Journal of Posthumanism
2025
Volume: 5, No: 5, pp. 3454–3462
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i5.1754

Connected Medical Devices: From Technological Advancement to Legal Risk

Houda Alhoussari[1]

Abstract

Connected Medical Devices (CMDs), a key component of the Internet of Medical Things (IoMT), are revolutionizing healthcare by enabling real-time monitoring and data-driven patient management. However, their growing use also raises major cybersecurity and data protection concerns. In Saudi Arabia, while general frameworks such as the Personal Data Protection Law (PDPL) and Essential Cybersecurity Controls (ECC) offer a foundation, they lack CMD-specific provisions. This article examines the risks associated with CMDs, evaluates the Saudi legal framework in comparison with international standards like GDPR and HIPAA, and identifies regulatory gaps. Through legal and comparative analysis, the study proposes concrete recommendations to enhance security, including secure-by-design principles, stronger penalties for data breaches, and training for healthcare professionals. The findings aim to support Saudi Arabia's Vision 2030 by balancing innovation with robust data protection. This research contributes to the development of a safer and more resilient healthcare system in the digital age.

Keywords: *Internet of Medical Things (IoMT), Connected Medical Devices (CMDs), Cybersecurity in Healthcare, Health Data Protection.*

Introduction

The Internet of Medical Things (IoMT) is transforming healthcare by integrating cutting-edge technologies that enhance diagnostic accuracy, patient care, and treatment outcomes. This ecosystem encompasses diverse innovations, including connected medical devices (CMDs), artificial intelligence-driven imaging systems, smart hospital rooms, and robotic surgery platforms (Alfulij, N., et al., 2024, March 3). Among these, CMDs have emerged as a pivotal component due to their ability to monitor, diagnose, and manage health conditions in real-time. These devices not only improve healthcare delivery but also foster seamless interaction between patients, healthcare professionals, and systems.

While CMDs offer significant potential, their rapid adoption introduces critical challenges, particularly in cybersecurity and data protection (Camara et al., 2015) . These devices handle vast amounts of sensitive health data, making the security and confidentiality of this information a priority. However, the lack of device-specific regulations exacerbates these challenges, especially in jurisdictions like Saudi Arabia, where data protection relies on general frameworks such as the Personal Data Protection Law (PDPL)[2] and Essential Cybersecurity Controls (ECC)[3].

[1] Assistant Professor of Commercial & Digital Law, College of Law – Prince Sultan University, Riyadh, Saudi Arabia, Email: hhoussari@psu.edu.sa, & Researcher at the Western Institute: Law and Europe (IODE), Rennes University, France. Email: houda.alhoussari@univ-rennes.fr,

[2] Personal Data Protection Law, amended pursuant to Royal Decree N (M/148), 27/03/2023.

[3] National Cybersecurity Authority, Essential Cybersecurity Controls, ECC-2 : 2024.

This study addresses the critical question: How can Saudi Arabia secure connected medical devices and the sensitive data they generate while fostering innovation ? It examines the substantial impact of CMDs on healthcare delivery and the economy, identifies key vulnerabilities in their use, and evaluates the effectiveness of existing regulatory frameworks.

The methodology of this study combines a legal and comparative analysis of Saudi Arabia’s PDPL and ECC with international standards such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA).

The study is structured as follows: the first section defines the IoMT and explores its applications, focusing on CMDs. The second section analyzes the risks linked to CMDs, including data security and cybersecurity challenges. The third section reviews the regulatory and protective measures in Saudi Arabia. Lastly, the study concludes with strategic recommendations to enhance data security while promoting sustainable innovation in alignment with Vision 2030.

Research Methodology

This research uses a qualitative legal method. It combines normative legal analysis with comparative reasoning.

The aim is to assess Saudi Arabia’s legal framework for connected medical devices (CMDs). The study identifies regulatory gaps and suggests improvements based on international standards.

The research follows three main steps:

Legal Document Analysis

First, the study reviews key Saudi laws. These include the Personal Data Protection Law (PDPL) and the Essential Cybersecurity Controls (ECC). It also examines SFDA regulations related to CMDs. The analysis focuses on legal definitions, obligations, and data protection measures.

Comparative Legal Review

Second, the study compares the Saudi framework with the EU’s GDPR and the US HIPAA. It examines areas such as data classification, breach notification, and device security. This comparison highlights similarities and regulatory gaps.

Reflexive Assessment

Third, the study reflects on broader legal challenges. It considers how current laws respond to emerging technologies. It also explores ethical concerns, such as accountability and patient trust. The analysis integrates perspectives on cybersecurity, AI, and blockchain.

Sources include legal texts, official policies, academic publications, and cybersecurity reports. This approach ensures a solid and context-sensitive legal evaluation of CMD regulation in Saudi Arabia.

Literature Review

The Internet of Medical Things (IoMT) is increasingly recognized as transformative for healthcare systems globally, significantly enhancing diagnostic precision, patient monitoring, and overall clinical outcomes (Camara et al., 2015; Medtech Deloitte, 2018; Osama et al., 2023). Connected Medical Devices (CMDs), integral components of IoMT, offer substantial improvements in healthcare delivery by enabling real-time health data collection and facilitating patient-provider interaction (Halperin et al., 2008; Umpierrez, 2018). However, the benefits of these technologies are accompanied by critical cybersecurity vulnerabilities and data protection risks, thus requiring rigorous attention to legal and regulatory frameworks (Kosta & Bowman, 2012; Sarabdeen et al., 2022).

Recent literature emphasizes that cybersecurity threats related to CMDs include ransomware attacks, unauthorized access, data interception, and exploitation due to weak authentication methods or insufficient encryption standards (Mahendru, 2024; IBM Security Report, 2023). Additionally, human errors such as using weak passwords or failure to adhere to cybersecurity protocols are highlighted as significant factors contributing to vulnerabilities (Alsharif & Mishra, 2021).

Comparatively, Saudi Arabia's regulatory framework, particularly the Personal Data Protection Law (PDPL) and Essential Cybersecurity Controls (ECC), is recognized for establishing foundational standards for data protection (National Cybersecurity Authority, ECC-2: 2024). Nevertheless, several studies indicate substantial gaps regarding regulations explicitly tailored to CMDs, contrasting significantly with international standards like the European Union's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA), which provide more comprehensive, device-specific data protection protocols (Sarabdeen & Ishak, 2025; Lindstad & Rosager-Ludvigsen, 2023).

Moreover, literature underscores the importance of categorizing health data based on nature, correlation, and purpose, as outlined in Saudi PDPL, emphasizing the necessity for stringent protection measures due to the sensitive nature of this data (Alhoussari, 2025; Lucas, 2017). The application of advanced technological solutions such as blockchain and artificial intelligence is proposed to strengthen cybersecurity practices further, enhancing data integrity and confidentiality (Khallaf et al., 2024; Dhali et al., 2022).

Overall, existing studies agree on the urgency for enhanced regulatory measures, stronger penalties for data breaches, and the adoption of a security-by-design approach to CMD development (Camara et al., 2015; Haut Autorité de santé, 2017). Training healthcare professionals and raising user awareness about cybersecurity threats and protective measures are also identified as critical components for securing CMDs and associated health data effectively (Jobran, 2024; SFDA, 2022). This literature review thus establishes the foundational knowledge necessary for exploring how Saudi Arabia can effectively align its cybersecurity regulations for CMDs with global best practices and Vision 2030 goals.

Concepts

Connected Medical Device

CMD refers to a medical device embedded with digital connectivity features, enabling the exchange of data over networks such as the Internet or wireless systems. These devices are designed to collect, transmit, analyze, and receive data, facilitating real-time health monitoring and management. Specifically, CMDs are used to monitor, diagnose, treat, or manage health conditions, while fostering seamless interaction between patients, healthcare professionals, and medical systems (Haute Autorité de santé, DMC, Nov. 2017).

Wellness Applications

CMDs differ significantly from wellness applications (e.g., MyFitnessPal, Headspace, StepUp, Happify). While wellness applications are primarily focused on promoting general lifestyle and health improvements such as managing stress, tracking physical activity, or monitoring sleep. These applications are not designed to diagnose, treat, or manage medical conditions.

Accurate and scientifically validated data collected by CMDs for medical or clinical purposes, such as heart rate or blood pressure, which are integrated into electronic medical records, can be classified as health data by purpose, as discussed below (Aumans Avocats, March 2024). In contrast, indicative and less precise data collected for personal use, such as step tracking with a pedometer, which is not intended for precision or clinical application, is not considered health data.

This distinction highlights that the functions of CMDs and wellness applications may overlap in certain cases (Alhoussari, 2025).

Categories of Health Data

Health data can be categorized into three main categories:

Health Data by Nature: Saudi data protection law defines health data as personal information concerning an individual's physical, mental, or psychological health, along with healthcare services provided to them. This includes preventive, curative, rehabilitative, and hospitalization services, as well as the provision of medications (Art. 1, Paras. 13 and 14, PDPL). Health data is classified as sensitive when it pertains to highly private information, such as genetic data, biometric data, mental health records, or details about specific conditions, including disabilities or reproductive treatments (Art. 1, Para. 11, PDPL).

By nature, health data includes several key categories, such as clinical data (e.g., medical history, diagnoses, treatments, and information collected through connected medical devices). It also comprises biological and genetic data from analyses or DNA tests, as well as behavioral and psychological data related to lifestyle or mental health (Kosta & Bowman, 2012). These types of data are safeguarded under professional secrecy, as mandated by Article 21 of the Law of Practicing Healthcare Professions.

Health Data by Correlation: This category encompasses health-related data that, when combined with other information, can provide insights into an individual’s health status (e.g., weight and step count, blood pressure and physical exertion). Such data, while not inherently medical, gains significance through correlation with other variables. For example, a combination of step count and weight can indicate activity levels and overall fitness, while blood pressure and physical exertion may reveal potential cardiovascular issues. These correlations highlight the importance of context in interpreting data, as they uncover patterns relevant to prevention, diagnosis, or management of medical conditions.

Additionally, Connected Medical Devices (CMDs) generate financial data, which also gains relevance when correlated with health data. This includes records such as insurance claims, consultation fees, or device maintenance costs. For instance, a continuous glucose monitoring device produces financial data through billing for its use, sensor replacements, and teleconsultations. When combined with other datasets, such as glucose readings or treatment records, this financial data can reveal sensitive information about a patient’s health or financial situation. The interplay between these data types underscores the need for strict privacy protections to ensure confidentiality and prevent misuse (Medtech Deloitte, 2018).

Health Data by Purpose: This refers to data that acquires the status of health data due to its use for medical purposes, even though it is not inherently medical in nature (e.g., sleep quality). For instance, data related to an individual's physical activity, dietary habits, or environmental exposure can be classified as health data when utilized to assess, prevent, or manage medical conditions. Such data often becomes critical when integrated into medical decision-making processes or electronic health records, as it provides insights that support personalized care, diagnosis, or treatment planning.

The classification of these data types highlights the importance of their context and usage, underscoring the need for proper protection to maintain their confidentiality and integrity within healthcare systems.

Type of Connected Medical Devices

Connected medical devices include a variety of technologies designed to meet diverse healthcare needs. Among them are:

- Health Monitoring Devices: These include smartwatches and fitness trackers designed to measure vital parameters such as heart rate, blood pressure, and oxygen saturation. These devices provide real-time insights into an individual's health, enabling early detection of anomalies and promoting proactive healthcare management (Halperin et all, 2008, 129)

- Devices tailored to specific conditions, such as smart insulin pumps or continuous glucose monitoring systems, which simplify diabetes management by automating aspects of care (Umpierrez, 2018).

- Remote monitoring solutions, which enable healthcare professionals to track patients' health conditions at home, reducing unnecessary hospitalizations. Connected rehabilitation devices, such as smart physiotherapy equipment, assist patients in performing exercises correctly and independently.

- Implantable connected medical devices, equipped with software capable of communicating and transmitting data to external devices. These technological advancements significantly enhance patients' quality of life (Sarabdeen et al., 2022).

- Simpler devices, such as fall detection sensors, play a crucial role in promoting the independence of elderly individuals living alone.

These technologies collectively contribute to transforming healthcare delivery, improving patient outcomes, and fostering autonomy and well-being across various demographics.

Discussion and Results

Threats Associated with the Use of Connected Medical Devices

The use of CMDs offers significant advantages but also comes with various threats. These risks include:

Data Security Threats

Sensitive medical data and patients' financial information face significant risks of theft or fraud. Even when anonymized, such data is not immune to re-identification, particularly when cross-referenced with other datasets or sources. Ineffective data management practices can further exacerbate these vulnerabilities, compromising confidentiality, diminishing patient trust, and potentially leading to instances of discrimination (Mahendru, 2024).

Cybersecurity Threats

CMDs are vulnerable to ransomware attacks, where malicious software locks their functionality until a ransom is paid, thereby compromising their availability to patients (Osama et all, 2023). Additionally, these devices can serve as entry points into healthcare systems, and the data transmitted to these systems is at risk of interception if communications are not adequately secured with robust encryption protocols. Finally, software vulnerabilities or weak authentication mechanisms can lead to unauthorized access to CMDs, exposing patients to risks both to their health and the confidentiality of their data (SFDA, 2022).

These threats underscore the urgent need for intervention to secure connected medical devices and the sensitive health data they generate.

Review of Protection Measures for Connected Medical Devices in Saudi Arabia

Regulatory Framework

In Saudi Arabia, connected medical devices are strictly regulated by the Saudi Food and Drug Authority (SFDA). To market these devices in the Saudi market, manufacturers must obtain a Medical Device Marketing Authorization (MDMA), which certifies their compliance with required safety and efficacy standards (Jobran, 2024).

The registration process involves the submission of a detailed technical dossier, including information on the design, manufacturing, clinical performance, and risk management of the device. Foreign manufacturers are also required to appoint a local Authorized Representative (AR) to facilitate communication with the SFDA and ensure ongoing compliance with the applicable regulations (SFDA, 2022).

Additionally, the SFDA has implemented a Unique Device Identification (UDI) system, requiring each medical device to be assigned a unique identifier to enhance traceability and post-market surveillance. UDI information must be registered in the SFDA's UDI system, with this requirement being applied progressively based on the device's risk class (Lucas, 2018).

It is crucial for manufacturers to comply with these stringent regulations to ensure patient safety and maintain the integrity of the Saudi healthcare system.

Health Data Protection and Regulatory Comparisons

The protection of health data generated by CMDs in Saudi Arabia is not governed by specific regulations. Instead, it relies on general regulatory frameworks governing personal data, such as the PDPL and the ECC**.**

Firstly, the PDPL places significant emphasis on health data due to its sensitive nature. It imposes strict consent requirements for the collection (Jobran, 2024), processing, and storage of such data, ensuring its security and use solely for legitimate purposes, such as medical care, scientific research, or the management of public health crises (Articles 2 and 3, PDPL). The law also acknowledges the responsibility of medical institutions to ensure data security and promptly report any breaches.

Secondly, the ECC**,** developed by the National Cybersecurity Authority (NCA), provide a critical framework for protecting critical systems, including CMDs. These controls are based on the CIA triad (Confidentiality, Integrity, Availability). They aim to ensure the confidentiality of health data by implementing measures such as data encryption in transit and at rest, thereby preventing unauthorized access. The integrity of information is maintained through mechanisms like multi-factor authentication and intrusion detection systems (SIEM), which help prevent and rectify unauthorized alterations to data. Finally, the availability of critical systems is enhanced through strategies like network segmentation and regular software updates (Khallaf et al. 2024), ensuring continuous and secure access to data even in the event of a cyberattack (ECC, 2024).

In comparison with international standards (Sarabdeen & Ishak? 2025) such as the GDPR and HIPAA, it is notable that only HIPAA specifically addresses connected devices when they handle Electronic Protected Health Information (ePHI) in the medical field, requiring specific measures for their security (45 CFR § 164.308 to § 164.316 HIPAA). In contrast, neither the GDPR nor the PDPL provides specific rules applicable to connected medical devices (Lindstad & Rosager-Ludvigsen, 2023). The second notable difference among these three standards is the weaker penalties for health data breaches under the PDPL, which are capped at 5 million SAR (Art. 35), compared to 20 million euros under the GDPR and 1.5 million USD under HIPAA.

However, the effective implementation of these measures remains limited in light of the significant challenges posed by CMDs.

Implementation Challenges

Vulnerability of CMDs

These technologies exhibit critical vulnerabilities that make them particularly susceptible to cyberattacks. Often deployed without robust security protocols, IoMT devices are exposed to external intrusions, primarily due to a lack of regular updates. This weakness was highlighted in a study conducted by Kaspersky (2020), which revealed that over 70% of these devices are not properly updated (IBM Report, 2023). The root of this vulnerability lies in the absence of integrated security from the design phase (Security by Design), where encryption is not consistently applied before transmitting data.

Human Errors

Human errors represent a major vulnerability in cybersecurity. Risky practices, such as using weak passwords or sharing information insecurely, expose these devices to cyberattacks. For instance, a cyberattack in 2022 on a hospital network in Saudi Arabia revealed that default passwords were still being used for some critical connected devices, compromising the security of sensitive data generated and exchanged by these systems (Alsharif & Mishra, 2021).

Recommendation to strengthen data security

To strengthen the security of health data, It is crucial To:

1. *Enhance Regulations and Penalties:* Mandate the reporting of data breaches, enforce stricter penalties for violations involving sensitive data, and align Saudi regulations with international standards (e.g., GDPR, HIPAA) for cross-border data transfers.

2. *Strengthen Device Security from the Design Phase (Security by Design)* Incorporate robust security mechanisms, such as encryption and multi-factor authentication, into CMDs from the design stage and adopt recognized cybersecurity standards to ensure uniform protection.

3. *Train and Raise Awareness Among Users:* Implement training programs for healthcare professionals on cybersecurity best practices and educate patients using connected devices at home on essential security measures.

4. *Implement Regular Audits and Controls*: Ensure automatic and regular software updates while maintaining the compatibility of devices with modern cybersecurity technologies.

5. *Adopt Technological Innovations*: Leverage artificial intelligence to detect threats (Dhali et al., 2022) and blockchain technology (Alhoussari, 2025) to secure data exchanges effectively.

Conclusion

Connected Medical Devices represent a major breakthrough in healthcare, offering unprecedented opportunities to enhance patient care and management. However, these technologies come with significant challenges, particularly in terms of cybersecurity and data protection. A proactive approach that combines robust regulatory frameworks, secure-by-design devices, regular updates, and increased user awareness is essential to ensure their safety and maintain patient trust. Investing in these measures is crucial to maximize the benefits of CMDs while minimizing the associated risks.

Acknowledgments

Author of this Article would like to thank the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU) for their financial and academic support to conduct this research and publish it in a reputable Journal.

References

Alfulij, N., Kasabi, M., Aldeeb, H. (2024, March 3). Medical errors in robotic surgery in Islamic jurisprudence and law. IEEE, 116–120.

Alhoussari, H. (2025). Blockchain and healthcare data. In Blockchain & Privacy (pp. 105–123). Bruylant.

Alhoussari, H. (2025). Securing health data in the digital age: Challenges, regulatory frameworks, and strategic solutions in Saudi Arabia. Creative Publishing House. https://doi.org/10.62754/joe.v4i1.6052

Alsharif, M., & Mishra, S. (2021). Impact of human vulnerabilities on cybersecurity. Computer Systems Science and Engineering, 40. DOI:10.32604/csse.2022.019938.

Aumans Avocats. (2024, March 25). Objets connectés de santé : enjeux juridiques. https://aumans-avocats.com/objets-connectes-de-sante-enjeux-juridiques/

Barrett, M., Boyne, J & Brandts, J. (2019). Artificial intelligence supported patient self-care in chronic heart failure: A paradigm shift from reactive to predictive, preventive and personalised care. EPMA Journal, 10, 445–448.

Bibi, L., Hamma, H & Srikaran, I. (2023). Cas d'utilisation des dispositifs médicaux connectés en France. Mémoire. https://doi.org/10.34746/ids173

Camara, C., Peris-Lopez, P., & Tapiador, J. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 55, 272–289. https://doi.org/10.1016/j.jbi.2015.04.007

Deloitte Centre for Health Solutions. (2018, July). Medtech and the Internet of Medical Things: How connected medical devices are transforming health care.

European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union.

Halperin, D., Heydt-Benjamin, T & Ransford, B, (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero power defenses. Proceedings—IEEE Symposium on Security and

Privacy, 129.

Haut Autorité de Santé. (2017, November). Dispositifs médicaux connectés (DMC) : Guide pour le dépôt d'un dossier auprès de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé.

Health Insurance Portability and Accountability Act, USA,1996.

IBM Security Report (2023) sur les cybermenaces dans le secteur de la santé.

Jobran, M. (2024, November 14). Enregistrement des dispositifs médicaux SFDA (MDMA).

Khallaf, F., Ali, M., Alkhaldi, M., & Alotaibi, A. (2024, September). Blockchain-based color medical image cryptosystem for industrial Internet of Healthcare Things (IoHT). Springer Netherlands. https://doi.org/10.1007/s11042-023-16777-w

Kosta, E., & Bowman, D.-M. (2012). Implanting implications: Data protection challenges arising from the use of human ICT implants. In D. M. Gasson et al. (Eds.), Human ICT Implants: Technical, Legal and Ethical Considerations (p. 102). TMC Asser Press.

Lindstad, S., & Rosager-Ludvigsen, K. (2023). When is the processing of data from medical implants lawful? Medical Law Review, 31, 317–339. DOI: 10.1093/medlaw/fwac038

Lucas, J. (2017). Sharing personal data with computerised uses in regards of patient's explicit free consent. Ethics, Medicine and Public Health, 3, 10–18.

Mahendru, P. (2024, August 5). The state of ransomware in the healthcare sector in 2024. SOPHOS. https://news.sophos.com/fr/2024/08/05/etat-des-ransomwares-dans-le-secteur-de-la-sante-en-2024/

Mahendru, P. "The state of ransomware in the healthcare sector in 2024", SOPHOS, https://news.sophos.com/fr/2024/08/05/etat-des-ransomwares-dans-le-secteur-de-la-sante-en-2024/

National Cybersecurity Authority. (2024). Essential Cybersecurity Controls (ECC-2).

Osama, M., Ateya, A & Sayed, M. (2023, August). Internet of Medical Things and Healthcare 4.0: Trends, requirements, challenges, and research directions. MDPI. https://doi.org/10.3390/s23177435

Personal Data Protection Law, amended pursuant to Royal Decree No. M/148. (2023, March 27).

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Sarabdeen, J., & Ishak, M. (2025). A comparative analysis: Health data protection laws in Malaysia, Saudi Arabia, and EU General Data Protection Regulation (GDPR). International Journal of Law and Management, 67(1), 99–119. https://doi.org/10.1108/IJLMA-01-2024-0025.

Sarabdeen, J., Chikhaoui, E., & Mazahir, M. (2022). Creating standards for Canadian health data protection during health emergency – An analysis of privacy regulations and laws. Heliyon, 8(5), e09458. https://doi.org/10.1016/j.heliyon.2022.e09458.

SFDA. (2022). Requirements for Unique Device Identification (UDI) for Medical Devices (Version 4.0).

Umpierrez, G & Klonoff, D. (2018). Diabetes technology update: Use of insulin pumps and continuous glucose monitoring in the hospital. Diabetes Care, 41(8), 1579–1589.