Cyberbiosecurity in Healthcare: Securing Medical Devices from Digital and Biological Threats

Valentine Okpalanozie[1], Abuh Ibrahim Sani[2], Oluwaseyi Adeleye[3], Fatimah Eniafe[4], Raheemat Adefabi[5], Oludolamu Onimole[2], Jude Osamor[6], Xavier Palmer[7] and Lucas Potter[7]

[1]TMF, Lagos, Nigeria
[2]University of Bradford, UK
[3]Federal University of Technology, Akure, Nigeria
[4]DJA, Lagos, Nigeria
[5]Teesside University, Middlesbrough, UK
[6]Cyblack
[7]BiosView, USA

valentineokpalanozie@gmail.com
saniabuh@gmail.com
oludolamuonimole@gmail.com
adeleyeoluwaseyiadedoyin@gmail.com
omobolanlezara@gmail.com
raheematopeyemi@gmail.com
jude.osamor@ieee.org

Abstract: Technological innovations constantly transform, and these transformations extend over all sectors of life, irrespective of the original innovation's purpose. Due to the need for constant improvements in patient care, new technology is commonly applied to healthcare environments. As the transformation keeps emerging, it, in turn, creates more attack vectors because of the interconnectivity in these devices. These interconnectivity features are why they are called smart devices. The smart device explains why they can connect to networks, process data, and interact intelligently with their environment and users. As these devices create attack vectors due to their interconnectivity, so do we have to pay attention to these attack vectors. Effects of biological data falling into the wrong hands should be of concern in the health sector due to its potential effect on the health of a patient and on the reputation of the health organization. Efforts have been made to safeguard data in the health sector, like the HIPPA framework, designed to protect sensitive patient health information. But there is a need to go beyond focusing on just personal data to broader aspects of the health sector, like cyber threats in medical devices. While cyberbiosecurity literature exists in industries like maritime, food and agriculture, no consideration has been given to the health sector. With the innovations in medical devices, there is a need for a nexus between cybersecurity and biosecurity, to maximize their abilities to tackle the loopholes created by this technological development. Cyberbiosecurity bridges this gap by shifting the focus on how to secure the different aspects of these devices like the software, firmware, and hardware. This research explores the emerging field of cyberbiosecurity by outlining the key digital and biological threats in medical devices and implications, challenges in securing medical devices and propose a framework for solid cyberbiosecurity practices to mitigate the risk in medical devices

Keywords: Cyberbiosecurity, Medical devices, Biological data protection, Healthcare cybersecurity, Interconnected smart devices

1. Background

Networked health technology is becoming increasingly essential in healthcare. Connected health technologies help patients, healthcare professionals, and health authorities make better-informed healthcare decisions and improve health outcomes (Awad, S. et al., 2023). This allows healthcare to extend beyond traditional clinical settings, reaching homes, workplaces, and travel locations, while providing patients with care that integrates seamlessly into their daily lives (Kumar et al., 2023). While internet-connected medical devices offer significant benefits, they also introduce substantial security and privacy risks, especially as healthcare systems handle sensitive and critical medical data (Sana, 2024). The Internet of Medical Things (IoMT) devices are particularly vulnerable due to their widespread use and relatively underdeveloped security measures (Thomasian & Adashi, 2021; Affia et al., 2023). For instance, in 2017, the FDA issued warnings about the possibility of a pacemaker being hacked with its battery depleted or incorrect pacing pulses being delivered (George and Hovan George, 2023). Cybersecurity researcher Jay Radcliffe demonstrated how possible and simple it was to compromise the integrity of the device by breaking into his own implanted insulin pump device and changing the insulin parameters. Going a step further, Jack Barnaby showed the possibility of hacking the insulin pump and injecting a deadly dosage of insulin into a mannequin's pancreas (Torgersen et al., 2024)

The security landscape for connected medical devices is influenced by various frameworks and regulations designed to mitigate risks and ensure compliance. For example, HIPAA regulations require healthcare providers to implement administrative, physical, and technical safeguards to protect patient data (Abbasi & Smith, 2024). However, despite these existing frameworks, the rapid evolution of technology and the increasing complexity of cyber threats to medical devices highlight gaps in current measures. This emphasizes the need for a more comprehensive cyberbiosecurity approach that addresses both technological and biological aspects.

1.1 Problem Statement

1.1.1 Vulnerabilities in connected medical devices

The healthcare sector is utilizing digital advancements to improve patient experiences and outcomes, beginning with electronic health records (EHRs), database of patient health data and connected devices (Ali *et al.*, 2025). However, the integration of these connected medical devices, software, and networks results in increased vulnerabilities (Li *et al.*, 2023). Inaccurate diagnostic data from compromised connected medical devices could result in incorrect treatment choices, or in the case of implantable devices, could compromise patient safety by changing how therapy is administered (Jaime *et al.*, 2023). For example, Magnetic Resonance Imaging (MRI) machines and insulin pumps rely on software, firmware, and wireless connections to operate. However, they may also expose sensitive data and can be remotely manipulated, putting patients at risk (Bracciale et al., 2023).

1.1.2 Gap between cybersecurity and biosecurity

There is a significant gap in addressing Cyberbiosecurity risks due to a disconnect between biosciences and cybersecurity. Disagreements exist on terminology, boundaries of the field, and how it differentiates from related areas like cybersecurity and biosecurity (Greenbaum, 2023). In biosciences, awareness of the impact of cyberattacks on biological systems is limited, and there is a lack of a shared framework to tackle these risks. This leaves professionals unprepared, as there is also little specialised training for those in cybersecurity or biotechnology to handle Cyberbiosecurity challenges (Noran & Fouad, 2024). Addressing the cybersecurity needs of life sciences requires an interdisciplinary approach, complicated by biological systems' unique characteristics and vulnerabilities (Shankar et al., 2024). Additionally, there is a lack of a solid legal framework and strategy for cyber-biosecurity, which necessitates the development of comprehensive policies with proactive engagement from all stakeholders (Bhushan, 2023). There is also a need for stronger collaboration and investment across stakeholders to address the intersection of cybersecurity and biosecurity, with a focus on understanding and mitigating cybersecurity risks in the biotechnology sector (Greenbaum, 2023).

1.1.3 Need for integrated protection approach

Integrating cybersecurity and biosecurity measures is imperative to address vulnerabilities in connected medical devices. Recent research focuses on the need for cybersecurity by design in medical devices. Initiatives like "Cyber-Biosecurity by Design" integrate security throughout the device development lifecycle to address cyber threats effectively (Elgabry, 2023). There is also the need for integrated Cyberbiosecurity training, which includes cross-training in healthcare and cybersecurity. This emphasizes the necessity of a comprehensive protection approach to effectively prepare a proactive workforce against emerging threats (Adeoye et al., 2023)

This integrated approach would not only safeguard patient data but also ensure the reliability of medical device functions.

1.2 Study Aims and Scope

The primary aim of this research is to develop a comprehensive understanding of Cyberbiosecurity in the context of medical devices, focusing on how to protect both digital and biological data. This study will analyse the risks and vulnerabilities in connected medical devices and current security measures, while also exploring the gaps between existing cybersecurity and biosecurity frameworks. The scope will include discussion of regulatory challenges and emerging threats to propose an integrated protection model applicable to the healthcare sector.

2. Literature Review

2.1 Medical Devices and Security

2.1.1 Types of connected medical devices

Connected medical devices are smart objects intended for medical use that communicate via the internet with each other and other systems, providing real-time monitoring of patient's vitals, interactions, and medical

conditions. These devices offer numerous advantages, such as aiding doctors in making informed treatment decisions, improving patient outcomes, and reducing costs (Machal, 2023).

2.1.2 Risks associated with connected medical devices

According to Schwartz et al. (2018), connected medical devices offer numerous benefits but also pose significant risks to patient privacy and safety, as unauthorized access could expose sensitive data or control them, potentially endangering patients' lives. A large amount of sensitive patient information, such as health records, test results, and prescription doses, is collected and transmitted by these devices, making it an attractive target for cybercriminals (Machal, 2023). Malware attacks can disrupt device functionality, leading to incorrect dosages and therapy delays, as many devices lack cybersecurity features, making them highly susceptible to cyberattacks (Machal, 2023). Another critical concern is the breach of privacy. These devices handle vast amounts of sensitive data that must be carefully safeguarded to prevent misuse, which could lead to severe consequences (Ray, 2021).

Unlike unconnected smart medical devices, which require physical proximity for their vulnerabilities to be exploited, connected medical devices face the same cyber threats as other digital technologies (eHealth Initiative, 2019). In July 2019, the Department of Homeland Security (DHS) issued an advisory highlighting vulnerabilities in nearly 200 million devices, collectively referred to as URGENT/11 (eHealth Initiative, 2019). Three months later, the Food and Drug Administration (FDA) confirmed that certain medical devices were also susceptible to vulnerabilities detailed in URGENT/11 (eHealth Initiative, 2019).. This emphasizes the importance of adopting a threat-centric approach to securing the connected health ecosystem, as failure to do so could allow sophisticated attackers to covertly alter diagnostic or treatment data without detection.

2.1.3 Current security measures

Many have not prioritized security strategies or budgets, often due to a lack of understanding among management, insufficient funds, skill gaps, and regulatory complexities (Wilson & Rollman, 2022). In response, the FDA has taken proactive steps, notably in their 2014 guidance on cybersecurity in medical devices, which encourages manufacturers to address cybersecurity during premarket submissions by identifying assets, assessing vulnerabilities, and developing mitigation strategies (Wilson & Rollman, 2022).

Several other agencies within the U.S. Department of Health and Human Services play a role in keeping medical devices safe and secure (United States Government Accountability Office, 2023):

1. **The Centers for Medicare and Medicaid Services (CMS)** collaborates with public and private organizations to support FDA guidelines for securing legacy medical devices, which often lack modern cybersecurity protections.
2. **The Office for Civil Rights (OCR)** ensures that organizations handling medical device data comply with HIPAA regulations, protecting patient privacy and sensitive health information.
3. **CISA (Cybersecurity and Infrastructure Security Agency)** issues medical advisories on vulnerabilities, exploits, and cybersecurity threats affecting medical devices, helping healthcare providers stay ahead of emerging risks.
4. **NIST (National Institute of Standards and Technology)** develops standards, guidance, and cybersecurity frameworks to strengthen the healthcare sector's security, including protections for medical devices.

Together, these agencies work to ensure that medical devices remain both effective and secure in an increasingly digital world.

Frost & Sullivan (2019) predicts the addition of 20 to 30 billion medical devices in the healthcare sector, raising concerns about security policies for legacy devices (eHealth Initiative, 2019; Frost & Sullivan, 2019). New regulations have been introduced to enhance the security of these older devices, but replacing or re-certifying them can be costly and complex. Therefore, innovative strategies are essential to protect connected medical devices and ensure IoMT security (Frost & Sullivan, 2019).

2.2 Cyberbiosecurity Framework

The cyberbiosecurity framework is a systematic, interdisciplinary methodology that addresses the unique security concerns emerging at the convergence of cyberspace, biosecurity, and biotechnology (Bhushan, 2023).

2.2.1 Concept definition and scope

According to Bhushan (2023), cyber-biosecurity is understanding vulnerabilities in integrated life and medical sciences, cyber systems, supply chains, and infrastructure systems. It involves preventing, safeguarding against, mitigating, investigating, and attributing threats for security, competitiveness, and resilience. Digitization in biological research and healthcare is crucial to protect sensitive information (Bhushan, 2023; Tomulescu, 2020). Cybersecurity involves safeguarding electronic data, systems, and networks. Cyberbiosecurity represents a critical application, concentrating on preventing illicit intrusions and activities while protecting data, information, and online resources related to life sciences, medicine, health, agriculture, and food sciences (Duncan, 2019). This approach integrates cybersecurity and biosecurity concepts, addressing the complexity of biological systems and ethical considerations.

2.3 Integration Opportunities in Healthcare

The use of cyberbiosecurity in healthcare presents opportunities to enhance the security and resilience of medical systems and data. A crucial aspect is the safeguarding of genomic data, essential for individualized therapeutics (Fouad, 2024). According to Elgabry (2023), cyberbiosecurity ensures the confidentiality and integrity of data during its sharing and storage across research networks and cloud platforms. Medical IoT devices, including pacemakers, insulin pumps, and connected diagnostic instruments, are a primary emphasis, where cyberbiosecurity mitigates illegal access and improves device reliability, hence protecting patient safety (Fouad, 2024).

In healthcare infrastructure, biomanufacturing systems are tailored to medicine production, and laboratory automation is enhanced by cyberbiosecurity tools that protect against manipulation and disturbances (Bhushan, 2023). Telemedicine platforms and remote health monitoring systems can be enhanced to protect patient privacy and HIPAA standards, while cyberbiosecurity mitigates vulnerabilities in healthcare research laboratories, safeguarding proprietary data and systems (Fouad, 2024). Integrating cyberbiosecurity enables healthcare systems to bolster confidence, comply with regulatory standards, and reduce risks in a swiftly changing digital and biological environment.

3. Methodology

3.1 On Device Analysis and Threats

Cybersecurity priorities for medical systems differ and relate to deployment. Confidentiality is a priority for hospital systems, preventing data breaches, or ransomware (which can also impact the availability of systems if made unusable by encryption). Protection of the individual is a priority when patients are exposed to medical devices as part of their care, including implantable devices. Availability of such devices is a priority. 'Non-medical' or wellbeing devices, such as fitness trackers, also have confidentiality as a priority, albeit with much lower impact. (Stouffer et al., 2015)

Risk evaluation methodology:

The proliferation of electronic computing (e.g., software), networking, and wireless communication technologies necessitates cybersecurity. Many of today's medical devices and healthcare systems use or rely on electronic technologies, which means they must address cybersecurity.

Per FDA guidance, "Cybersecurity is preventing unauthorized access, modification, misuse, or denial of use, or the unauthorized use of information stored, accessed, or transferred from a medical device to an external recipient. (Food and Drug Administration, 2015). Cybersecurity analysis involves understanding the following:

- What needs to be protected (i.e., assets).
- What threats (and attacks) are potentially applicable?
- What are the potential cybersecurity harms and associated effects of an exploit, and how is security harm connected to safety risk?
- What are the potential scenarios (i.e., system vulnerabilities) that expose assets to the threats?
- What are the potential causes (e.g. conditions, events) can result in system vulnerabilities?
- What cybersecurity risk controls are needed to protect the assets and mitigate risks
- How is cybersecurity risk connected with safety risk?

Identifying and Protecting Assets

Cybersecurity asset identification for a medical device can start with identifying the electronic information that must be protected based on the device's intended use. The electronic information for a medical device can fit into one or more of the following categories: network-communicated information, health information, software information, and information that may need protection from a business perspective. These categories help to ensure adequate coverage and do not need to be orthogonal. Although there could be multiple layers of other systems, subsystems, and components that ought to be protected from a cybersecurity perspective, identifying the electronic information that ultimately needs to be protected would be beneficial. During the development of a new medical device, this asset identification process should take place as early as the product concept phase, just as the safety risk management process should proactively identify the different groups of people and environments with which the device may interact so that their safety can be considered in the risk analysis. (Wu & Kusinitz, 2015).

Risk Control via Proactive Detectability and Recovery

The purpose of cybersecurity is to protect electronic information assets, which can be less noticeable when compromised compared to physical damage. Unlike users who report adverse events with medical devices, hackers typically do not disclose their malicious actions, highlighting the need for effective detection and recovery from cyber threats. This should be integrated into device design, featuring capabilities to log and respond to cyber compromises, as well as methods for configuration recovery by authorized personnel. Current medical device complaint processes are largely reactive, while postmarket cybersecurity should focus on proactive monitoring of potential attacks or incidents (Association for the Advancement of Medical Instrumentation, 2012).

3.2 Framework Development

3.2.1 Security control design

So far, different threats that can affect the healthcare sector via connected medical devices have been mentioned. Conscious efforts should be made to prevent these threats from escalating from threats to actual attacks, and one way of doing this is to map out security control designs to prevent such events from happening.

Input Validation: In hospitals, some connected devices require the input of some data to function. If a threat actor maliciously takes control of such devices, he or she can engineer a database injection attack by inputting the wrong character to destabilise the database. Preventing such an event requires implementing proper input validation on medical devices.

Timestamp Requests and Encryption: One key characteristic of smart devices is their ability to communicate with one another due to their connectivity. To prevent threat actors from exploiting this communication—such as in a replay attack—implementing timestamp requests is essential. By configuring a limited time window, measured in seconds, for communication between two devices, we can help thwart replay attacks. This approach ensures that an attacker does not have sufficient time to redirect the communication to their own network. Similarly, encryption is vital for securing the communication between connected medical devices. Secure encryption methods, such as HTTPS or TLS, are necessary to protect the confidentiality of the data transmitted by these devices. Additionally, implementing device and IP verification can enhance the monitoring of communications between devices. This layer of security makes it easier to detect any intrusions during the monitoring process.

Employee Training: One of the weakest links in securing digital assets is humans, whose psychological vulnerabilities can be exploited through attacks like phishing, vishing, and social engineering. In healthcare, these vulnerabilities are especially concerning due to the operation of connected medical devices, where successful attacks can lead to unauthorized access. Employee training is an effective control measure, teaching staff what information is appropriate to share and how to identify and respond to scams, thereby reducing social engineering incidents. Access control is also crucial for security. Attacks using malicious code, such as Trojan horses or ransomware, often succeed due to unintended user actions. Implementing a robust access control strategy, like the principle of least privilege, can minimize these risks by granting users only the permissions necessary for their roles. This limits the potential impact of inadvertent attacks and reduces the chances of lateral movement within the organization, protecting sensitive information from unauthorized access.

Rate Limiting: One of the ways to overwhelm a server is by sending a large number of requests simultaneously, thereby preventing the server from responding to legitimate requests and shutting down. A malicious actor can

engineer Denial of Service (DOS) in a hospital by using a tricky method, like social engineering, to get into the internal network, thereby obstructing normal activities, which can result in total shutting down of critical services completely, just as the case of the 2019 ransomware attack on Alabama's DCH Health System (Heimdal Security, n.d.). The shutdown of such a server can lead to loss of life because it can affect some patients who need immediate medical attention. Availability of servers and devices in healthcare is paramount, and one way to ensure such availability is to implement rate limiting.

These secure controls will ensure that smart medical devices communicate securely and are not susceptible to attack. Even when they are, the effect is minimal and can be contained immediately.

Implementation strategy: The implementation strategy outlines the practical application of recommended solutions to mitigate vulnerabilities in connected medical devices. Careful planning is essential in the initial phase, which begins by identifying key stakeholders, including IT teams, medical professionals, and device manufacturers. To ensure a comprehensive understanding of potential threats, an initial risk assessment is conducted to analyze the existing infrastructure and identify specific vulnerabilities. This assessment helps create a detailed roadmap that defines each participant's roles and responsibilities and establishes reasonable deadlines. Once the planning phase is complete, the deployment phase begins. This phase includes organizing staff training programs that feature customized awareness workshops and simulated phishing tests to address social engineering threats. To protect device communications, multi-factor authentication and secure encryption protocols, such as HTTPS and TLS, are implemented. Role-based access control (RBAC) and least privilege policies are established to manage permissions effectively. Additionally, monitoring systems are put in place to log and review device interactions, and mechanisms such as timestamping are added to prevent replay attacks.

Cyber Risk Mitigation Framework for Protecting Digital and Biological Data in Medical Devices.

Security Control Measure	Description	Impact Mitigation	Implementation Strategy	Stakeholders Responsible
Input Validation	Ensures only correctly formatted information is allowed.	To prevent SQL injection, buffer overflow attacks.	Validate whitelists and blacklists Sanitise using regex patterns.	All Employees IT Security
Time Stamp Request and Encryption	Ensures data integrity and confidentiality	To prevent replay attacks	Use TLS encryption for all device communications. Use digitally signed timestamps on logs.	IT Security Network Admins
Employee Training	Educates employees about cybersecurity best practices.	Reduces risk of phishing attack Protect against insider threats.	Provide frequent cybersecurity awareness training Regularly Practice simulated phishing operations	All Employees
Rate Limiting	Controls request frequency to prevent attack	Protect against DDoS attacks, brute-force attempts	Implement API rate limitation. Enforce login attempt limitations.	IT Security

Validation approach: The validation approach guarantees that the measures implemented reduce risks associated with connected medical devices and produce the intended results. This entails establishing success metrics, evaluating the reliability of the solutions implemented, collecting information, and continuously improving the plan.

Certain metrics are established to gauge success, failure, or areas for improvement. Assessments conducted before and after training are used to gauge staff knowledge gains to gauge the effectiveness of security awareness programs. While system resilience is evaluated by comparing downtime brought on by cyberattacks before and following implementation, incident reduction is determined by tracking the number of reported security incidents.

The above measures' efficacy is confirmed through testing techniques. Penetration testing evaluates the strength of authentication procedures, encryption protocols, and access controls by simulating cyberattacks. On the other hand, stress testing assesses how resilient systems are to DoS attacks, while phishing simulations test how well employee training works against social engineering attempts. Validation relies heavily on data collection and analysis. Monitoring tool logs are examined to spot questionable activity and new patterns, and incident reports are examined to determine how frequently and seriously breaches occur. User feedback is obtained via surveys to assess the controls' usability and practicality and ensure they meet real-world requirements. Finally, post-implementation performance is compared against benchmarks or industry standards to assess overall effectiveness. This ensures that the implemented solutions are functional and continuously improved to address evolving threats.

4. Discussion and Conclusion

4.1 Framework Effectiveness

The framework proposed in this article has indicated how the healthcare industry can reduce threats associated with medical devices from becoming an attack and protect organizational reputation. The technique focuses on proactive post-market cybersecurity monitoring as well as intrinsic security control measures like input validation and timestamp encryption. These techniques ensure that vulnerabilities found in the healthcare medical devices such as database injection attacks, replay attacks, and unencrypted communications are not only detected but also remedieted. Furthermore, outlining potential cyber threats in medical devices fulfilled the identification and mitigation objective which will help prevent these vulnerabilities from turning into a full-scale attack.

Benefits and limitations

The article outlines the advantages of implementing cyber biosecurity in healthcare, particularly in protecting healthcare devices. However, certain challenges may hinder healthcare organizations from fully realizing these benefits. Enhanced data security is analyzed as a way to reduce unauthorized access, data breaches, and cyberattacks within the healthcare industry. The integration of cybersecurity and biosecurity offers a holistic approach to addressing vulnerabilities in medical devices. The article underscores the necessity for healthcare organizations to take proactive measures, empowering them to stay ahead of potential threats instead of relying on reactive solutions. Some limitations of the proposed methodology include the complexity of implementation, which can be challenging for healthcare systems due to outdated infrastructure. While employee training is suggested as a solution, human errors persist despite such training. The effectiveness of training can vary, and not all personnel may consistently follow the established security protocols. Moreover, the rapid pace of technological advancements could render key components of the proposed framework outdated or inadequate, necessitating regular updates and modifications to keep pace with the evolving cyber landscape. Overall, the article primarily focuses on digital and biological data related to medical equipment, but it does not delve deeply into other aspects of healthcare cyber biosecurity, such as patient records or extensive hospital networks. Future exploration should focus on enhancing the flexibility, affordability, and scalability of cyber biosecurity solutions in the healthcare sector. This will ensure their effectiveness in protecting healthcare systems from evolving threats. Specifically, future studies should consider how artificial intelligence (AI) and machine learning (ML) can be leveraged for real-time detection and response to threats in connected healthcare devices. In conclusion, the article calls for a continuous effort to improve cyber biosecurity in healthcare, emphasizing the need for solutions that can adapt to the changing threat landscape.

5. Conclusion

The work explores the critical intersection of technological advancements and cybersecurity in healthcare, focusing on cyberbiosecurity. As smart medical devices become more integrated into networks, they create new vulnerabilities, highlighting the urgent need for comprehensive security measures. While these innovations enhance patient care, they also pose significant risks from cyber threats that can jeopardize both patient health and organizational reputation. This research notes the inadequate focus on cyberbiosecurity in healthcare compared to industries like maritime and agriculture. It proposes a framework to protect personal health information, and to secure the software, firmware, and hardware of medical devices. The study aims to identify key medical devices, the data they produce, the cyber threats they face, and the challenges in securing this data. Ultimately, it advocates for a holistic approach that integrates cybersecurity and biosecurity measures to better protect against evolving threats, ensuring patient safety and safeguarding healthcare organizations from the consequences of data breaches.

References

Abbasi, N., & Smith, D. A. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. *Journal of Knowledge Learning and Science Technology, 3(3),* 278. https://doi.org/10.60087/jklst.vol3.n3.p.278-287.

Adeoye, S.O. et al. (2023). Cyberbiosecurity Workforce Preparation: Education at the Convergence of Education at the Convergence of Cybersecurity and Biosecurity. *NACTA Journal, 67(1),* 341–350. https://doi.org/10.56103/nactaj.v67i1.151.

Affia, A.A.O., Finch, H., Jung, W., Samori, I.A., Potter, L., & Palmer, X.L. (2023). IoT health devices: Exploring security risks in the connected landscape. *IoT, 4(2),* 150-182.

Ali, T.E. et al. (2025). Trends, prospects, challenges, and security in the healthcare internet of things. *Computing, 107(1).* https://doi.org/10.1007/s00607-024-01352-4.

Association for the Advancement of Medical Instrumentation. (2012). ANSI/AAMI/IEC TIR80001-2-2:2012: Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks, and controls. Arlington, VA: Association for the Advancement of Medical Instrumentation.

Awad, S., Aljuburi, L., Lumsden, R. S., Mpandzou, M., & Marinus, R. (2023). Connected health in US, EU, and China: Opportunities to accelerate regulation of connected health technologies to optimize their role in medicines development. *Frontiers in Medicine.* https://doi.org/10.3389/fmed.2023.1248912.

Bhushan, M. (2023). Cyber-Biosecurity: An Emerging National Security Frontier. *Journal of Defence Studies, 17(2),* 93–119. https://idsa.demosl-03.rvsolutions.in/system/files/jds/jds-17-2_Mrinmayee-Bhushan.pdf.

Bhushan, M. (2023). Cyber-biosecurity. *Journal of Defence Studies, 17(2),* 93-119.

Bonomi, S., Santucci, G., Lenti, S., Sorella, M., Tanasache, F. D., Palleschi, A., Ciccotelli, C., & Magalini, S. (2020). Cyber-attacks and threats for healthcare – a multi-layer thread analysis. Paper presented at the *2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM),* 5705–5708. https://doi.org/10.1109/BIBM49941.2020.9313302.

Bracciale, L., Loreti, P., & Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. *Scientific Reports, 13(1).* https://doi.org/10.1038/s41598-023-45927-1.

eHealth Initiative. (2019). The challenges in securing connected medical devices.

Elgabry, M. (2023). Towards cyber-biosecurity by design: An experimental approach to Internet-of-Medical-Things design and development. *Crime Science, 12(1).* https://doi.org/10.1186/s40163-023-00181-8.

Food and Drug Administration. (2015). Content of premarket submissions for management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff. Available at: www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

Fouad, N.S. (2024). Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation. *European Journal of International Security,* 1-21.

Frost & Sullivan. (2019). Medical Device and Network Security - Coming to terms with the Internet of Medical Things (IoMT).

George, A.S., & Hovan George, A.S. (2023). The Emergence of Cybersecurity Medicine: Protecting Implanted Devices from Cyber Threats. https://doi.org/10.5281/zenodo.10206563.

Greenbaum, D. (2023). The Convergence of Biotechnology and Cybersecurity: A Primer on the Emerging Field of Cyberbiosecurity. In *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (pp. 1–6). Springer International Publishing. https://doi.org/10.1007/978-3-031-26034-6_1.

Heimdal Security. (n.d.). The DCH ransomware attack: A teachable moment in cyber-history. Heimdal Security. Available at: https://heimdalsecurity.com/blog/dch-ransomware-attack/ [Accessed 23 January 2025].

Independent Security Evaluators. (2016). *Securing Hospitals.* Available at: https://securityevaluators.com/hospitalhack/securing_hospitals.pdf.

Jaime, F.J. et al. (2023). Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. *Sensors, 23(21),* 8944. https://doi.org/10.3390/s23218944.

Kumar, D., Hasan, Y., & Afroz, S. (2023). Mobile Health Monitoring System: A Comprehensive Review. *International Journal of Research Publication and Reviews, 4(6),* 1922–1954. https://doi.org/10.55248/gengpi.4.623.45128.

Li, N. et al. (2023). A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. *Security and Safety, 2,* 2022010. https://doi.org/10.1051/sands/2022010.

Machal, M. (2023). An Overview About Connected Medical Devices and Their Risks. *Studies in Health Technology and Informatics, 305,* 119-122.

Milbank Q. (2014). The Milbank quarterly: A multidisciplinary journal of population health and health policy, *92(1),* 114–150. https://doi.org/10.1111/1468-0009.12043.

Noran, S., & Fouad, N. S. (2024). Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation. *European Journal of International Security, 9(4),* 553. https://doi.org/10.1017/eis.2024.19.

Ray, A. (2021). *Cybersecurity for connected medical devices.* Academic Press.

Sana, M. (2024). Privacy and Security Concerns in IoT-based Healthcare Systems. *International Journal of Multidisciplinary Sciences and Engineering, 15(1).*

Schwartz, S. et al. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology, 52(2),* 103-111.

Shankar, D. D., Azhakath, A. S., Khalil, N., J., S., T., M., & K., S. (2024). Data mining for cyber biosecurity risk management – A comprehensive review. *Computers & Security, 137,* 103627. https://doi.org/10.1016/j.cose.2023.103627.

Stouffer, G. A., Morse, M. L., & Smith, W. L. (2015). Medical device innovation: Regulation and the evolution of safety. *National Library of Medicine.*

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of Medical Things. *Health Policy and Technology, 10(3),* 100549. https://doi.org/10.1016/j.hlpt.2021.100549.

Tomulescu, C. (2020). Cyberbiosecurity: A short review. In *Smart Cities International Conference (SCIC) Proceedings,* 8, 393-410.

Torgersen, L. N. S., Schulz, S. M., Lugo, R. G., & Sütterlin, S. (2024). Patient informed consent, ethical and legal considerations in the context of digital vulnerability with smart, cardiac implantable electronic devices. *PLOS Digital Health, 3(5).* https://doi.org/10.1371/journal.pdig.0000507.

United States Government Accountability Office. (2023). *Medical Device Cybersecurity.*

Wilson, A., & Rollman, A. (2022). *Cybersecurity for Medical Devices in a Connected Healthcare System.*

Wu, F., & Kusinitz, A. (2015). Best practices in applying risk management terminology. *Biomed Instrum Technol., spring(suppl),* 19–24.

Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Communications Surveys & Tutorials, 21(4),* 3723. https://doi.org/10.1109/comst.2019.291