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput. 2023;37(5):1123-32.
16. Bughio KS, Cook DM, Shah SAA. Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring. Sensors (Basel). 2024;24(9).
17. Muhammad Fakhrul Safitra ML, Hanif Fakhrurroja. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability. 2023;15(18) (13369).
18. Kotz D, Gunter CA, Kumar S, Weiner JP. Privacy and Security in Mobile Health: A Research Agenda. Computer (Long Beach Calif). 2016;49(6):22-30.
19. A. J. Burns MEJ, Peter Honeyman. A brief chronology of medical device security. Communications of the ACM. 2016;59(10):66 - 72.
20. Keman Huang XW, William Wei, and Stuart Madnick. The Devastating Business Impacts of a Cyber Breach: Harvard Business Review 2023 [Available from: https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.
21. Qwerx. Cybersecurity [Internet]2023. Available from: https://www.qwerx.co/blog/medical-device-cybersecurity#:~:text=An%20analysis%20of%20more%20than,their%20attacks%20against%20healthcare%20institutions.
22. Parihar A PJ, Prajapati BG, Trambadiya B, Thakkar A, Engineer P,. Role of IOT in healthcare: Applications, security & privacy concerns. Intelligent Pharmacy. 2024.

23. Karthikeyan Lingasubramanian RK, Nagendra Babu Gunti, Thomas Morris. Study of Hardware Trojans Based Security Vulnerabilities in Cyber Physical Systems 2018 IEEE International Conference on Consumer Electronics (ICCE); 03/29/2018; Las Vegas, Nevada, United States2018.
24. Lyngaas S. Cyberattack disrupts operations at major US health care network: CNN Business; 2024 [08/05/2024]. Available from: https://www.cnn.com/2024/05/08/tech/cyberattack-disrupts-healthcare-network/index.html.
25. Alder S. Change Healthcare Reports Ransomware Data Breach to HHS: The HIPAA Journal; 2024 [cited 2024. Available from: https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.
26. Kapko M. Norton Healthcare ransomware attack exposes 2.5M people: Cybersecurity Drive; 2023 [Available from: https://www.cybersecuritydive.com/news/norton-healthcare-ransomware-attack/702140/.
27. Davies G. A year on from the NHS Ransomware Attack: AIRBUS; 2023 [Available from: https://www.protect.airbus.com/blog/a-year-on-from-the-nhs-ransomware-attack/.
28. Reuters. Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom: Reuters; 2022 [Available from: https://www.reuters.com/business/healthcare-pharmaceuticals/medibank-says-hacker-accessed-data-97-mln-customers-refuses-pay-ransom-2022-11-06/.
29. ETCISO. AIIMS ransomware attack: what it means for health data privacy: Economic Times; 2022 [Available from: https://ciso.economictimes.indiatimes.com/news/aiims-ransomware-attack-what-it-means-for-health-data-privacy/96538957.
30. Alder S. PHI of 521,000 Individuals Compromised in Security Breach at Morley Companies: The HIPAA Journal; 2022 [Available from: https://www.hipaajournal.com/phi-of-521000-individuals-compromised-in-security-breach-at-morley-companies/.
31. Dameff C, Tully J, Chan TC, Castillo EM, Savage S, Maysent P, et al. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA Netw Open. 2023;6(5):e2312270.
32. Abbou B, Kessel B, Ben Natan M, Gabbay-Benziv R, Dahan Shriki D, Ophir A, et al. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Digit Health. 2024;6:1321485.
33. Harvey H, Carroll H, Murphy V, Ballot J, O'Grady M, O'Hare D, et al. The Impact of a National Cyberattack Affecting Clinical Trials: The Cancer Trials Ireland Experience. JCO Clin Cancer Inform. 2023;7:e2200149.
34. Inkster B, Knibbs C, Bada M. Cybersecurity: a critical priority for digital mental health. Front Digit Health. 2023;5:1242264.
35. Fouquet H. Paris Hospitals Target of Failed Cyber-Attack, Authority Says: Bloomberg; 2020 [Available from: https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says?embedded-checkout=true.
36. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873.
37. Keogh RJ, Harvey H, Brady C, Hassett E, Costelloe SJ, O'Sullivan MJ, et al. Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center. J Cancer Policy. 2024;39:100466.
38. Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspect Health Inf Manag. 2022;19(Spring):1i.
39. Eddy N. Healthcare cyberattacks are costing an average of $11 million per breach 2024 [Available from: https://www.healthcarefinancenews.com/news/healthcare-cyberattacks-are-costing-average-11-million-breach.
40. Mohd Javaida AH, Ravi Pratap Singhb, Rajiv Suman. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023;1(100016).
41. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors (Basel). 2021;21(15).
42. Alanazi AT. Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. Cureus. 2023;15(10):e47026.
43. Choi SJ, Johnson ME. The relationship between cybersecurity ratings and the risk of hospital data breaches. J Am Med Inform Assoc. 2021;28(10):2085-92.
44. Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. Healthc Manage Forum. 2024;37(1):17-20.
45. Luidold C, Jungbauer C. Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. Front Med (Lausanne). 2024;11:1379852.
46. Argyridou E, Nifakos S, Laoudias C, Panda S, Panaousis E, Chandramouli K, et al. Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. J Med Internet Res. 2023;25:e41294.
47. Mehrtak M, SeyedAlinaghi S, MohsseniPour M, Noori T, Karimi A, Shamsabadi A, et al. Security challenges and solutions using healthcare cloud computing. J Med Life. 2021;14(4):448-61.
48. Alhuwail D, Al-Jafar E, Abdulsalam Y, AlDuaij S. Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. Appl

Clin Inform. 2021;12(4):924-32.
49. Koppelman L. Next. 2024. [cited 2024]. Available from: https://www.nextdlp.com/resources/blog/cybersecurity-predictions-for-2024.
50. Eastwood B. How SIEM Tools Fit into a Healthcare Organization's Security Strategy: HealthTech; 2024 [Available from: https://healthtechmagazine.net/article/2024/02/how-siem-tools-fit-healthcare-organizations-security-strategy.
51. Cynet. Endpoint Detection and Response (EDR) in Healthcare 2023 [Available from: https://www.cynet.com/endpoint-protection-and-edr/edr-in-healthcare/.
52. Federation IH. Artificial intelligence and cybersecurity in healthcare (YEL2023): International Hospital Federation; 2023 [08/05/2024]. Available from: https://ihf-fih.org/news-insights/artificial-intelligence-and-cybersecurity-in-healthcare/.
53. Hale C. Impact of Artificial Intelligence on Healthcare Cybersecurity: Linkedin; 2023 [Available from: https://www.linkedin.com/pulse/impact-artificial-intelligence-healthcare-charles-hale/.
54. Suleski T, Ahmed M, Yang W, Wang E. A review of multi-factor authentication in the Internet of Healthcare Things. Digit Health. 2023;9:20552076231177144.
55. Jabin MSR. Operational disruption in healthcare associated with software functionality issue due to software security patching: a case report. Front Digit Health. 2024;6:1367431.
56. Agrawal V, Agrawal S, Bomanwar A, Dubey T, Jaiswal A. Exploring the Risks, Benefits, Advances, and Challenges in Internet Integration in Medicine With the Advent of 5G Technology: A Comprehensive Review. Cureus. 2023;15(11):e48767.
57. Sachdeva S, Bhatia S, Al Harrasi A, Shah YA, Anwer K, Philip AK, et al. Unraveling the role of cloud computing in health care system and biomedical sciences. Heliyon. 2024;10(7):e29044.
58. Iftikhar S. Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Comput Sci. 2024;10:e1772.
59. Jerry-Egemba N. Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. Healthc Manage Forum. 2024;37(1):21-5.
60. Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, et al. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors (Basel). 2024;24(4).
61. Chunwen Liu RT, Yang Wu, Yun Feng, Ze Jin, Fangjiao Zhang, Yuling Liu, Qixu Liu. Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity. 2024;7.
62. Jalali MS, Russell B, Razak S, Gordon WJ. EARS to cyber incidents in health care. J Am Med Inform Assoc. 2019;26(1):81-90.
63. Gonzalez-Granadillo G, Gonzalez-Zarzosa S, Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel). 2021;21(14).