Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/20252197

Cybersecurity Threats in Medical Devices: An Examination of Nursing Science, Role, and Patient Safety Interventions

Abdulrahman abdullah saif Alsahli [(1)] , Seham suleman hamd Alsaeed [(2)] , Fuad Moraia Mohammed Hakami [(3)] , Rawabi Hamdan Muklif [(4)] , Tagreead Gaman Al shrari [(5)] , Wssmiah Fahad ALsaad [(6)] , Ahlam ali alnami [(7)] , Samaria Ali Ali Mahnasi [(8)] , Kathiyh Jaman ALyami [(9)] , Aisha Hafiz Ibrahim [(10)] , Nesreen Hafiz Ibrahim [(10)] , Eman Hafiz Ibrahim [(10)]

(1) First District (Western Tuwaiq Health Centrr, Ministry of Health, Saudi Arabia,
(2) First District (Western Tuwaiq Health Centr) , Ministry of Health, Saudi Arabia,
(3) Iradah for mental health Jazan,Ministry of Health, Saudi Arabia,
(4) Maternity and Children's Hospital, Ministry of Health, Saudi Arabia,
(5) Tuwaiq Health center, Ministry of Health, Saudi Arabia,
(6) ALqwiaiah general Hospital, Saudi Arabia,
(7) Primary Health Care Center, Al-Sahafa, Ministry of Health, Saudi Arabia,
(8) Aldaar albayda' althaania PHC Riyadh, Ministry of Health, Saudi Arabia,
(9) First health cluster Riyadh, Ministry of Health, Saudi Arabia,
(10) Al murooj PHC, Ministry of Health, Saudi Arabia

Abstract

Background: The integration of networked medical devices with healthcare, while positive, has presented significant cybersecurity threats. These risks compromise device operation, patient data, and safety. Nurses, as heavy users of devices, are a critical but unaddressed line of protection against such threats.

Aim: The aim of this review is to synthesize literature between 2015-2024 to talk about cybersecurity threats in medical devices, assess nursing knowledge and preparedness, present evolving nursing roles, and examine strengthened patient safety practices.

Methods: A narrative review was conducted by conducting a systematic search on major scholarly databases (PubMed, CINAHL, Scopus) for English-language articles released during the time period 2015-2024. Keywords used were medical devices, cybersecurity, nursing, and patient safety.

Results: The review identifies an enormous gap in formal education related to cybersecurity among nurses, rendering them unprepared to recognize or handle threats. At the same time, nursing duties are informally broadened to incorporate cyber-hygiene activities. The findings bring attention to the imperative necessity of formalizing the role of a nurse as a frontline warrior against threats.

Conclusion: A formal integration of cybersecurity into nursing practice is urgently needed. This can be achieved through formalized educational frameworks, clear practice guidelines, and improved interdisciplinary cooperation in order to ensure patient safety in the technology era.

Keywords: medical device security, nursing informatics, patient safety, cybersecurity education, clinical governance.

1. Introduction

The modern system for delivering health care is integrally dependent on technology. The pervasive increase in smart, networked medical devices has brought with it astounding benefits like increased diagnostic accuracy, automated treatment interventions, and seamless data export into Electronic Health Records (EHRs). This Internet of Medical Things (IoMT) setting promises a new era of personalized and efficient care (Joyia et al., 2023). But this cyber-enabled revolution has a catastrophic vulnerability: the integrity of the medical devices themselves. These items are most often developed with use efficacy and clinical effectiveness as primary objectives, with security considerations addressed as an afterthought or in ways incompatible with clinical processes (Williams & Woodward, 2015).

Well-publicized incidents have demonstrated the actual risks. The 2017 WannaCry ransomware attack incapacitated parts of the United Kingdom's National Health Service (NHS), prompting rescheduling of appointments and diversion of emergency patients (Ghafur et al., 2019). More targeted attacks have shown the possibility of immediate damage, such as the theoretical possibility for malicious actors to hijack wireless infusion pumps to administer fatal amounts of medication (Jaipong et al., 2023). The United States Food and Drug Administration (FDA) has issued periodic safety communications regarding vulnerabilities in a wide

*Corresponding author e-mail: aalsahli@moh.gov.sa (Abdulrahman abdullah saif Alsahli).

Receive Date: 30 September 2025, Revise Date: 30 October 2025, Accept Date: 1 November 2025

variety of equipment, ranging from pacemakers and insulin pumps to surgical robots (FDA, 2019, 2023).

In this multi-dimensional threat landscape, nurses are the largest group of healthcare providers and the primary users of most point-of-care medical devices. Nurses are the first to identify device failure, data anomaly, and other unusual system behavior that could indicate a cybersecurity incident (Dart & Ahmed, 2023). Despite their pivotal position, education and ongoing professional development for nurses have been hesitant to incorporate cybersecurity principles. The discussion has primarily remained within IT and engineering communities, leading to a dangerous disconnect between the people who manage security and those who operate the devices on the frontlines of care (Ahmed, 2022). This review aims to bridge that gap by examining critically the intersection of medical device cybersecurity and nursing practice.

Methodology

This is a narrative literature review regarding cybersecurity threats in medical devices, i.e., the information, roles, and guidelines relevant to the nursing profession. Systematic searching across key academic databases, i.e., PubMed, CINAHL, Scopus, and Web of Science, was conducted. Keywords and Boolean operators employed: ("medical device" OR "infusion pump" OR "patient monitor" OR "IoMT") AND ("cybersecurity" OR "cyber security" OR "vulnerability" OR "hacking") AND ("nurs" OR "nursing knowledge" OR "nursing education" OR "clinical workflow") AND ("patient safety" OR "risk management" OR "clinical engineering"). The search was limited to English-language journals from 2015 to 2024 to capture the most up-to-date and relevant trends. Government and regulatory agency reports (e.g., the FDA, HHS, ENISA) and industry white papers relevant to the subject were also examined.

The first search return was over 300. Articles were filtered on title and abstract for relevance to the underlying themes. Studies that included only technical vulnerabilities without mentioning clinical implications or studies including hospital IT networks in general, without a specific focus on medical equipment or the nursing practice, were excluded. Out of 78 sources selected for full-text review, 40 of which are cited herein to support analysis and discussion. The findings are summarized into thematic sections below.

The Cybersecurity Vulnerability Environment of Medical Devices

Understanding the exact nature of cybersecurity vulnerabilities is the determining factor in comprehending the accompanying risk and defense needed. The incorporation of information technology into clinical activities has exposed medical devices to a range of general security vulnerabilities. These vulnerabilities usually arise from older systems designed for isolated usage without newer security functionality and from business demands in favor of rapid development and clinical functions rather than secure engineering (Vakhter et al., 2021). Chief weaknesses are exposed network services, by which improper access can be achieved and pivoted to critical devices like infusion pumps (Beavers & Pournouri, 2019); unencrypted data transport, by which eavesdropping and manipulation of patient information can be achieved (Roy et al., 2020; Zhong et al., 2022); and the prevalence of weak or hardcoded credentials, providing an easy attack path (Stern et al., 2019).

Besides, zero-day firmware and software vulnerabilities are a serious challenge, as patches require stringent testing and device downtime, contributing to major periods of known risk (Brantly & Brantly, 2020). Physical security is even a concern, as open ports facilitate the direct injection of malware (McLaughlin et al., 2009). The clinical implications of such vulnerabilities are severe and immediate and may involve unavailability of the device, integrity of data, confidentiality violated, and above all, the turning of a life-support device into a cause of injury by corrupting its core safety function (Jaipong et al., 2023).

Within this vulnerable setting, certain device models handled daily by nurses are particularly at risk due to their treatment or monitoring function and increased interconnectivity. Infusion pumps are a high-profile risk, with demonstrated vulnerabilities allowing remote attackers to alter drug libraries or alter doses of medication (Bracciale et al., 2023; McAlpine & VanKampen, 2011). Clinical team's eyes and ears, patient monitors can be hacked to display false vital signs that can induce inappropriate interventions or mask the deterioration of a patient (Xu et al., 2019). Ventilators and anesthetic machines, both life-sustaining devices, represent an immediate threat to life when hacked because cyber-attacks can alter tidal volumes or gas mixtures (Stern et al., 2019). Even implanted devices such as pacemakers and ICDs are not secure, with their wireless link being the potential entry point for an attacker to disable treatment or administer a lethal shock (Thielfoldt, 2022). Finally, networked point-of-care testing devices, such as blood glucose monitors, can produce tainted data that immediately leads to inappropriately managed clinical practice, e.g., incorrect insulin dosing (Ahmed, 2022). The overt linkage between these technical vulnerabilities and their immediate patient safety consequences is outlined in Table 1 and Figure 1.

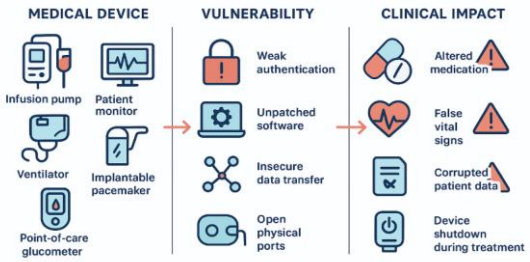

Figure 1: Cybersecurity Vulnerabilities in Common Medical Devices and Their Clinical Impact

Table 1: Common Medical Device Vulnerabilities and Immediate Patient Safety Consequences

Vulnerability Type	Example	Potential Patient Safety Impact	Relevant Nursing Observation
Weak Authentication	Default admin/password on a patient monitor.	Unauthorized access to change alarm limits or disable alarms.	Missed a critical event due to silenced alarms; unexpected changes to monitor settings.
Unpatched Software	Known vulnerability in an infusion pump's operating system.	Remote takeover of the pump to alter the infusion rate or dose.	Patient receives an under- or over-dose of medication; the pump behaves erratically.
Insecure Data Transfer	Unencrypted transmission of vitals from monitor to EHR.	Data interception and manipulation (e.g., spoofing a normal SpO2 for a hypoxic patient).	Clinical decision based on inaccurate data in the EHR; discrepancy between bedside monitor and central station/EHR.
Open Ports	Unprotected USB port on an anesthesia machine.	Introduction of malware that disrupts device operation.	Device failure or unexpected reboot during a procedure; strange error messages on screen.

Nursing Knowledge, Perceptions, and Role Transitions

The effectiveness of any frontline defense necessarily rests on its knowledge and awareness, and in medical device cybersecurity, nurses create a valuable human sensor network. However, the level of knowledge of the practice of nursing outlines a tremendous readiness gap that goes hand in hand with patient safety. There is a substantial body of evidence proposing that this knowledge gap is vast and persistent. Ground-breaking studies by Kruse et al. (2017) led the charge in outlining that while healthcare practitioners were alert to data protection, their knowledge of specific threat vectors and related practices for mitigation was severely limited. Alarming, therefore, are more recent figures to confirm that such disparity remains largely unsettled. In 2022, a survey of more than 500 U.S. nurses found that less than 30% had ever had any education at all on medical device cybersecurity, and more than 70% were unable to give typical indicators that the device was compromised (Dart & Ahmed, 2023). It is significant to note that this lack of knowledge is not because of apathy but that nurses are highly attuned to their widespread duty of patient safety, but feel largely ill-equipped to deal with the complexities of cyber-risks, becoming a situation of anxious helplessness (Kamerer & McDermott, 2020; Brown et al., 2021).

The pathogenesis of this ignorance is multimodal, rooted in systemic factors in practice and education. In the first place, traditional nursing education curricula are primarily packed with essential clinical, pharmacological, and pathophysiologic material with minimal room for the integration of health informatics, not to speak of the specialized niche field of cybersecurity (CIUCHI, 2022). Second, hospital training programs usually focus narrowly on overall data privacy needs, such as the needs of HIPAA and basic password hygiene, and do not touch on the unique architecture of operational technology (OT) environments and the specific indicators of compromise within medical devices (Brantly & Brantly, 2020). This is compounded by a general cultural and perceptual divide, where cybersecurity is routinely seen as the purview of the IT department, thus the development of operational silos that categorically exclude clinical staff from security-related considerations and planning (Coventry & Branley, 2018).

This general lack of awareness has concrete and dangerous consequences for clinical practice. Without training to recognize digital red flags, nurses may unintentionally become vectors for security breaches. For example, unusual device behavior—like an unplanned reboot of an infusion pump, a patient monitor showing gibberish data, or an abrupt slowdown of the entire network—is too frequently shrugged off as a simple "technical glitch" instead of being explored as a possible cyber-incident (McAlpine & VanKampen, 2011). Moreover, poor cyber-hygiene practices like the use of unauthorized USB drives, hooking up personal cell phones to medical equipment charging stations, or writing down passwords at nursing stations become the standard, inviting easily preventable risks (McLaughlin et al., 2009). Perhaps most significantly, when unplanned incidents occur, the ambiguity around the correct reporting mechanism—Clinical Engineering, IT security, or unit management—is to blame for causally significant delays in investigation and containment, allowing threats to propagate (Brown et al., 2021). The result is an objectively compromised organizational security posture where the very people most likely to be threatened are least prepared to defend against it and thus producing a weak point in the patient safety chain.

Concurrently, and at times without open recognition, the increasingly threatening environment is both implicitly and explicitly redefining the bedside nurse's role and responsibilities and adding duties critical to cyber-hygiene and organizational resilience to their portfolio. The most critical evolution is the role of the nurse as first responder and human sensor to

technological anomaly. In analogy with assessing patient deterioration, nurses now need to assess for signs of technological deterioration (Dart & Ahmed, 2023). It requires being vigilant for equipment malfunctioning outside normal parameters and considering a cyber-attack as a possible underlying cause of mechanical failure. It also needs real-time data integrity validation, for instance, cross-verifying bedside monitor and Electronic Health Record (EHR) heart rates and accepting discrepancies as potential data manipulation rather than sync errors (Xu et al., 2019). Finally, it involves reporting the suspicious behavior formally and in detail through the proper incident response mechanism, including forwarding the necessary forensic information for the security team to investigate (CIUCHI, 2022).

Aside from this sentinel role, nurses are essentially charged with a specific set of routine operational duties having substantive security implications. Such routine practices that are embedded in routine procedures constitute the building blocks of clinical cyber-hygiene. Credential administration, including adherence to robust, unique password policies and an absolute prohibition against credential sharing, is a fundamental safeguard. Similarly, simply logging off from workstations and devices is a widely overlooked but serious security protocol (Coventry & Branley, 2018). Physical protection of the device, such that medical devices are not left alone in public areas where they can be physically tampered with, and the immediate reporting of stolen or lost assets, is another critical nursing role (Williams & Woodward, 2015). Also, the nurses must be made part of and cognizant of the critical need for patching and update processes, integrated together with planned device downtime despite the immediate disruption to the clinical process (Dutta, 2017). The nurse's duty is also increasing beyond the confines of hospital walls. As more people utilize personal connected health devices, education of patients is increasingly being delivered by nurses, teaching patients how to use insulin pumps and continuous glucose monitoring safely and warning them of threats like health-data-related phishing attacks (Thielfoldt, 2022). Moreover, nurses professionally have the duty of being patient advocates by contesting the safety and usability of the devices they are required to use and calling for cybersecurity to be a paramount consideration in clinical technology procurement and implementation processes (George & George, 2023). The scope of this career shift is summarized in Table 2 and Figure 2.

Table 2: The Evolution of Nursing Responsibilities in the Context of Medical Device Cybersecurity

Domain of Responsibility	Traditional Nursing Role	Evolving Cybersecurity-Informed Role
Device Operation & Monitoring	Operate the device for clinical purposes; respond to clinical alarms.	Operate device securely; identify and report *cyber-anomalies* (e.g., unexpected reboots, strange screen messages, data discrepancies).
Patient Assessment	Assess patient condition based on clinical signs and device data.	Assess the *veracity of device data* as part of the clinical picture; trust but verify when data seems incongruent.
Documentation & Communication	Document patient data and care provided in the EHR.	Accurately report and document suspected device malfunctions or anomalies for IT/Engineering investigation.
Infection Control	Practice aseptic technique to prevent biological infections.	Practice "digital hygiene" (e.g., no unauthorized USBs, proper logout) to prevent malware infections.
Patient Education	Educate on disease management and medication use.	Educate patients on the secure use of their personal connected medical devices.

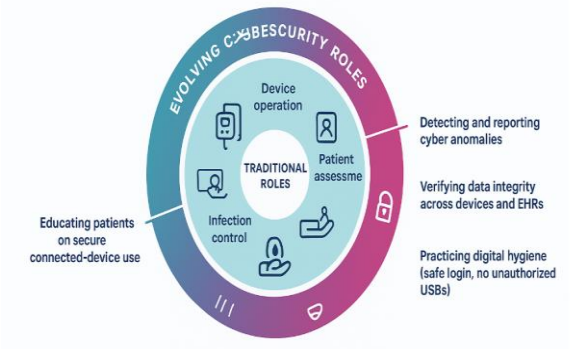

Figure 2: The Expanded Role of Nurses in Safeguarding Medical Device Cybersecurity

Strengthening Patient Safety Protocols with a Cybersecurity Lens

Patient safety protocols are the floor-level basis of nursing practice, and exploring these well-established protocols through a cybersecurity lens is a pragmatic way of developing systemic resilience without needing a complete and disruptive overhaul of existing workflows. One of the pathways to pursuing this convergence is to introduce specific cybersecurity considerations to established safety checks. For instance, the initial "Five Rights" of drug administration can be complemented by an additional "Right Device" verification. This would involve the nurse ensuring that the smart infusion pump is not only running but also operating in a healthy manner from a

cybersecurity perspective, which may include ensuring an active security certificate is present and ensuring the drug library is the correct, uncompromised version to prevent dosing errors resulting from malicious intervention (Newaz et al., 2021).

Moreover, standard procedure habits like patient safety huddles and shift reporting can be employed to increase collective awareness by incorporating a "technology status" report. Mentioning that a ventilator has a pending critical security update or that certain patient monitors have been experiencing anomalous network instability primes the incoming shift to be aware of the same quirks (Siegel et al., 2020). Of comparable importance is the rationalization of incident reporting systems to move beyond generic "device malfunction" categories. These need to be supplemented with more detailed sub-categories distinguishing between suspected mechanical failure, software failure, and potential cybersecurity events because this quality information is priceless in pattern recognition and proactive risk management by clinical engineering and IT security teams (Athinaiou, 2022).

Besides simplifying regular checks, health care facilities must develop and drill cyber-specific emergency procedures to the same degree of seriousness as for fire or heart attack. Nurses' roles in such backup procedures must be elaborately outlined and drilled. One of the support columns of such protocols is failover to manual modes of care, including training and specific guidelines for rapid fallback to manual blood pressure cuffs, pulse oximeters, and manual IV drip rates in the event that networked equipment is not available or is failed (Gernhardt & Groš, 2022). Alongside such clinical adaptation, a pre-discussed and well-communicated communication chain is required to ensure that a pointed cyber-incident initiates an immediate and concerted action by Clinical Engineering, IT Security, and hospital administration without bypassing essential clinical decision-makers (Coventry & Branley, 2018). To ensure competence and prevent panic in a real event, such cyber-specific response protocols should be validated through regular drills and simulations. Incorporating cyber-attack simulations into hospital-wide drills acclimates the entire clinical team to a unified endeavor, generating muscle memory and establishing roles in pressure (Park et al., 2023).

Recommendations and Future Directions

Addressing the complex issues of concern within this review requires collaborative, multi-stakeholder action across academia, clinical practice, healthcare administration, and the medical technology industry. Each significant group is framed with recommendations to forge a shared defense. Nursing professional development and education require a paradigm shift to bridge the widespread knowledge gap. Firstly, undergraduate and graduate nursing programs will integrate digitally oriented core concepts of digital health and cybersecurity into their own core curricula in an organized manner. Such programs must extend beyond theory to encompass operational realities of medical device operation, common vulnerabilities, and the role of the nurse in mitigation of clinical risk (Athinaiou, 2022; Dart & Ahmed, 2023). Secondly, to satisfy the current workforce's needs, professional nursing organizations and hospitals must develop and offer compulsory, ongoing, role-specific continuing education. These modules would be very hands-on in nature, employing case studies and simulation according to the local clinical threat and devices (George & George, 2023). Finally, an effort needs to be made to progress advanced certification in nursing informatics and facilitate nursing professional organizations to back the formal endorsement of cybersecurity-related responsibilities in official scope-of-practice documents to legitimize and standardize this new role (Siegel et al., 2020).

For policymakers and healthcare organizations, priority should be given to creating an enabling environment that empowers the clinical frontline. This begins with encouraging robust, interprofessional collaboration by establishing formal channels—such as shared committees and joint incident response teams—that unite nursing management, clinical engineering, and IT security in the coproduction of policy and procedure (Kioskli et al., 2021). Furthermore, security needs to be workflow-based; IT and security policy needs to be tried and tested for clinical use to be convenient and intuitive. Unduly burdensome procedures that impede care for patients will eventually be circumvented by staff, eventually compromising security (Williams & Woodward, 2015). Tactically, healthcare organizations must leverage their purchasing power by incorporating cybersecurity as a prime focus of the procurement process, mandating transparent evidence of secure development processes from vendors and preferential treatment of devices with robust, yet easy-to-manage, security features (FDA, 2023).

Finally, the regulatory agencies and device manufacturers have an inherent responsibility to build security into the very essence of medical technology. Regulatory agencies like the U.S. Food and Drug Administration must keep simplifying and enforcing pre-market guidance and post-market surveillance, making manufacturers demonstrate a "security-by-design" culture from inception to a device's lifecycle end (FDA, 2023). Manufacturers, in response, must innovate to have secure and effective patching mechanisms. They have to develop patches that impact the clinic as minimally as possible and do not incur excessively long downtime for verification, thereby closing the window of exposure that is so vulnerable between the discovery of a vulnerability

and having it remediated in the clinic (Vakhter et al., 2022).

Conclusion

Healthcare digitization is irreversible and, largely, good. Yet, despite widespread concerns about cybersecurity threats from the Internet of Things, the cybersecurity risks inherent in networked medical devices are a clear and present threat to patient safety. This review has confirmed that nurses, as the chief users and guardians of these devices, hold a uniquely strategic role within the healthcare cybersecurity environment. But an entrenched knowledge gap combined with an absence of formalized training leaves this front-line defense unprepared. The roles of nurses are already adapting in practice to add cyber-hygiene and threat detection duties, but this change has not been explicitly underpinned by education, policy, or procedure.

In order to protect patients in the digital age, cybersecurity must be formally incorporated into the fabric of nursing practice. This calls for a concerted effort to educate the current and future nursing workforce, to redefine clinical activities and safety practices to include cyber-threats, and to break down silos between clinical, engineering, and IT disciplines. With education for nurses, policy clarity, and a seat at the security table, the health care profession can mobilize its largest workforce into its greatest human firewall to protect the promise of medical technology from being breached by its vulnerabilities.

References

1. Ahmed, N. B. (2022). *Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience* (Doctoral dissertation, IMT-MINES ALES-IMT-Mines Alès Ecole Mines-Télécom).
2. Athinaiou, M. (2022). *Model-based Management of Cyber Resiliency for Healthcare Systems* (Doctoral dissertation, University of Brighton).
3. Beavers, J., & Pournouri, S. (2019). Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. In *Blockchain and clinical trial: Securing patient data* (pp. 249-267). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-11289-9_11
4. Bracciale, L., Loreti, P., & Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. *Scientific reports*, *13*(1), 19509. https://doi.org/10.1038/s41598-023-45927-1
5. Brantly, A. F., & Brantly, N. D. (2020). Patient-centric cybersecurity. *Journal of Cyber Policy*, *5*(3), 372-391. https://doi.org/10.1080/23738871.2020.1856902
6. Brown, L., Horvath, L., & Stevens, D. (2021). World Leaders on Covid-19: A text corpus of leaders' response and personality trait predictions. https://hdl.handle.net/10871/125317
7. CIUCHI, C. (2022, April). Developing a comprehensive model for digital lifelong learning using cyber resilience framework. In *Proceedings of the International Conference on Cybersecurity and Cybercrime-2022* (pp. 105-112). Asociatia Romana pentru Asigurarea Securitatii Informatiei.
8. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008
9. Dart, M., & Ahmed, M. (2023). Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed Methods Study. *JMIR Human Factors*, *10*(1), e48220. https://doi.org/10.2196/48220
10. Dutta, S. (2017). *Striking a balance between usability and cyber-security in IoT devices* (Doctoral dissertation, Massachusetts Institute of Technology). http://hdl.handle.net/1721.1/113508
11. Food and Drug Administration (FDA). (2019). *Content of premarket submissions for management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff*. U.S. Department of Health and Human Services. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
12. Food and Drug Administration (FDA). (2023). *Cybersecurity in medical devices: Quality system considerations and content of premarket submissions*. U.S. Department of Health and Human Services. https://www.fda.gov/media/119933/download
13. Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ digital medicine*, *2*(1), 98. https://doi.org/10.1038/s41746-019-0161-6
14. George, A. S., & George, A. H. (2023). The emergence of cybersecurity medicine: protecting implanted devices from cyber threats. *Partners Universal Innovative Research Publication*, *1*(2), 93-111. https://doi.org/10.5281/zenodo.10206563
15. Gernhardt, D., & Groš, S. (2022, May). Use of a non-peer reviewed sources in cyber-security scientific research. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1057-1062). IEEE.

https://doi.org/10.23919/MIPRO55190.2022.9803478

16. Jaipong, P., Siripipattanakul, S., Sriboonruang, P., Sitthipon, T., Jaipong, P., Siripipattanakul, S., ... & Sitthipon, T. (2023). A review of metaverse and cybersecurity in the digital era. *International Journal of Computing Sciences Research*, *7*, 1125-1132.
17. Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.*, *12*(4), 240-247.
18. Kioskli, K., Fotis, T., & Mouratidis, H. (2021, August). The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. In *Proceedings of the 16th international conference on availability, reliability and security* (pp. 1-9). https://doi.org/10.1145/3465481.3470033
19. Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, *10*(4), 48-53. https://doi.org/10.1016/S2155-8256(20)30014-4
20. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. https://doi.org/10.3233/THC-161263
21. McAlpine, B., & VanKampen, D. (2011). Clinical engineering and information technology: working together to implement device integration. *Biomedical Instrumentation & Technology*, *45*(6), 445-449. https://doi.org/10.2345/0899-8205-45.6.445
22. McLaughlin, S., Podkuiko, D., & McDaniel, P. (2009, September). Energy theft in the advanced metering infrastructure. In *International Workshop on Critical Information Infrastructures Security* (pp. 176-187). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14379-3_15
23. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, *2*(3), 1-44. https://doi.org/10.1145/3453176
24. Park, O., Jeon, M., Kim, M., Kim, B., & Jeong, H. (2023, October). The Effects of a Simulation-Based Patient Safety Education Program on Compliance with Patient Safety, Perception of Patient Safety Culture, and Educational Satisfaction of Operating Room Nurses. In *Healthcare* (Vol. 11, No. 21, p. 2824). MDPI. https://doi.org/10.3390/healthcare11212824
25. Roy, M., Chowdhury, C., & Aslam, N. (2020). Security and privacy issues in wireless sensor and body area networks. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms* (pp. 173-200). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-22277-2_7
26. Siegel, E., Glaeser, E. L., Kozyrkov, C., & Davenport, T. H. (2020). *Strategic Analytics: The Insights You Need from Harvard Business Review*. Harvard Business Press.
27. Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: an analysis of FDA product summaries. *BMJ open*, *9*(6), e025374. https://doi.org/10.1136/bmjopen-2018-025374
28. Thielfoldt, K. (2022). *Internet of medical things cybersecurity vulnerabilities and medical professionals' cybersecurity awareness: a quantitative study* (Doctoral dissertation, Colorado Technical University).
29. Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2021). Security for emerging miniaturized wireless biomedical devices: threat modeling with application to case studies. *arXiv preprint arXiv:2105.05937*. https://doi.org/10.48550/arXiv.2105.05937
30. Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2022). Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet of Things Journal*, *9*(15), 13338-13352. https://doi.org/10.1109/JIOT.2022.3144130
31. Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305-316. https://doi.org/10.2147/MDER.S50048
32. Xu, C., Wang, N., Zhu, L., Sharif, K., & Zhang, C. (2019). Achieving searchable and privacy-preserving data sharing for cloud-assisted E-healthcare system. *IEEE Internet of Things Journal*, *6*(5), 8345-8356. https://doi.org/10.1109/JIOT.2019.2917186
33. Zhong, L., He, S., Lin, J., Wu, J., Li, X., Pang, Y., & Li, Z. (2022). Technological requirements and challenges in wireless body area networks for health monitoring: A comprehensive survey. *Sensors*, *22*(9), 3539. https://doi.org/10.3390/s22093539