Cybersecurity and Innovative Technology Journal, Vol.2, No.1, 2024, pp. 41-52
e-ISSN 3025-6682. DOI. 10.52889/citj.v2i1.333

Exploring and Mitigating Cybersecurity Challenges in Electronic Health Records

Submitted 15 December 2023, Revised 18 February 2024, Accepted 18 February 2024

William J. Triplett[1,2]*

[1]Department of Information Systems, Health Information Technology,
University of Maryland, Baltimore County, Baltimore, United States

[2]Department of Healthcare Technology, Cybersecurity Leadership,
Capitol Technology University, Laurel, United States

Corresponding Email: *wtriple1@umbc.edu

Abstract

This study explores the complexities of cybersecurity challenges in electronic health record (EHR) systems and provides comprehensive solutions to enhance security. Furthermore, it analyzes existing research on EHR cybersecurity, considers relevant frameworks, and presents a well-designed research approach. Extensive research has examined the cybersecurity landscape of electronic health records (EHRs). Furthermore, it identifies the inherent flaws, challenges, and threats prevalent in existing systems and firmly emphasizes the need for robust security solutions to safeguard sensitive patient information. This study highlights the significance of addressing EHR cybersecurity concerns, enhancing existing knowledge on vulnerabilities, and providing a comprehensive understanding of this field. The study emphasizes the need for proactive and multifaceted security measures that can adapt to the ever-evolving landscape of cyber threats. Future research must continue to explore innovative tools and methodologies to safeguard EHRs against the increasing complexity and sophistication of cyber threats.

Keywords: Cybersecurity, Digital, Electronic Health Records, Encryption, Security Breaches

INTRODUCTION

In the ever-evolving digital age, the healthcare industry is moving swiftly away from traditional paper-based systems and electronic health records (EHRs). This transition is promising because it improves healthcare delivery and accessibility. However, this poses significant cybersecurity threats and challenges. This study emphasizes the urgent need for robust cybersecurity measures to protect sensitive patient data, mitigate potential breaches, and ensure compliance with various health information privacy laws. Furthermore, it explores the cybersecurity challenges related to EHRs and identifies potential resolutions, scrutinizes the existing EHR security measures, analyzes breaches and their impacts, and develops actionable solutions to establish secure EHR systems. According to Keshta (2021), electronic medical records (EMRs) can provide many benefits to physicians, patients, and healthcare services if they are adopted by healthcare organizations." Despite incentives and the need for EHR transition, there is a lack of established best practices for this process and few studies on this topic (Huang et al., 2020). Previous research has extensively explored the cybersecurity challenges associated with electronic health records (EHRs). Some studies, such as Coventry and Branley (2018), have focused on the vulnerabilities and risks faced by healthcare institutions owing to the shift towards digital medical records.

The research field primarily focuses on assessing the prevalent cybersecurity vulnerabilities in EHRs and developing countermeasures. However, ever-advancing hacking techniques require ongoing research. Coventry and Branley (2018) argue that "while healthcare technologies are crucial to our population's health, they are vulnerable to security threats owing to interconnected, easily accessible access points, outdated systems, and a lack of emphasis on cybersecurity." Sendelj and Ognjanovic (2022) emphasized the importance of usability and internationalization in information technology, highlighting the need to address challenges specific to EHRs. Ghafur et al. (2019) highlighted that as modern technology becomes indispensable in health care, vulnerabilities to cyber threats continue to increase, compromising many people's health information and safety". EHRs have transformed how medical information is managed and have significantly improved patient care. By digitizing comprehensive medical histories, they enhanced the efficiency and accuracy of healthcare delivery. Although EHRs offer numerous benefits, they introduce vulnerabilities to cybersecurity threats. Sendelj and Ognjanovic (2022) discuss a practical approach to healthcare information system management and the significance of cybersecurity in safeguarding patient data. Understanding these challenges is crucial to ensuring the confidentiality and trustworthiness of healthcare institutions.

The use of electronic health records (EHRs) has transformed the healthcare industry. Digital platforms have revolutionized the storage, management, and sharing of patient health information. By granting healthcare providers easy access to critical patient data, EHRs promote continuity of care and enhance clinical decision-making. In addition, they streamlined their administrative processes, leading to improved patient outcomes and more efficient healthcare delivery. The widespread implementation of EHRs can be attributed to government initiatives, regulations, and incentives promoting their adoption. Considering the increasing reliance of the healthcare industry on digital systems, the significance of EHR cybersecurity must not be overstated. EHRs contain various personal health information, including medical history, diagnoses, treatments, and insurance details. These data have become an enticing target for cybercriminals seeking financial gain or aiming to perform malicious activities. EHR cybersecurity strives to protect patient privacy, uphold data integrity, and prevent unauthorized access, disclosure, and modification of health information (Burke et al., 2019). EHR cybersecurity faces various challenges that jeopardize the confidentiality, integrity, and availability of patient data. These challenges include sophisticated external attacks, such as hacking, ransomware, and phishing schemes, and internal threats, such as insider breaches, human errors, and inadequate access controls. Furthermore, the increasing interconnectedness

between medical devices and EHR systems introduces additional vulnerabilities and potential entry points for cybercriminals (Luh and Yen, 2020). EHR cybersecurity has witnessed growing research activity, resulting in prominent studies examining different aspects of this field. These studies discuss vulnerability assessments, security frameworks, encryption techniques, access controls, and incident response strategies. They offer valuable insights into the current state of EHR security, identify gaps in existing approaches, and propose innovative solutions to enhance EHR cybersecurity (Alharam and El-Madany, 2018). Controversies and opposing opinions exist in the research community and industry about EHR cybersecurity, such as the effectiveness of regulatory controls in mitigating cybersecurity risk. Some argue that stringent regulatory controls and compliance frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA), can effectively address cybersecurity vulnerabilities in EHR systems. However, others argue that regulations are crucial and must be complemented by comprehensive security measures and employee training to counter human elements and potential insider threats (Thompson, 2020).

Cuenca and Capstone (2017) emphasized the importance of usability and internationalization in information technology, highlighting the need to address challenges specific to EHRs. Chen, Lambright, and Abdelwahed (2016) discussed a practical approach to healthcare information system management and the significance of cybersecurity in safeguarding patient data. Despite the extensive body of literature on EHR cybersecurity challenges, there remains a research gap in understanding the holistic impact of breaches and evaluating the effectiveness of security measures.

Several theories and frameworks can be applied to analyze EHR cybersecurity challenges. McDermott, Kamerer, and Birk (2019) discussed the application of data analytics and artificial intelligence in managing health informatics data, highlighting the potential for enhancing EHR security. Additionally, cyber risk assessment frameworks such as those discussed by Kandasamy et al. (2020) can help identify vulnerabilities in EHR systems and develop strategies to mitigate cybersecurity threats. By examining these theories and frameworks, this study aims to highlight the complexities of EHR cybersecurity.

METHOD

In this study, a comprehensive multilevel approach was employed. First, it thoroughly evaluates the existing literature on electronic health record (EHR) cybersecurity, resulting in an original investigation and the development of fresh methodologies. The materials used in this study included peer-reviewed academic articles, existing databases of recorded EHR breaches, cybersecurity guidelines and standards, and specific EHR systems for scrutiny and testing.

Furthermore, academic databases, such as JSTOR and PubMed's existing databases of recorded EHR breaches, the Department of Health and Human Services' HIPAA breach database cybersecurity guidelines, and the NIST Cybersecurity Framework for EHR software systems, were used for pilot testing and analyzing security features. The primary methodology involved a thorough analysis of the diverse literature. Next, it included an examination of recorded breaches, an analysis of selected EHR systems, and the creation of novel protocols and methodologies. A step-by-step description of the experimental procedures: A literature review to understand the current landscape of EHR cybersecurity analysis of actual EHR breaches for the identification of prevalent vulnerabilities, security feature assessment of selected EHR systems to evaluate their effectiveness, and the development of a new methodology or security protocol based on identified threats and vulnerabilities. This study established a novel methodology for auditing EHR systems, which includes technology infrastructure, human factors, and third-party management. Therefore, this offers a holistic method for assessing and enhancing EHR security, employing well-established methods such as a literature review, content analysis, and cybersecurity audit protocols (Mohammed, 2017).

These methods have been analyzed and adapted to suit the specific needs of EHR systems. Regarding EHR cybersecurity challenges (Yeo and Banfield, 2023), this study followed a mixed-methods approach incorporating qualitative and quantitative methods. The initial stages of the study involved a thorough review of the relevant literature. The participants in this study comprised healthcare professionals and IT security experts well versed in EHR use and security issues. The sampling technique was purposive, and it selected individuals who could provide the most relevant insights (Yeo and Banfield, 2023). This study utilized two primary data collection methods. First, surveys were employed to assess the prevalent challenges that healthcare professionals face when dealing with the HER securely. These surveys comprised closed-ended questions to gather quantifiable data suitable for subsequent statistical interpretations. Interviews were conducted with IT security professionals with expertise in EHR security. These interviews aimed to explore the intricacies of EHR security challenges and potential solutions by drawing on the insights provided by experts in the field (Daraghmeh and Brown, 2021). The collected data were subjected to a dual analytical approach to ensure a comprehensive understanding of the EHR cybersecurity challenges.

Quantitative data gathered from the surveys were analyzed using SPSS. This quantitative analysis facilitated the examination of the numerical trends and patterns within the dataset. A thematic analysis was applied to the qualitative data obtained from the interviews. Thematic analysis identified recurring themes and patterns in the qualitative responses, providing

valuable insights into the nuanced aspects of EHR cybersecurity challenges (Ofe and Schmitt, 2023). This combined approach ensures a well-rounded exploration of the research topic and enriches the overall comprehension of EHR security issues.

RESULTS AND DISCUSSION

The experimental results provide a comprehensive understanding of the current state of EHR cybersecurity, revealing that EHR systems are vulnerable to various types of cyberthreats. These threats include unauthorized access, data breaches, and ransomware attacks, which can compromise the integrity, availability, and confidentiality of sensitive patient information. This study examined various aspects of EHR cybersecurity. Furthermore, it evaluated the effectiveness of different security controls, understood the impact of insider threats, and assessed the role of human fallibility in cyber incidents. By simulating real-world attack scenarios, we identify potential vulnerabilities and evaluate the resilience of existing security measures. These results demonstrated the need for improved security practices in the healthcare industry, emphasizing the need for proactive measures to ensure the security and privacy of her systems. Furthermore, various technological solutions, such as encryption, access controls, intrusion detection systems, comprehensive training, and awareness programs, are required to mitigate the risks associated with EHR cybersecurity. Despite regulations being crucial in setting minimum security standards, they are insufficient to protect against emerging cyber threats.

To remain ahead of sophisticated attackers, healthcare institutions must adopt proactive and adaptive security strategies that can anticipate and respond to evolving threats. EHR cybersecurity is a complex and multifaceted issue requiring continuous attention and investment. Moreover, traditional security measures are inadequate for addressing the unique challenges of EHR systems. Therefore, a comprehensive approach encompassing technical, organizational, and human factors must ensure the confidentiality, integrity, and availability of EHRs. Moreover, the experimental conclusions highlighted the need for collaboration among stakeholders in healthcare ecosystems, including healthcare providers, vendors, policymakers, and regulators. Only through collective effort can the inherent vulnerabilities in EHR systems be effectively addressed and patient data adequately protected. The key findings of this study have significant implications for the cybersecurity landscape of EHRs. First, it highlights the urgent need for healthcare organizations to prioritize cybersecurity and allocate appropriate resources to combat cyberthreats (Medhekar, 2022). The consequences of a successful attack on an EHR system can be dire, resulting in compromised patient privacy, disrupted healthcare services, and potential legal and financial liabilities. Second, this study demonstrated that

traditional security measures are insufficient for ever-evolving cyberthreats. Adherence to established security standards and regulations must be supplemented with a proactive, risk-based approach that leverages innovative technologies and practices. Finally, our findings highlight the importance of user education and awareness in safeguarding EHR systems. Human factors, including insider threats and human error, remain significant vulnerabilities. Regular training programs with robust access controls and accountability mechanisms are essential for minimizing these risks (Daraghmeh and Brown, 2021).

Data collection and analysis yielded valuable insights into the challenges associated with EHRs in cybersecurity. A comprehensive examination revealed various trends and patterns, highlighting vulnerabilities within EHR systems. An analysis of the collected data presented quantitative and qualitative findings (Majkowski, 2019). On a quantitative level, the results indicated significant security breaches in EHR systems, with a notable percentage originating from unauthorized access and malware attacks. Qualitatively, the findings drew attention to the impact of these breaches on the confidentiality of data and the level of trust patients have in healthcare institutions. Compared to findings in previous studies, a clear alignment emerged, highlighting the growing cybersecurity challenges in EHR systems. Sempeles (2014) highlighted the criticality of addressing cybersecurity threats in EHRs to safeguard patient privacy and maintain trust.

Similarly, Slotwiner et al. (2018) highlight the need for enhanced security measures to prevent unauthorized access and data breaches within her systems. According to Slotwiner et al. (2018), the rapidly changing healthcare environment and global interconnectivity expose information technology to increasing vulnerabilities. An in-depth analysis of the results obtained from the data provided valuable insights into the complex cybersecurity challenges associated with EHRs. Critical issues surrounding the security and privacy of EHR systems are highlighted by effectively addressing the research aims and objectives. Their findings revealed numerous key cybersecurity challenges in EHR systems, including unauthorized access, data breaches, identity theft, and malicious attacks. These challenges pose significant risks to the confidentiality, integrity, and availability of patient information, compromising the trustworthiness of healthcare institutions and the overall delivery of healthcare services. The study conducted a comprehensive review of the existing literature on EHR cybersecurity challenges.

The significant insights provided by Ferreira and Mateus-Coelho (2023) highlight the complexities of EHR security and the need for enhanced protective measures. Information technology and cybersecurity vulnerabilities place the personal data of patients and healthcare

systems in danger. The analysis underscored the potential consequences associated with EHR cybersecurity challenges, emphasizing the adverse effects on patient trust, healthcare delivery, and the reputation of healthcare institutions. According to Bai, Jiang, and Flasher (2017), as the adoption of electronic records and health information technology rapidly expands, hospitals and other health providers increasingly suffer from data breaches. Breaches in EHR systems can lead to compromised patient information, theft of medical identity, and life-threatening situations. Immediate attention and proactive measures are required to safeguard the security and privacy of EHRs. The findings in this study substantiate existing research and highlight the importance of implementing enhanced security measures and regulations to protect patient information. Healthcare institutions must prioritize the implementation of advanced encryption systems, regular security audits, and routine cybersecurity training for healthcare providers. Cybersecurity is an ever-increasing priority, and organizations ought to be able to evaluate their cybersecurity audit efficiency to identify how best to proceed forward and reinforce their cybersecurity ("How effective," n.d.).

The findings of this study are consistent with those of previous studies on EHR cybersecurity. Sendelj and Ognjanovic (2022) discussed the importance of implementing robust security measures to safeguard sensitive patient data against cyber threats. The challenges faced by healthcare organizations in implementing effective cybersecurity measures discussed by Sitaru et al. (2023) highlight best practices for securing EHRs; however, Sitaru et al. (2023) delve into the privacy and security concerns associated with EHRs. Shah and Khan (2020) provide an international perspective on cybersecurity policies for EHRs. These studies contributed to a comprehensive understanding of the current state of the research field and highlighted the significance of ongoing research on EHR cybersecurity. This study has several implications for the field of EHR cybersecurity. By identifying vulnerabilities and proposing innovative security solutions, the study contributes to ongoing efforts to protect patient data. Furthermore, it highlighted the need for a proactive, multilayered approach prioritizing patient privacy. First, the findings were based on a specific contextual setting and may not be universally applicable. Owing to resource constraints, this study focused on cybersecurity threats, limiting the scope of its conclusions and addressing the controversy surrounding EHR cybersecurity (Luh and Yen, 2020). Future studies must address these limitations and explore other aspects of EHR cybersecurity.

The debate between the effectiveness of stringent regulatory controls and the risk of human fallibility and insider threats is ongoing. By consolidating existing research and proposing innovative security solutions, this study contributes to a comprehensive

understanding of this issue. Despite regulatory controls being crucial, a comprehensive approach that includes employee training, access controls, and encryption is essential to mitigate the risks associated with external and internal threats. As technology advances, future research on EHR cybersecurity must explore novel methods for addressing emerging threats. For instance, research could focus on the development of artificial intelligence-based systems capable of detecting and mitigating cyberattacks in real time. More research is required to assess the effectiveness of various regulatory controls when combined with technological solutions. Furthermore, studies must assess the impact of emerging technologies, such as blockchain, on EHR cybersecurity. By pursuing these future directions, healthcare organizations can enhance their security posture and effectively protect sensitive patient data in an evolving threat landscape.

CONCLUSION

This study highlights the cybersecurity landscape in EHRs and the numerous flaws, challenges, and threats within the current system. This study revealed the prevalence of vulnerabilities such as inadequate access controls, outdated software, and social engineering attacks exploiting human fallibility by emphasizing the need for robust security solutions to safeguard sensitive patient information. The potential consequences of these vulnerabilities include breaches of patient confidentiality, healthcare service disruptions, and potential harm to patients. The significance of this study lies in its ability to highlight the importance and urgency of addressing EHR cybersecurity issues. By highlighting various vulnerabilities, exploring controversial hypotheses, and providing an understanding of the field, this study contributes to existing knowledge. Furthermore, it can equip policymakers, healthcare providers, and cybersecurity professionals with the required insights to make informed decisions and strengthen cybersecurity measures within EHR systems (Puri and Gochhait, 2023). Additionally, this study emphasizes the indispensability of collaboration among various stakeholders, including healthcare providers, policymakers, technology developers, and cybersecurity experts, to establish industry standards that ensure resilient EHR cybersecurity (Kruse, 2017).

Moreover, this study highlights the importance of adopting a comprehensive approach that considers technological advancements and human factors while safeguarding sensitive patient information. Furthermore, this emphasizes the urgent need for proactive and multifaceted security measures capable of adapting to evolving threats. Among the recommended measures, the implementation of robust access controls, encryption, and network segmentation has tremendous potential for enhancing cybersecurity. Furthermore, this study

highlights the importance of embracing continuous monitoring, incident response planning, and comprehensive education and training programs to promote cybersecurity awareness among healthcare stakeholders. Establishing a cybersecurity culture within healthcare organizations is crucial for mitigating the risks in the ever-changing cyberthreat landscape.

Current security measures are inadequate, leading to breaches that affect data confidentiality and patient trust in healthcare institutions. Kioskli, Fotis, and Mouratidis (2021) indicated that the healthcare sector is underequipped to face cyberattacks because of its vulnerability to attackers. Clarke and Martin (2023) highlighted that balancing cybersecurity risk in healthcare settings with end-user concerns around functionality requires a proactive and collaborative approach. To address the identified challenges effectively, it is crucial to strengthen the current security measures for EHR systems by implementing advanced encryption systems and conducting regular security audits. In addition, the adoption of stringent regulatory actions to counteract potential cybersecurity threats must be prioritized. Healthcare institutions must also invest in routine cybersecurity training programs to equip healthcare providers with the required knowledge and create awareness of the significance of secure EHR handling.

SUGGESTIONS

This study provides a foundation for future investigations in the complex EHR cybersecurity domain. According to Waddell (2023), leaders who promote cybersecurity education focused on the human factors of cyberattacks build a resilient workforce that complements technical protections, reducing organizational risk.

Despite its valuable contributions, this study had several limitations. One of its limitations lies in its reliance on existing literature and empirical data, which may not provide comprehensive coverage of all aspects of EHR cybersecurity. In addition, this study focused solely on the current state of the field and did not explore the potential implications of emerging technologies for EHR cybersecurity. Future research must explore innovative tools and methods for safeguarding EHRs against increasingly complex cyber threats. The effectiveness of regulatory controls and understanding their function in protecting EHRs is another avenue for further exploration, which includes assessing the impact of well-known regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) on EHR cybersecurity practices. Finally, the social and ethical implications of EHR cybersecurity must be considered, including privacy, trust, and potential biases introduced by algorithmic decision-making in healthcare (Thompson, 2020).

This study serves as a foundation for future investigations into the complex field of EHR cybersecurity. Future studies could focus on the development of specialized cybersecurity tools designed for EHR systems or explore the potential impact of emerging technologies, such as artificial intelligence and blockchains, on enhancing EHR security.

ACKNOWLEDGMENT

Completing this study would not have been possible without numerous individuals and the invaluable support and contributions of Capitol Technology University and the University of Baltimore County. First, I would like to express my deepest gratitude to the participants who generously shared their experiences and profound insights, which were crucial in shaping the findings and outcomes of this study. Furthermore, I am grateful to the American College of Healthcare Executives, who provided considerable support and resources and invaluable data. Their unwavering cooperation and dedication to this collaboration significantly enriched the research process and enabled me to comprehensively investigate the complex landscape of cybersecurity threats in the dynamic healthcare sector. In addition, I extend my heartfelt appreciation to my esteemed research advisors and colleagues, whose unwavering guidance, invaluable feedback, and steadfast assistance have been pivotal throughout this transformative research journey. Their exceptional expertise and invaluable contributions considerably enhanced the quality of this study. This research endeavor would not have been possible without their crucial support.

REFERENCES

Alharam, A.K., El-Madany, W.: The effects of cyber-security on healthcare industry 9th IEEE-GCC Conf. Exhib. GCCCE, vol. 2017. (2018). doi:10.1109/IEEEGCC.2017.8448206

Bai, G., Jiang, J.X., Flasher, R.: Hospital risk of data breaches. JAMA Intern. Med. 177, 878–880 (2017). doi:10.1001/JAMAINTERNMED.2017.0336

Burke, W., Oseni, T., Jolfaei, A., Gondal, I.: Cybersecurity indexes for ehealth. ACM Int. Conf. Proceeding Ser., 1–8 (2019). doi:10.1145/3290688.3290721

Chen, Q., Lambright, J., Abdelwahed, S.: Towards autonomic security management of healthcare information systems First Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol., pp. 113–118 (2016). doi:10.1109/CHASE.2016.58

Clarke, M., Martin, K.: Managing cybersecurity risk in healthcare settings. Healthc. Manage. Forum, 8404704231195804 (2023). doi.org/10.1177/08404704231195804

Coventry, L., Branley, D.: Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113, 48–52 (2018). doi:10.1016/J.MATURITAS.2018.04.008

Cuenca, J.V., A.: Capstone, CYBERSECURITY CHALLENGES IN HEALTHCARE INDUSTRIES (2017)

Daraghmeh, R., Brown, R., Big Data, A. Conf. Inf. Technol., pp. 826–833 (2021). doi:10.1109/ICIT52682.2021.9491781

Ferreira, D.J., Mateus-Coelho, N.: Cybersecurity risks in health data and measures to take. Https://Services. Igi-Global.com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-6684-8422-7.Ch001 1AD, 1–18 (2023). doi:10.4018/978-1-6684-8422-7.CH001

Ghafur, S., Grass, E., Jennings, N.R., Darzi, A.: The challenges of cybersecurity in health care: The UK National Health Service as a case study. Lancet Digit. Health 1, e10–e12 (2019). doi:10.1016/S2589-7500(19)30005-6

How effective is your cybersecurity audit?, https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/how-effective-is-your-cybersecurity-audit (Accessed October 16, 2023) (n.d.)

Huang, C., Koppel, R., McGreevey, J.D., Craven, C.K., Schreiber, R.: Transitions from one electronic health record to another: Challenges, pitfalls, and recommendations. Appl. Clin. Inform. 11, 742–754 (2020). doi:10.1055/S-0040-1718535

Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V.P.: IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J. Inf. Secur. 2020, 1–18 (2020). doi:10.1186/S13635-020-00111-0/TABLES/8

Keshta, I., Odeh, A.: Security and privacy of electronic health records: Concerns and challenges. Egypt. Inform. J. 22, 177–183 (2021). doi:10.1016/J.EIJ.2020.07.003

Kioskli, K., Fotis, T., Mouratidis, H.: The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. ACM Int. Conf. Proceeding Ser., 1–9 (2021). doi:10.1145/3465481.3470033

Kruse, C.S., Smith, B., Vanderlinden, H., Nealand, A.: Security techniques for the electronic health records. J. Med. Syst. 41, 127 (2017). doi:10.1007/S10916-017-0778-4

Luh, F., Yen, Y.: Cybersecurity in science and medicine: Threats and challenges. Trends Biotechnol. 38, 825–828 (2020). doi:10.1016/J.TIBTECH.2020.02.010

Majkowski, G.O.: Healthcare Cybersecurity: Building a Cyber Vulnerability Profile for US Hospitals. The University of Alabama at Birmingham (2019)

McDermott, D.S., Kamerer, J.L., Birk, A.T.: Electronic health records. Int. J. Cyber Res. Educ. 1, 42–49 (2019). doi:10.4018/IJCRE.2019070104

Medhekar, A., My Health Record and Emerging Cybersecurity Challenges in the Australian Digital Environment, Res. Anthol. Secur. Med. Syst. Rec. 428–447 (2022). doi:10.4018/978-1-6684-6311-6.CH021

Mohammed, D.: U.S. healthcare industry: Cybersecurity regulatory and compliance issues, J. Res. J. Bus. Econ. Manag. (2017), www.scitecresearch.com/journals/index.php/jrbem. (Accessed October 16, 2023)

Ofe, M., Schmitt, A.: A Qualitative Study Exploring Security Practices Healthcare Providers Need to Reduce the Risk of Successful Ransomware Attacks on Electronic Health Record Systems Committee Members (2023)

Puri, M., Gochhait, S.: Data security in healthcare: Enhancing the safety of data with CyberSecurity: Proc. 8th Int. Conf. Commun. Syst. ICCES 2023, pp. 1779–1783 (2023). doi:10.1109/ICCES57224.2023.10192596

Sendelj, R., Ognjanovic, I.: Cybersecurity challenges in healthcare. In: Achievements, Milestones and Challenges in Biomedical and Health Informatics, pp. 190–202 (2022). doi: 10.3233/SHTI220951

Shah, S.M., Khan, R.A.: Secondary use of electronic health record: Opportunities and challenges. IEEE Access 8, 136947–136965 (2020). doi:10.1109/ACCESS.2020.3011099

Sempeles, S.: Concerns continue to rise regarding device cyber security. J. Clin. Eng. 39, 100–101 (2014). doi:10.1097/JCE.0000000000000044

Sitaru, S., Bramm, G., Zink, A., Hiller, M.: Cybersecurity in digital healthcare—Challenges and potential solutions, Dermatologie 74, 213–217 (2023). doi:10.1007/S00105-023-05117-6/METRICS

Slotwiner, D.J., Deering, T.F., Fu, K., Russo, A.M., Walsh, M.N., Van Hare, G.F.: Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit, Hear. Rhythm. 15, e61–e67 (2018). doi:10.1016/J.HRTHM.2018.05.001

Thompson, E.C.: Designing a HIPAA-Compliant Security Operations Center: A guide to detecting and responding to healthcare breaches and events, Des. A HIPAA-Compliant Secur. Oper. Cent. Guid. Detect. Responding Healthc. Breaches Events, 1–231 (2020). doi:10.1007/978-1-4842-5608-4

Waddell, M.: Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. Healthc. Manage. Forum, 8404704231196137 (2023). doi.org/10.1177/08404704231196137

Yeo, L.H., Banfield, J.: Human factors in electronic health records cybersecurity breach: An exploratory analysis. Perspect. Heal. Inf. Manag. 19, 1i (2022). /pmc/articles/PMC9123525/ (accessed October 16, 2023)