A Review of Cyber Threats to Medical Devices Integration with Electronic Medical Records

Aeshah Alhammad
Faculty of Information Science and Technology
University Kebangsan Malaysia
Malaysia, Bangi ,43600
Aesha.h@live.com

Maryati Mohd. Yusof,
Faculty of Information Science and Technology
University Kebangsan Malaysia
Malaysia, Bangi ,43600
maryati.yusof@ukm.edu.my

Dian Indrayani Jambari
Faculty of Information Science and Technology
University Kebangsan Malaysia
Malaysia, Bangi ,43600
dian@ukm.edu.my

2022 International Conference on Cyber Resilience (ICCR) | 978-1-6654-6122-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCR56254.2022.9995984

***Abstract*— Medical devices and Electronic Medical Records (EMR) have been technologically integrated, transforming their independent structure and functionality. There is a significant increase in medical device deployment in healthcare institutions. However, the integration exposes them to cyber threats, which can undermine effective care delivery and threaten patient safety. The World Health Organization has noticed a significant rise in cyberattacks following the COVID-19 outbreak. This paper reviews the literature on cyber threats affecting the medical device integration with EMR (MDI-EMR). It highlights the cyber threats to the MDI-EMR and the effectiveness of control mechanisms. The most common cyber threats to MD include phishing, ransomware attacks, data breaches, Distributed Denial of Service attacks, and SQL injection. Security challenges associated with the EMR and medical devices are also threating their confidentiality, integrity, and availability. The review enables researchers to better understand safety, security and privacy issues related to the MD-EMR, as well as available solutions.**

Keywords—Medical devices, electronic medical records, cyber threats, control mechanisms, safety, security, privacy

I. Introduction

In the modern digital healthcare sector, medical devices, such as defibrillators, vital signs monitors, ventilators, and infusion pumps, are connected to Electronic Medical Records (EMR), which are the cornerstone of Health Information Systems (HIS). Medical devices operate in a sophisticated technological environment composed of networks, software and operating systems, challenging their cybersecurity [1]–[4]. For example, network-connected medical devices are linked to HIS [5], exposing the healthcare sector to massive security breaches and cybersecurity issues because of the security vulnerabilities in the medical devices [2], [4]. EMR manages medical information across various medical facilities from anywhere [6], and it is an essential tool for high-quality, safe, and cost-effective healthcare [7]. It shares and exchanges information across systems to improve healthcare delivery, reduce errors, and further innovate the healthcare industry [8], [9]. Medical device integration with EMR (MDI-EMR) is an example of such emerging, innovative technology.

However, integrated health systems can be undermined by cyber threats or cyberattacks. Even though there are several mitigation strategies and countermeasures, cyber threats are still increasing. Cyberattacks are recurring in health organizations, severely affecting high and middle-income hospitals [10]. The attacks come in several forms, such as WannaCry and Petya ransomware, targeting HIS [11]. When hospitals are exposed to cyber threats, vital machinery, such as that used in the Intensive Care Unit (ICU), fails to work. Home devices such as nebulizers, where interventions rely on power, can also be seriously affected [12]. Furthermore, hospitals can struggle with the disruption of significant medical operations and the disclosure of patient personal information [10]. Cybersecurity is meant to shield cyberspace from possible cyber threats or attacks [13]. The cybersecurity of MDI-EMR requires technical, organizational, and human considerations. Device manufacturers, clinicians, and patients are among the significant stakeholders in building the cybersecurity of healthcare institutions, such as hospitals.

This paper reviews the types and sources of cyber threats and the effectiveness of mitigation strategies. Practically, the review shows concerned agencies if there is consistency in the cybersecurity of MDI-EMR and reveals the cybersecurity awareness among key stakeholders like clinicians and IT specialists. Due to increasing problems in MDI-EMR cybersecurity [14], it is necessary to understand it as a complex socio-technical challenge. According to the World Health Organization (WHO), cyberattacks have increased five times during 2021 [5], which pose a potential threat to all medical procedures and seriously jeopardize the healthcare system. While human behaviors, technological problems, internal operational faults, and external factors can boost cyber risks, the COVID-19 pandemic is the greatest risk originating from human behaviors and technological inadequacies (Social Engineering) [15]. The paper is organized as follows: Section two presents the method of the literature review. Section 3 shows an overview of related work. Section 4 discusses the review, and section 5 concludes the paper and presents the limitations of the review.

II. MATERIALS AND METHODS

The literature review was based on the guidelines of Tranfield et al.[16]. We searched electronic databases, including Google Scholar, ProQuest, PubMed, Web of Science, Science Direct, Saudi Digital Library, FDA websites and e-books. The terms used in the database searches were (a) cybersecurity/security, (b) EMR, (c) medical devices/networked medical devices, (d) cyber risks/threats to EMR/medical devices, (e) medical devices connected to EMR, (f) cybersecurity vulnerabilities/threats, (g) EMR/EHR cybersecurity, (h) integrated medical devices (i) Health Information System (HIS), (j) cyber threats, (k) cyber threat evaluation frameworks/models.

III. OVERVIEW OF RELATED WORK

Table 1 shows an overview of previous studies related to the cybersecurity of MDI-EMR.

978-1-6654-6122-1/22/$31.00 ©2022 IEEE

TABLE I. *THEME ANALYSIS OF THE REVIEWED LITERATURE*

Reference	***Theme***	***Findings/Conclusions***
[17]	Cybersecurity trends and threats in healthcare institutions	Healthcare institutions must continually adapt to the ever-changing cybersecurity trends and threats by identifying all the external and internal threats and trends of their integrated medical devices.
[5], [9], [18]–[20]	Medical device vulnerabilities and cybersecurity challenges	Further identification of possible attacks on class II and III medical devices is needed. There are possible threats during the transmission of patient and device data. Further research is needed to explore data privacy protection and medical device cybersecurity.
[9], [21], [22]	Security threats to medical devices	With the development of medical devices' connectivity and interconnection capabilities to network, security threats have been increasing rapidly. Healthcare organizations attempted to provide protections against cyberattacks like malicious software which cause device operation disruption, sending false information to devices and unauthorized commands issued to devices. There are five hacking methods: scanning attack, spoofing attack, injection attack, broken authentication and session management, and DoS attack.
[1], [6], [19], [23]	Cyber threats to medical devices	Clinicians' accessibility to the EMR and use of different medical equipment might be restricted by an adversary. Attackers have various motivations. The concept, design, deployment, and use of these devices include security considerations. Security measures associated with medical devices use can enhance security and privacy.
[3], [5], [9], [18]–[20], [24]	Countermeasures taken to reduce cyberattacks on medical devices	Experts must be given risk-assessment and mitigation instructions on cybersecurity risks to MDI-systems since hospitals are suffering from the repercussions of neglected precautions and emerging cybersecurity challenges. Threats and medical advancements are emerging.

A. Cyber Threats to the MDI-EMR

With the development of network-connected medical equipment, EMR, and communication networks, hospitals are becoming increasingly dependent on HIS for organizational, economic, and health operations. An EMR can share medical information with medical devices. The files in the EMR contain essential patient information such as age, weight, test results, allergies, and prescribed medication. However, there is an ongoing concern about their exposure to cyberattacks [6], [7]. Using networked devices allows attackers to exploit system vulnerabilities by manipulating the device settings [1], which consequently affects their operation [5]. Several studies focused on data breaches in the EMR [18], [25], but limited research investigated the cybersecurity of medical devices [10] which may or may not be intentionally attacked [5]. Privacy violations are spiraling proportionately with the emergence of network-based medical equipment [9]. Cyberattacks on medical devices threaten patient safety [21]. Therefore, it is necessary to identify the cyber threats emerging from the EMR, network and medical devices as well as the best cybersecurity practices.

Interoperability across system software, operating environment, healthcare equipment interfaces, and data communication networks are the foundation of a digitalized health system [1], [26]–[28]. Poor integration of medical devices and information systems resulted in incomplete information necessary for workflow and decision-making, affecting process efficiency and posing risk to patient safety. In contrast, MDI-EMR improved the quality of medical care and treatment. It decreased drug and diagnostic errors, reduced care and treatment costs, and boosted clinicians' productivity and efficiency. Additionally, it reduced hospital stays by minimizing unnecessary testing [29]. Even though digital transformation provides advanced medical care, it has created the unexpected and increased risk of cyberattacks [25], [30], [31]. As they focus more on patient care [19], [32], poor cybersecurity practices make healthcare facilities suffer from cyber threats that can cost lives [33]. Some healthcare organizations neglect or have weak cybersecurity strategies, prioritizing availability over confidentiality [34]. Furthermore, the complexity of digital health infrastructure, networking and connectivity increases its cybersecurity vulnerability.

The interaction and integration of medical devices will continue to increase in the ICU, and radiological and surgical divisions [3]. Medical devices use various resources, such as an EMR, within a network. There are four types of networked medical devices: embedded devices (such as pacemakers), external equipment (such as insulin pumps), static equipment (such as connected infusion pumps), and consumer goods (e.g., FitBit or Nike Fuel band) [1], [35]. In addition, the FDA divides medical equipment into three categories according to the potential dangers they pose. Class I and II both have low to moderate risk, but class III has a higher to enormous risk [9]. Interconnected systems need technologies to deal with a pool of electronic patient information appropriately without compromising their security [36]. However, the more intensive the connectivity of medical devices to a network, the more likely a cyberattack to occur [3]. Even implantable medical devices controlled by a wireless network showed cybersecurity failure [37].

Meanwhile, an attack on the EMR's database can prevent physicians from retrieving patient information; and consequently, treatment delays [18]. A cyberattack on an EMR affects the medical device that is connected to the same network. Therefore, medical devices connected to the EMR can be affected by an unintentional attack [5]. According to the Food and Drug Administration (FDA), the software used by medical devices makes them more vulnerable to cyber threats [38].

Digital healthcare system offers massive personal data. However, cyberattacks on these assets threaten their confidentiality, accessibility, and integrity [27]. Therefore, there must be mitigation strategies to safeguard health organizations from security challenges that occur during data transfer and storage. In their systematic review, Offner et al. [19] concluded that the healthcare sector still lacks sophisticated technical and human resources to solve its cybersecurity challenges. The health industry needs to boost its cybersecurity capability and develop advanced technological solutions to prevent constantly evolving cybersecurity threats. Emerging cyber risks require emerging cybersecurity controls to mitigate them [24]. Healthcare businesses must understand how risks affect systems' vulnerabilities and choose appropriate mitigation strategies [24].

One of the approaches which address cyber threats is the STRIDE Threat Model, developed by Microsoft and commonly used in governments and industries [39]. It is a formal, structured, and well-documented approach that classifies threats into Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation of Privilege. Table 2 shows threat categories and desired security properties. Each of the six threat classifications represents an attack method that could target information security components, and each threat category is associated with a specific IT property that helps combat that specific threat [40], [41]. The model enabled stakeholders to assess potential threats' risks and impacts and develop countermeasures to mitigate them. For example, Stine et al. [41] developed a cyber risk scoring system for medical devices based on the STRIDE model.

TABLE II. THREAT CATEGORIES AND DESIRED SECURITY PROPERTIES

Threat Category	***Target***	***Threat example***	***What the attacker does***
Spoofing (S)	***Local machine***	▪ Process	▪Creates a file to be used as original before the real process ▪Abuses names
		▪ Filename	▪Creates a file in the local directory ▪Creates a link and changes it ▪Creates many files in a target directory ▪Sends viruses
	Network	▪ Machine	▪IP spoofing ▪DNS spoofing ▪DNS compromise ▪IP redirection ▪Attacks on the Internet of Things (IoT) Devices ▪Insecure devices
		▪ Person	▪Takes over an account ▪Sets the display name ▪Manipulates a user's identity ▪Blackmail ▪Phishing
		▪ Role	▪Declares themselves to be that role ▪Man in the middle (MITM) attack
Tampering (T)	***File***	▪ Data leakage ▪ Data theft ▪ Sensitive data exposure	▪Modifies files that an organization owns and relies on ▪Takes over a file ▪Compromises system integrity ▪Default passwords
	Memory	▪ Modify code ▪ Modify compromised disk	▪ Changes the organizational code/supplied data ▪Ransomware
	Network	▪ Redirect data flow to their machine ▪ Modify data flowing over the network ▪ Malware	▪Attacks a network layer to redirect traffic ▪Uses network tampering to improve spoofing attack ▪Ransomware
Repudiation (R)	***Network/ EMR/MD***	▪ Repudiate an action ▪ Repudiate attacks on logs	▪Claims not to have clicked ▪Claims not to have received ▪Claims not to be a fraud victim ▪Uses someone else's account ▪Modifies data flowing over a network ▪Disgruntled employee ▪Insider threat
Information disclosure (I)	***Data stores***	▪ Data leakage ▪ Data theft ▪ Sensitive data exposure ▪ Compromised disk	▪ Compromising confidentiality ▪SQL Injection Exploit
	Data Flow	▪ Data from Network ▪ Malware	▪Reads data on a network ▪Redirects traffics to enable reading data on a network
		▪ Metadata ▪ Unauthorized access	▪Learns secrets by analyzing traffic ▪Learns who talks to whom by watching the DNS or analyzing social network information
Denial of Service (D)	***Temporary (network) or persistence (fill a disk)***	▪ Against a process	▪Occupies memory or CPU ▪Uses a process as an amplifier "Too many login attempts" ▪Compromising availability ▪Vandalizes and disrupts services
		▪ Against a data store	▪Fills the data store ▪Creates excess requests to slow the system
		▪ Against a data flow ▪ Malware	▪Consumes network resources ▪Denial of Service Attack
Privilege elevation (EoP)		▪ EoP against process via corruption	▪Sends codes that cannot be handle or processed properly by the system ▪Gains read/write access to memory ▪Privilege escalation attack ▪Non-compliance
		▪ EoP via misused authorization checks	▪Unauthorized access
		▪ EoP via data tampering	▪Modifies bits on disk

B. Privacy and Security Vulnerabilities in the EMR

Several studies investigated concerns about the confidentiality of personal data, which is crucial to effective EMR implementation [42], [43]. According to several polls, there are various concerns about protecting the confidentiality of clinical records. 39% of the participants stated that their patient data was safe and protected, and over two-thirds of the participants were not concerned about protecting their individual patient history [44], [45]. Some participants did not worry much about it and had confidence in the safety of their information in several situations. 50% of interviewees were anxious about their information safety due to information exchange over the web [44]. Approximately half of the respondents believed that disclosing their patient data would compromise their confidentiality [45].

C. Confidentiality Issues Associated with the EMR

The fast deployment of the EMR has not been safeguarded by appropriate cybersecurity measures, leaving the health sector vulnerable to serious cyberattacks[46]. Some research discussed organizational, architectural, and technical security considerations that include various security practices used by healthcare systems to safeguard private EMR data. Organizational safeguarding consists of measures like performing assessments, placing a cybersecurity administrator, and creating backup plans [47]. The precautions for confidentiality centered on creating compliant security plans and processes. The architectural safeguarding includes organizational protection strategies as well as the physical security of medical records to prevent access by unauthorized individuals or those who would exploit them. Privacy violations occur as a result of architectural security violations. An approach for physical protection may be to designate security positions. Applying technical safeguards that secure the information systems included in a healthcare organization's network is also essential for safeguarding organizational privacy since most security vulnerabilities involve digital media, such as workstations and other electronic gadgets[48]. Protection mechanisms like firewalls and cryptography, antivirus scan, and data verification are equally important[6]. The most popular safety precautions, however, are firewalls and cryptography. Major security precautions include virus protection, information security personnel, and cloud services, although their acceptance is budget-dependent[46].

D. Best Practices in Healthcare Settings

Cybersecurity refers to the body of processes and practices aimed to secure networks, devices, programs operating in medical devices, and data kept in the EMR from any possible threats, cyberattacks, damage, or unauthorized use. Also, medical device cybersecurity refers to the tools and practices that prevent attackers from gaining unauthorized access to or control over them and the data they generate [49]

Knowing the possible attacks on medical devices and identifying system vulnerabilities by using integrated cybersecurity practices in hospitals allows physicians to rely on medical devices for their multiple functions [41]. The reported countermeasures and architectures in the literature are still limited in terms of resource depletion, attack reduction, and applicability [18]. Patient lives can be saved by identifying the cyber threats emerging from the EMR, network or medical devices. An efficient cybersecurity control identifies new security vulnerabilities in EMR, medical devices or networks and resolves them promptly without compromising the safety of patients [23].

The weaknesses of current mitigation strategies can be attributed to several issues. Implementing cybersecurity is very challenging since hospitals have numerous medical devices [50]. Designing efficient and lightweight security and privacy-preserving solutions for medical devices remains challenging because integrated medical devices are susceptible to network vulnerabilities [46],[47]. Furthermore, cybersecurity practitioners have limited access to medical devices, particularly implanted medical devices, for testing and experimentation purposes to avoid potential cyberattacks [52].. Cybersecurity best practices refer to the policies, procedures or strategies to protect data [53]. To achieve optimum cybersecurity, healthcare organizations need to identify potential threats, the best practices in selecting a policy and the measurement that mitigates or avoids cyberattacks [24]. A way to protect medical devices from attacks is to shield them from attackers by operating them in a restricted environment [3]. An effective information security plan is based on preventive, detective measures [1]. Physical, administrative, and technological controls must be implemented in an interrelated manner to protect data with their storage area, devices, and network, as shown in Fig. 1 [25][54].

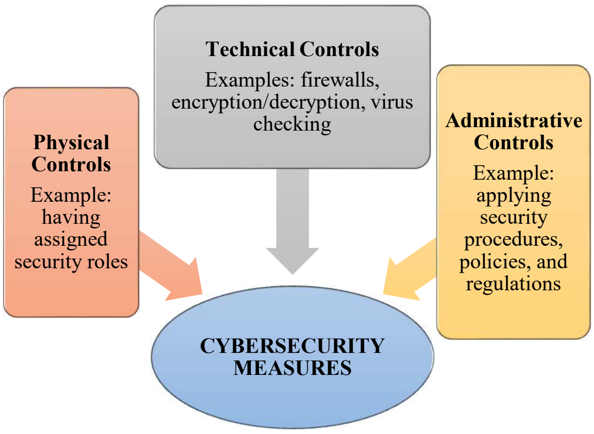
Technical Controls
Examples: firewalls, encryption/decryption, virus checking
Physical Controls
Example: having assigned security roles
Administrative Controls
Example: applying security procedures, policies, and regulations
CYBERSECURITY MEASURES

Fig. 1. Cybersecurity measures

IV. Discussion

Research on cyber threats associated with the MDI-EMR calls for further work. Research on cyber risk governance is limited; there is a dearth of hazard analysis for the particular requirements of healthcare institutions. This problem must be approached using a comprehensive and interdisciplinary strategy to respond to managerial challenges. Additionally, this review demonstrates dynamic challenges of identifying and mitigating MDI-EMR risks. One of the major IT risks in healthcare facilities and organizations is the [1] of a cyber-based platform by invaders, fraudsters, or unethical individuals to collect information on the users of the health organization's system . Organizations may leverage the digital infrastructure, known as the cyber-based platform, to make life simpler for their workers. Everybody is at risk, since this system can be manipulated to allow the adversary to obtain crucial health data pertinent to their activity.

Cyber threats have a detrimental impact on organizations, including the communication platforms which make up the interactive cyberspace to save, modify, and communicate data and including organizational, physical, and service-related data sources. Therefore, more work is needed to provide further insights of the topic.

Risks associated with HIS, including the EMR, are emphasized under the most significant categories, such as deliberate, software, and process controls. As cyberattacks are damaging and challenging to mitigate, it is important to safeguard them. The MDI-EMR assists employees and clinicians by allowing remote labor for clinical and managerial purposes, but it is important to alert healthcare services and their users of internal and external risks [18]. Internal problems include poorly built communications systems and inefficiencies. It is increasingly difficult to make sense of every behavior as these threats become more widespread. For instance, telehealth carries a significant danger of inflicting injury. A common cyber concern is remote access to patients' computerized medical information. Invaders may take advantage of this accessibility to obtain unauthorized access to databases. Invaders can also access data by taking advantage of employee carelessness and weaknesses in technology.

Effective risk management, preventive and reactive risk evaluation, stipulating insurance plans to safeguard stakeholders and healthcare services, high-performance technologies and continuous quality improvement are recommended as ways to enhance cyber risk governance [55]. Software for device protection, security patches, and anti-malware must be regularly updated. To protect patient health and reduce risks, healthcare staff must also undergo continuous safety training. The literature emphasized on the value of risk management procedures for reducing risks in the healthcare industry [56], [57]. It promotes both active and passive risk evaluation tools to analyze, regulate, and control risks efficiently.

V. CONCLUSION

This paper reviews cyber risks related to the MDI-EMR. Conclude something on the prevalence, impact, mitigation of MDE-EMR. Further research on addressing cyber threat challenges is needed in global, multi-disciplinary, structured and specific categorization of operational cybersecurity perspectives. More work is also needed to examine external circumstances, including hazards, legal challenges, commercial problems, and service requirements.

REFERENCES

[1] V. Hassija, V. Chamola, B. C. Bajpai, Naren, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction?," Sustain. Cities Soc., vol. 66, Mar. 2021, doi: 10.1016/j.scs.2020.102552.

[2] B. Ransford et al., "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists," Pacing Clin. Electrophysiol., vol. 40, no. 8, pp. 913–917, Aug. 2017, doi: 10.1111/pace.13102.

[3] M. Willing, C. Dresen, U. Haverkamp, and S. Schinzel, "Analyzing medical device connectivity and its effect on cyber security in german hospitals," BMC Med. Inform. Decis. Mak., vol. 20, no. 1, pp. 1–15, Sep. 2020, doi: 10.1186/s12911-020-01259-y.

[4] J. J. Cebula and L. R. Young, "A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images," no. December, 2010, [Online]. Available: http://www.sei.cmu.edu.

[5] J. Goldman, B. Minzter, J. Ortiz, M. Banoub, and B. Rothman, "Formation of an ASA Cybersecurity Task Force (CSTF) to Protect Patient Safety," ASA Monit., 2020.

[6] C. Eliash, I. Lazar, and N. Nissim, "SEC-C-U: The Security of Intensive Care Unit Medical Devices and Their Ecosystems," IEEE Access, vol. 8, pp. 64193–64224, 2020, doi: 10.1109/ACCESS.2020.2984726.

[7] B. Aldosari, S. Al-Mansour, H. Aldosari, and A. Alanazi, "Assessment of factors influencing nurses acceptance of electronic medical record in a Saudi Arabia hospital," Informatics Med. Unlocked, vol. 10, pp. 82–88, 2018, doi: 10.1016/j.imu.2017.12.007.

[8] M. Ibrahim, A. Alsheikh, and A. Matar, "Attack graph modeling for implantable pacemaker," Biosensors, vol. 10, no. 14, pp. 1–12, Feb. 2020, doi: 10.3390/bios10020014.

[9] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review," IEEE Commun. Surv. Tutorials, vol. 21, no. 4, pp. 3723–3768, Oct. 2019, doi: 10.1109/COMST.2019.2914094.

[10] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, "The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review," BMC Med. Inform. Decis. Mak., vol. 19, no. 10, pp. 1–11, Jan. 2019, doi: 10.1186/s12911-018-0724-5.

[11] S. Furnell and D. Emm, "The ABC of ransomware protection," Comput. Fraud Secur., 2017.

[12] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks with Provable Security," IEEE Syst. J., vol. 11, no. 4, pp. 2590–2601, Dec. 2017, doi: 10.1109/JSYST.2016.2544805.

[13] M. Barrett et al., "NISTIR 8170: Approaches for Federal Agencies to Use the Cybersecurity Framework Approaches for Federal Agencies to Use the Cybersecurity Framework," NISTIR, 2020.

[14] J. William, M. . Gordon, A. Fairhall, A.L.M., and A. Landman, "Threats to Information Security — Public Health Implications," N. Engl. J. Med., pp. 1–3, 2017.

[15] V. Sushruth and K. R. Reddy, "Social Engineering Attacks During the COVID - 19 Pandemic," SN Comput. Sci., pp. 1–9, 2021, doi: 10.1007/s42979-020-00443-1.

[16] D. Tranfield, D. Denyer, and P. Smart, "Synchronous Computer Mediated Communication in English Language Classes During the Pandemic: A Case Study of Wuhan," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 13089 LNCS, pp. 325–333, 2021, doi: 10.1007/978-3-030-92836-0_28.

[17] S. S. Bhuyan et al., "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations," Journal of Medical Systems, vol. 44, no. 5. Springer, May 01, 2020, doi: 10.1007/s10916-019-1507-y.

[18] A. Razaque et al., "Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain," IEEE Access, vol. 7, pp. 168774–168797, 2019, doi: 10.1109/ACCESS.2019.2950849.

[19] K. L. Offner, E. Sitnikova, K. Joiner, and C. R. Maclntyre, "Towards understanding cybersecurity capability in Australian healthcare organisations : a systematic review of recent trends , threats and mitigation," Intell. Natl. Secur., vol. 00, no. 00, pp. 1–30, 2020, doi: 10.1080/02684527.2020.1752459.

[20] S. Das, G. P. Siroky, S. Lee, D. Mehta, and R. Suri, "Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices," Hear. Rhythm Soc., vol. 18, no. 3, Oct. 2021, doi: 10.1016/j.hrthm.2020.10.009.

[21] D.-W. Kim, J.-Y. Choi, and K.-H. Han, "Medical Device Safety Management Using Cybersecurity Risk Analysis," IEEE Access, vol. 8, pp. 115370–115382, 2020, doi: 10.1109/ACCESS.2020.3003032.

[22] Q. Chen, Toward realizing self-protecting healthcare information systems: Design and security challenges, 1st ed., vol. 114. Elsevier Inc., 2019.

[23] T. Granlund, J. Vedenpää, V. Stirbu, and T. Mikkonen, "On Medical Device Cybersecurity Compliance in EU," Coenell Univ., 2021, [Online]. Available: http://arxiv.org/abs/2103.06809.

[24] U. Y. Kabir, E. Ezekekwu, S. S. Bhuyan, A. Mahmood, and A. Dobalian, "Trends and best practices in health care cybersecurity insurance policy," Am. Soc. Healthc. Risk Manag., vol. 40, no. 2, pp. 10–14, Oct. 2020, doi: 10.1002/jhrm.21414.

[25] C. Abraham, D. Chatterjee, and R. R. Sims, "Muddling through cybersecurity: Insights from the U.S. healthcare industry," ELSEVIER, vol. 62, no. 4, pp. 539–548, Jul. 2019, doi: 10.1016/j.bushor.2019.03.010.

[26] M. Haghi, K. Thurow, and R. Stoll, "Wearable devices in medical internet of things: Scientific research and commercially available devices," Healthc. Inform. Res., vol. 23, no. 1, pp. 4–15, Jan. 2017, doi: 10.4258/hir.2017.23.1.4.

[27] S. Yuan, A. Fernando, and D. C. Klonoff, "Standards for Medical Device Cybersecurity in 2018," J. Diabetes Sci. Technol., vol. 12, no. 4, pp. 743–746, 2018, doi: 10.1177/1932296818763634.

[28] B. B. Zaidan, A. Haiqi, A. A. Zaidan, M. Abdulnabi, M. L. M. Kiah, and H. Muzamel, "A Security Framework for Nationwide Health Information Exchange based on Telehealth Strategy," J. Med. Syst., vol. 39, no. 5, pp. 1–19, 2015, doi: 10.1007/s10916-015-0235-1.

[29] B. M. Nzyoka, D. M. Mugo, and S. M. Ng'ang'a, "Medical Device Integration with Electronic Health Records: A Case Study of University of Nairobi Health Services, Kenya," Int. J. Comput. Technol., vol. 20, pp. 14–21, Jan. 2020, doi: 10.24297/ijct.v20i.8480.

[30] T. Webb and S. Dayal, "Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia," ScienceDirect, vol. 33, no. 4, pp. 559–563, Aug. 2017, doi: 10.1016/j.clsr.2017.05.004.

[31] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," J. Med. Internet Res., vol. 20, no. 5, p. e10059, May 2018, doi: 10.2196/10059.

[32] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure," IEEE Access, vol. 6, pp. 25167–25177, 2018, doi: 10.1109/ACCESS.2018.2817560.

[33] Herjavec Group, "The 2020 Healthcare Cybersecurity Report," pp. 1–5, 2020, [Online]. Available: www.herjavecgroup.com.

[34] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, no. April, pp. 48–52, 2018, doi: 10.1016/j.maturitas.2018.04.008.

[35] D. Zaldivar, L. A. Tawalbeh, and F. Muheidat, "Investigating the Security Threats on Networked Medical Devices," 2020 10th Annu. Comput. Commun. Work. Conf. CCWC 2020, pp. 488–493, 2020, doi: 10.1109/CCWC47524.2020.9031212.

[36] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks," Appl. Clin. Inform., vol. 7, no. 2, pp. 624–632, 2016, doi: 10.4338/ACI-2016-04-SOA-0064.

[37] L. Pycroft and T. Z. Aziz, "Security of implantable medical devices with wireless connections: The dangers of cyber-attacks," Expert Rev. Med. Devices, vol. 15, no. 6, pp. 403–406, Jun. 2018, doi: 10.1080/17434440.2018.1483235.

[38] U.S. Food and Drug Administration, "Medical Device Cybersecurity: What You Need to Know," FDA, Oct. 13, 2020. https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know (accessed Mar. 11, 2021).

[39] K. A. Seale, J. T. McDonald, W. B. Glisson, J. H. Pardue, and M. B. Jacobs, "Meddevrisk: Risk analysis methodology for networked medical devices," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2018-Janua, pp. 3271–3280, 2018, doi: 10.24251/hicss.2018.414.

[40] D. J. Bodeau, C. D. McCollum, and D. B. Fox, "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," Eccouncil, vol. 2507, no. 1, pp. 1–9, 2018, [Online]. Available: https://www.eccouncil.org/threat-modeling/.

[41] I. Stine, M. Rice, S. Dunlap, and J. Pecarina, "A cyber risk scoring system for medical devices," Int. J. Crit. Infrastruct. Prot., vol. 19, pp. 32–46, Dec. 2017, doi: 10.1016/j.ijcip.2017.04.001.

[42] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," Egypt. Informatics J., 2020, doi: 10.1016/j.eij.2020.07.003.

[43] C. R. Lyles, E. C. Nelson, S. Frampton, P. C. Dykes, A. G. Cemballi, and U. Sarkar, "Using Electronic Health Record Portals to Improve Patient Engagement: Research Priorities and Best Practices," Ann. Intern. Med., vol. 172, no. 11, pp. S123–S129, Jun. 2020, doi: 10.7326/M19-0876.

[44] G. Perera, A. Holbrook, L. Thabane, G. Foster, and D. J. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records," Int. J. Med. Inform., vol. 80, no. 2, pp. 94–101, 2011, doi: 10.1016/j.ijmedinf.2010.11.005.

[45] J. S. Ancker, M. Silver, M. C. Miller, and R. Kaushal, "Consumer experience with and attitudes toward health information technology: A nationwide survey," J. Am. Med. Informatics Assoc., vol. 20, no. 1, pp. 152–156, 2013, doi: 10.1136/amiajnl-2012-001062.

[46] A. Rao, N. Carreon Rascon, R. Lysecky, and J. W. Rozenblit, "Probabilistic Security Threat Detection for Risk Management in Cyber-Physical Medical Systems," IEEE Softw., 2018, doi: 10.1109/MS.2018.110165557.

[47] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF , COBIT , ISO / IEC 27002 and PCI DSS," Int. J. Inf. Vis., vol. 4, no. 4, pp. 225–230, 2020.

[48] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," Decis. Support Syst., vol. 108, pp. 57–68, 2018, doi: 10.1016/j.dss.2018.02.007.

[49] Ordr, "MEDICAL DEVICE SECURITY: WHY IT MATTERS, AND HOW TO GET IT," order, 2021. https://ordr.net/article/medical-device-security/.

[50] N. H. Lechner, "An Overview of Global Professional Publications Related to Medical Device cybersecurity," Cent. Eur. Conf. Inf. Intell. Syst., vol. 31, pp. 221–232, 2018, [Online]. Available: https://www.proquest.com/conference-papers-proceedings/overview-global-professional-publications-related/docview/2531366479/se-2?accountid=17242.

[51] J. Holdsworth, W. B. Glisson, and K. K. R. Choo, "Medical device vulnerability mitigation effort gap analysis taxonomy," Smart Heal., vol. 12, pp. 82–98, 2019, doi: 10.1016/j.smhl.2017.12.001.

[52] P. A. H. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," Med. Devices Evid. Res., vol. 8, pp. 305–316, Jul. 2015, doi: 10.2147/MDER.S50048.

[53] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," Int. J. Commun. Networks Inf. Secur., vol. 12, no. 3, pp. 417–432, 2020.

[54] S. Nifakos et al., "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," Sensors, vol. 21, no. 15, p. 5119, 2021, doi: 10.3390/s21155119.

[55] A. Sardi and E. Sorano, "Dynamic performance management: An approach for managing the common goods," Sustain., vol. 11, no. 22, pp. 1–22, 2019, doi: 10.3390/su11226435.

[56] M. M. Yusof, "A case study evaluation of a Critical Care Information System adoption using the socio-technical and fit approach," Int. J. Med. Inform., vol. 84, no. 7, pp. 486–499, 2015, doi: 10.1016/j.ijmedinf.2015.03.001.

[57] M. M. Yusof, J. Kuljis, A. Papazafeiropoulou, and L. K. Stergioulas, "An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit)," Int. J. Med. Inform., vol. 77, no. 6, pp. 386–398, 2008, doi: 10.1016/j.ijmedinf.2007.08.011.